CYBERSÉCURITÉ

Comprendre la cybercriminalité : PHÉNOMÈNE, DIFFICULTÉS ET RÉPONSES JURIDIQUES

Rapport

Secteur du développement des télécommunications

Comprendre la cybercriminalité: phénomène, difficultés et réponses juridiques

Novembre 2014

La publication de l'UIT intitulée *«Comprendre la cybercriminalité: phénomène, difficultés et réponses juridiques»* a été préparée par le Professeur Marco Gercke. L'auteur remercie l'équipe du Département infrastructures, environnement propice et cyberapplications (IEE) du Bureau de développement des télécommunications de l'UIT.

La présente publication est disponible en ligne à l'adresse: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

Merci de penser à l'environnement avant d'imprimer ce rapport.

Table des matières

Page

Objectif

Le rapport de l'UIT intitulé «Comprendre la cybercriminalité: phénomène, difficultés et réponses juridiques» se propose d'aider les pays intéressés à comprendre les aspects juridiques de la cybercriminalité et de la cybersécurité et de contribuer à l'harmonisation des cadres juridiques. Dès lors, il vise à aider les pays à mieux comprendre les effets, au niveau national comme au niveau international, de la montée en puissance des cybermenaces, à prendre la mesure des obligations imposées par les instruments régionaux, nationaux et internationaux en vigueur, et à construire un cadre juridique solide.

Le présent rapport propose une vue d'ensemble des questions les plus pertinentes relatives aux aspects juridiques de la cybercriminalité, essentiellement envisagées sous l'angle de la demande des pays en développement. S'il est vrai que, du fait de la dimension transnationale de la cybercriminalité, les mêmes instruments juridiques s'appliquent aux pays développés et aux pays en développement, les références ont toutefois été choisies sous l'angle de ces derniers. En outre, un grand nombre de ressources permettront d'approfondir les différents sujets. Il est fait référence, dans toute la mesure possible, à des sources librement accessibles au public, y compris de nombreuses éditions gratuites de revues juridiques en ligne.

Le présent rapport est composé de six grands chapitres. Après une introduction (Chapitre 1), il propose une vue d'ensemble du phénomène de la cybercriminalité (Chapitre 2), notamment une description des modalités de commission des infractions et une explication des cyberdélits les plus courants, tels que le piratage, le vol d'identité et les attaques par refus de service. Il fournit également un aperçu des difficultés liées aux enquêtes sur les cyberdélits et à la poursuite en justice de leurs auteurs (Chapitres 3 et 4). Après un résumé des activités menées par certaines organisations régionales et internationales pour lutter contre la cybercriminalité (Chapitre 5), le rapport présente une analyse de différentes approches juridiques en matière de droit pénal matériel, de droit procédural, de coopération internationale et de responsabilité des fournisseurs d'accès à Internet (Chapitre 6), notamment des exemples de démarches adoptées au niveau international et de bonnes pratiques tirées de solutions retenues au niveau national.

La présente publication s'emploie à répondre au premier des sept buts stratégiques du Programme mondial cybersécurité (GCA) de l'UIT, qui préconise l'élaboration de stratégies en vue d'établir une législation en matière de cybercriminalité qui soit applicable à l'échelle mondiale et compatible avec les dispositions réglementaires en vigueur aux niveaux national et régional, et s'inscrit dans la démarche d'élaboration d'une stratégie nationale de la cybersécurité préconisée par la Commission d'études Q22/1 de l'UIT-D. La mise en place d'une infrastructure juridique appropriée fait partie intégrante de toute stratégie nationale de cybersécurité. Le mandat de l'UIT en matière de renforcement des capacités a été précisé par la Résolution 130 (Rév. Guadalajara, 2010) de la Conférence de plénipotentiaires de l'UIT sur le Renforcement du rôle de l'UIT pour « établir la confiance et la sécurité dans l'utilisation des TIC ». Pour assurer une cybersécurité au niveau mondial, il est essentiel que tous les Etats adoptent une législation adaptée contre l'exploitation des technologies de l'information et de la communication à des fins criminelles ou autres, y compris les activités visant à nuire à l'intégrité des infrastructures essentielles de l'information au niveau national. Etant donné que les menaces peuvent provenir de n'importe quel endroit de la planète, les enjeux sont, par essence, de portée internationale et appellent une coopération de tous les pays, une assistance aux enquêtes et des dispositions communes en matière de droit matériel et de droit procédural. Pour lutter contre la cybercriminalité et faciliter la coopération internationale, il est donc essentiel que les Etats harmonisent leurs cadres juridiques.

Déni de responsabilité concernant les liens hypertextes

Le présent rapport contient des centaines de liens qui renvoient le lecteur vers des documents mis à la disposition du public. Toutes les références ont été vérifiées à la date de l'ajout de ces liens aux notes de bas de page. Toutefois, il ne peut être garanti que le contenu actualisé des pages auxquelles renvoient de tels liens reste identique. Par conséquent, les références, dans toute la mesure possible, incluent également des informations concernant l'auteur ou l'institution responsable de la publication, le titre et, si possible, l'année de la publication pour permettre au lecteur de rechercher le document concerné si le lien n'est plus actuel.

1. Introduction

Bibliography (selected): *Aggarwal,* Role of e-Learning in A Developing Country Like India, Proceedings of the 3rd National Conference, INDIA, Com 2009*; Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Choudhari/Banwet/Gupta*, Identifying Risk Factors in for E-governance Projects, published in Wgarwal/Ramana, Foundations of E-government, 2007, page 270 *et. seq.*; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe, 2006; *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 *et seq.*; *European Commission,* Final Report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure, 2009; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141 *et seq.*; *Gercke*, Cybersecurity Strategy, Computer Law Review International 2013, 136 *et seq.; Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2; *Masuda*, The Information Society as Post-Industrial Society, 1980; *Molla*, The Impact of eReadingness on eCommerce Success in Developing Countries, 2004; *Ndou*, E-Government for Developing Countries, Opportunities and Challenges, DJISDC 2004, 18, page 1 *et seq.*; *Luiijf/Klaver*, In Bits and Pieces, Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society, 2000; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, 2005; *Tanebaum*, Computer Networks, 2002; *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1; *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52-56; *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2.

1.1 Infrastructures et services

Internet est l'une des infrastructures techniques dont la croissance est la plus rapide[1]. Les technologies de l'information et de la communication (TIC) sont aujourd'hui omniprésentes et la tendance à la numérisation va grandissant. La demande de connectivité à Internet et d'interconnexion des systèmes a conduit à l'intégration de l'informatique dans des produits qui, jusqu'alors, en étaient dépourvus, notamment les voitures et les bâtiments[2]. La distribution d'électricité, les infrastructures de transport, les services (notamment logistiques) des armées, etc., quasiment tous les services du monde moderne dépendent des TIC[3].

Si ces nouvelles technologies visent principalement à répondre à la demande des consommateurs occidentaux, les pays en développement peuvent aussi en tirer profit[4]. Etant donné qu'il est aujourd'hui possible d'acquérir un ordinateur pour moins de 200 USD[5], et de communiquer par voie hertzienne sur de longues distances (par WiMAX[6] par exemple), la plupart des habitants de pays en développement doivent être en mesure, plus facilement que jamais, d'accéder à Internet et aux produits et services qui en dépendent[7].

Au-delà du développement des infrastructures élémentaires pour mettre en œuvre ces nouvelles technologies, la société se transforme: les TIC servent de base au développement, à la fourniture et à l'utilisation des services en réseau[8]. Le courriel a supplanté le courrier traditionnel[9]; dans le monde des affaires, la présence sur le Web prime sur la diffusion publicitaire sur papier[10]; les services de communication et de téléphonie via Internet se développent plus rapidement que les communications filaires[11].

La société dans son ensemble, et les pays en développement en particulier, tirent des TIC et des nouveaux services en réseau un certain nombre d'avantages.

Les applications TIC (cybergouvernance[12], commerce électronique[13], cyberenseignement[14], cybersanté[15] et cyberenvironnement, etc.), vecteurs efficaces de la fourniture d'une large gamme de services de base dans les régions éloignées et zones rurales, sont considérées comme des facteurs de développement. Elles

peuvent faciliter la réalisation des objectifs de développement du millénaire, en luttant contre la pauvreté et en améliorant les conditions sanitaires et environnementales des pays en développement. Sous réserve d'adopter une bonne démarche, de se situer dans un contexte approprié et d'utiliser les processus de mise en œuvre adéquats, les investissements en faveur des applications et des outils TIC permettent d'améliorer la productivité et la qualité. En outre, les applications TIC peuvent renforcer les capacités techniques et humaines et faciliter l'accès aux services de première nécessité. A cet égard, le vol d'identité en ligne et la capture des justificatifs d'identité d'une personne et/ou de ses informations personnelles par Internet, avec l'intention de les réutiliser à des fins criminelles, sont aujourd'hui les principales menaces à l'expansion des services de cybergouvernance et de commerce électronique[16].

Le coût des services en ligne est souvent très inférieur à celui des services comparables hors ligne[17]. Ainsi, contrairement aux services postaux traditionnels, les services de messagerie électronique sont souvent gratuits ou proposés pour une somme modique[18]. L'encyclopédie en ligne Wikipedia[19] est accessible gratuitement, de même que des centaines de services d'hébergement en ligne[20]. Or, la modicité des coûts joue un rôle essentiel, car elle permet à de nombreux utilisateurs, y compris aux personnes aux revenus limités, d'avoir accès à ces services. C'est notamment le cas de nombreux habitants des pays en développement.

1.2 Avantages et risques

L'utilisation des TIC dans de nombreux domaines de la vie quotidienne a conduit à introduire le concept moderne de « société de l'information »[21], modèle de société qui offre d'immenses possibilités[22]. Ainsi, mettre l'information en libre accès, c'est la retirer des mains du pouvoir central et donc renforcer la démocratie (voir, par exemple, ce qui s'est passé en Europe de l'Est et en Afrique du Nord)[23]. De plus, certaines évolutions techniques améliorent notre quotidien, notamment les systèmes de banque et de boutique en ligne, les services mobiles de transmission de données et la téléphonie sur IP (VoIP). Ces quelques exemples montrent à quel point les TIC font aujourd'hui partie de notre quotidien[24].

Cela étant, l'expansion de la société de l'information s'accompagne de nouveaux dangers et de graves menaces[25]. En effet, des services essentiels, tels que la distribution d'eau et d'électricité, s'appuient aujourd'hui sur les TIC[26]. De même, les voitures, la régulation du trafic, les ascenseurs, la climatisation et le téléphone reposent sur la bonne marche de ces nouvelles technologies[27]. Menaces d'un nouveau genre, les attaques visant les infrastructures de l'information et les services Internet sont donc susceptibles de porter gravement atteinte à la société[28].

On recense déjà de telles attaques[29]: fraude en ligne, opérations de piratage, pour ne citer que quelques exemples d'infractions informatiques commises chaque jour à grande échelle[30]. Les pertes financières dues à la cybercriminalité sont extrêmement élevées[31]. Pour la seule année 2003, les logiciels malveillants ont causé jusqu'à 17 milliards USD de pertes[32]. Selon certaines estimations, les recettes provenant de la cybercriminalité ont atteint plus de 100 milliards USD en 2007, dépassant pour la première fois le marché illégal des stupéfiants[33]. D'après des travaux de recherche publiés en 2014, les pertes annuelles mondiales imputables à la cybercriminalité pourraient atteindre les 400 milliards USD. [34] Presque 60% des entreprises aux Etats-Unis estiment que la cybercriminalité leur coûte plus que les infractions matérielles[35]. Ces estimations le montrent clairement, il est vital de protéger les infrastructures de l'information[36].

La plupart des attaques mentionnées ci-dessus ne ciblent pas nécessairement l'infrastructure essentielle. Cela étant, le logiciel malveillant « Stuxnet », découvert en 2010, souligne la menace que présentent les attaquent visant l'infrastructure vitale[37]. Ce logiciel doté de plus de 4 000 fonctions[38] ciblait les systèmes informatiques qui exécutent des programmes généralement utilisés pour contrôler l'infrastructure essentielle[39].

1.3 Cybersécurité et cybercriminalité

La cybercriminalité et la cybersécurité sont difficilement dissociables au sein de l'environnement interconnecté. L'indissociabilité de ces deux aspects est mise en évidence par la Résolution de l'Assemblée

générale des Nations Unies de 2010 sur la cybersécurité[40], qui considère la cybercriminalité comme un défi majeur.

La cybersécurité[41] joue un rôle essentiel dans le développement des technologies de l'information et des services en ligne[42]. Pour garantir leur sécurité et leur bien-être économique, tous les pays doivent absolument renforcer la cybersécurité (et la protection des internautes) et protéger les infrastructures essentielles de l'information, objectif qui préside aujourd'hui au développement des nouveaux services, mais aussi à l'élaboration des politiques gouvernementales[43]. La prévention de la cybercriminalité fait partie intégrante de toute stratégie nationale de cybersécurité et de protection des infrastructures essentielles de l'information, ce qui comprend notamment l'adoption d'une législation appropriée contre l'utilisation des TIC à des fins criminelles ou autres et contre les activités visant à nuire à l'intégrité des infrastructures essentielles du pays. Au niveau national, il s'agit d'une responsabilité commune, qui demande de la part des autorités, du secteur privé et de la population une action coordonnée en matière de prévention, de préparation, de résolution des incidents et de reprise après incident. Au niveau régional et international, cela suppose une coopération et une coordination avec les partenaires concernés. L'élaboration et la mise en place d'un cadre et d'une stratégie au niveau national en matière de cybersécurité exigent donc une approche globale[44]. Les stratégies de cybersécurité – par exemple, le développement de systèmes techniques de protection ou la prévention, par la formation, des victimes de la cybercriminalité – peuvent contribuer à réduire les risques d'infraction dans le cyberespace[45]. Il est donc primordial, pour lutter contre la cybercriminalité, de développer et de soutenir les stratégies de cybersécurité[46].

La question de la cybersécurité pose des problèmes juridiques, techniques et institutionnels de dimension planétaire et de portée considérable, qui ne peuvent être résolus que par une stratégie cohérente, en tenant compte des initiatives existantes et du rôle des différentes parties prenantes, dans le cadre d'une coopération internationale[47]. A cet égard, le Sommet mondial sur la société de l'information (SMSI)[48] reconnaît les risques réels et importants que présentent une cybersécurité insuffisante et la prolifération de la cybercriminalité. Les paragraphes 108 à 110 de *L'Agenda de Tunis du SMSI pour la société de l'information*[49], annexe comprise, exposent un plan pour la mise en œuvre de multi-parties prenantes au niveau international du *Plan d'action de Genève du SMSI*[50]. Ces paragraphes décrivent ce processus selon onze grandes orientations et attribuent des responsabilités afin d'en faciliter la mise en œuvre. Lors du sommet, les dirigeants et les gouvernements mondiaux ont désigné l'UIT coordonnateur de la mise en œuvre de la grande orientation C5 du SMSI, « Etablir la confiance et la sécurité dans l'utilisation des TIC »[51].

En vertu de ce mandat, le Secrétaire général de l'UIT a lancé, le 17 mai 2007, le Programme mondial cybersécurité (GCA)[52], au côté de partenaires représentant des gouvernements, le secteur privé, des organisations régionales et internationales, des établissements universitaires et des organismes de recherche. Le GCA est un cadre mondial pour le dialogue et la coopération internationale, dont le but est de coordonner la réponse internationale à donner aux questions de plus en plus pressantes en matière de cybersécurité et d'améliorer la confiance et la sécurité dans la société de l'information. Il se situe dans le prolongement de travaux, d'initiatives et de partenariats existants, l'objectif étant de proposer des stratégies de niveau international, pour faire face aux enjeux actuels en matière de renforcement de la confiance et de la sécurité dans l'utilisation des TIC. Au sein de l'UIT, le Programme mondial cybersécurité vient compléter les programmes de travail existants en facilitant, dans un cadre de coopération internationale, la mise en œuvre des activités des trois Secteurs de l'UIT en matière de cybersécurité.

Le GCA comporte sept buts stratégiques principaux, qui s'articulent autour de cinq domaines de travail: 1) Cadre juridique; 2) Mesures techniques et de procédure; 3) Structures organisationnelles; 4) Renforcement des capacités et 5) Coopération internationale[53].

Pour lutter contre la cybercriminalité, il est nécessaire d'adopter une démarche globale. Etant donné que les mesures techniques à elles seules ne sauraient prévenir une infraction, quelle qu'elle soit, il est essentiel de permettre aux instances de répression d'enquêter sur les actes de cybercriminalité et de poursuivre en justice leurs auteurs de façon efficace[54]. Le domaine de travail « Cadre juridique » du GCA se concentre sur la manière de répondre, de façon compatible à l'échelle internationale, aux problèmes juridiques que posent les activités criminelles commises sur les réseaux TIC. Le domaine « Mesures techniques et de procédure » s'intéresse aux mesures phares visant à promouvoir l'adoption de démarches améliorées, notamment des mécanismes, des protocoles et des normes d'accréditation, pour renforcer la gestion de la

sécurité et du risque dans le cyberespace. Le domaine « Structures organisationnelles » porte essentiellement sur la prévention des cyberattaques, leur détection, les interventions à mener contre ces attaques et la gestion des crises qu'elles déclenchent, y compris la protection des infrastructures essentielles de l'information. Le domaine de travail « Renforcement des capacités » est consacré à l'élaboration de stratégies visant à développer des mécanismes de renforcement des capacités afin de sensibiliser les parties concernées, de transférer le savoir-faire et d'encourager la prise en compte de la cybersécurité dans les programmes politiques nationaux. Enfin, le domaine de travail « Coopération internationale » se concentre sur la coopération, le dialogue et la coordination à l'échelle internationale dans la lutte contre les cybermenaces.

Elément essentiel d'une stratégie de cybersécurité, l'élaboration d'une législation appropriée et, dans ce contexte, la définition d'un cadre juridique en matière de cybercriminalité. A cet égard, il convient tout d'abord de mettre en place les dispositions de fond en droit pénal nécessaires pour sanctionner les actes de fraude informatique, d'accès illicite, d'atteinte à l'intégrité des données ou à la propriété intellectuelle, de pornographie mettant en scène des enfants, etc.[55] A noter que l'existence, dans le code pénal, de dispositions visant des actes analogues commis en dehors d'Internet n'implique pas nécessairement l'applicabilité desdites dispositions à des actes perpétrés sur le réseau[56]. Il est donc essentiel d'analyser en détail les lois nationales en vigueur afin d'identifier les éventuelles lacunes[57]. Outre les dispositions de fond en droit pénal[58], les instances de répression doivent disposer des mécanismes et des instruments nécessaires pour instruire les affaires de cybercriminalité[59]. L'instruction de ce type d'affaire présente des difficultés[60], en particulier du fait que les auteurs de ces infractions peuvent agir à partir de n'importe quel endroit sur la planète (ou presque), tout en masquant leur identité[61]. En conséquence, ces mécanismes et instruments peuvent être assez différents de ceux utilisés pour enquêter sur les infractions classiques[62]

1.4 Dimensions internationales de la cybercriminalité

La cybercriminalité présente souvent une dimension internationale[63]. On notera par exemple que les contenus illicites transmis par courrier transitent souvent par plusieurs pays avant d'atteindre leur destinataire. Parfois, ils ne sont pas stockés dans le pays mais à l'étranger[64]. Il est donc essentiel que les Etats concernés par un cyberdélit collaborent étroitement aux enquêtes diligentées[65], ce que les accords en vigueur en matière d'entraide judiciaire ne favorisent pas, car ils reposent sur des procédures formelles et complexes, qui prennent souvent beaucoup de temps, et ne couvrent généralement pas les enquêtes spécifiques aux infractions informatiques[66]. Il est donc crucial de réviser les procédures afin de pouvoir rapidement réagir aux incidents et répondre aux demandes de coopération internationale[67].

Dans de nombreux pays, le régime d'entraide judiciaire repose sur le principe de la « double criminalité »[68]. C'est pourquoi une enquête internationale n'est généralement ordonnée que si l'infraction est sanctionnée dans tous les pays impliqués. Il existe certes des infractions, telles que la distribution de matériel pornographique impliquant des enfants, qui peuvent faire l'objet de poursuites n'importe où dans le monde, mais, malgré tout, les différences régionales jouent un rôle important[69]. C'est le cas notamment des infractions pour contenu illicite, par exemple discours haineux, qui sont sanctionnées différemment selon les pays[70]: il n'est pas rare que certains contenus légalement autorisés par certains soient jugés illicites par d'autres[71].

Partout dans le monde, l'informatique repose fondamentalement sur la même technologie[72]. Ainsi, à l'exception des différences linguistiques et du format des prises de courant, les ordinateurs et les téléphones portables vendus en Asie ressemblent de très près à ceux vendus en Europe. Le cas d'Internet n'est pas différent: du fait de la normalisation des réseaux, les pays africains utilisent les mêmes protocoles que les Etats-Unis[73]. C'est aussi pour cette raison que les internautes du monde entier peuvent avoir accès aux mêmes services[74].

Se pose alors la question des effets de l'harmonisation des normes techniques au niveau mondial sur l'évolution du droit pénal au niveau de chaque pays. En effet, s'agissant des contenus illicites, les internautes peuvent avoir accès à des informations venant du monde entier, et donc à certains contenus disponibles légalement à l'étranger mais considérés comme illicites dans leur pays.

L'harmonisation des normes techniques a donc permis la mondialisation des technologies et des services, mais elle devrait aller bien au-delà et conduire à l'harmonisation des législations nationales. Cependant, comme l'ont montré les négociations portant sur le premier Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité[75], le droit national évolue beaucoup plus lentement que les techniques[76].

Or, si Internet ne connaît pas les contrôles aux frontières, des moyens existent cependant de restreindre l'accès à certaines informations[77]. Le fournisseur d'accès peut, en général, bloquer l'accès à certains sites; l'hébergeur d'un site peut, de son côté, refuser les connexions venant de certains pays en filtrant les adresses IP (on parle de « ciblage IP »)[78]. Ces deux mesures, certes non sans faille, demeurent des instruments utiles pour préserver des différences territoriales dans un réseau mondial[79]. L'OpenNet Initiative[80] signale qu'une vingtaine de pays environ pratiquent ce type de censure[81].

1.5 Conséquences pour les pays en développement

Trouver des stratégies de riposte et des solutions aux menaces que présente la cybercriminalité est un défi majeur, tout spécialement pour les pays en développement. Une stratégie anticybercriminalité globale comporte généralement des mesures de protection technique ainsi que des instruments juridiques[82], dont l'élaboration et la mise en œuvre demandent du temps. Les mesures de protection techniques s'avèrent particulièrement coûteuses[83]. Les pays en développement doivent intégrer les mesures de protection dès le début du processus de mise en place d'Internet. En effet, bien qu'une telle approche risque, dans un premier temps, d'augmenter le coût des services Internet, elle permet d'éviter les coûts et les préjudices liés à la cybercriminalité et donc d'augmenter les gains à long terme, lesquels compensent largement tout investissement initial dans des mesures de protection technique et de garantie des réseaux[84].

Les pays en développement mettent en place des garde-fous moins efficaces. Ils sont donc exposés, plus que les autres, aux risques liés à l'insuffisance des mesures de protection[85]. S'il est impératif que les commerces traditionnels aient les moyens de protéger les consommateurs et les entreprises, il n'en va pas autrement des commerces en ligne ou reposant sur Internet. En effet, en l'absence de dispositifs de sécurité efficaces sur le réseau, les pays en développement pourraient avoir de grandes difficultés à promouvoir le commerce électronique et à prendre part à l'industrie des services en ligne.

Les pays développés, mais aussi les pays en développement, doivent impérativement élaborer des mesures techniques de promotion de la cybersécurité ainsi qu'une véritable législation de lutte contre la cybercriminalité. Si l'on considère les dépenses liées à la mise en place de garde-fous et de mesures de protection sur un réseau informatique existant, il y a tout lieu de croire qu'il faut prévoir ces dispositifs de sécurité dès la mise en place du réseau afin de réduire les coûts. Par ailleurs, il importe que les pays en développement mettent leur stratégie anticybercriminalité d'emblée en conformité avec les normes internationales.[86]

[1] On the development of the Internet, see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52 – 56; The World Information Society Report 2007, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information, see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[2] Regarding the threat of attacks against computer systems integrated in cars, see: BBC News, Cars safe from computer viruses, 11.05.2005, available at: http://news.bbc.co.uk/1/hi/technology/4536307.stm.

[3] See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1. *Bohn/Coroama/Langheinrich/Mattern/Rohs,* "Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications", Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf. A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[4] Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: http://www2007.org/workshops/paper_106.pdf.

[5] WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services (such as access to the Internet) over long distances. For more information, see: The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

[6] Under the "One Laptop per Child" initiative, inexpensive laptop computers should be distributed to children, especially those in developing countries. The project is organized by the United States-based non-profit organization OLPC. For more information, see the official OLPC website at www.laptop.org. Regarding the technology of the laptop, see Heise News, Test of the 100 dollar laptop, 09.05.2007, available at: www.heise.de/english/newsticker/news/89512.

[7] Current reports highlight that around 11 per cent of the African population has access to the Internet. See www.internetworldstats.com/stats1.htm.

[8] Regarding the impact of ICT on society, see the report Sharpening Europe's Future Through ICT – Report from the information society technologies advisory group, 2006, available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf.

[9] Regarding the related risks of attacks against e-mail systems, see the report that United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[10] Regarding the ability to block Internet-based information services by denial-of-service attacks, see below: § 2.5.5.

[11] Regarding the related difficulties of lawful interception of Voice over IP communication, see: *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf..

[12] Related to risks and challenges see for example: *Choudhari/Banwet/Gupta*, Identifying Risk Factors in for E-governance Projects, published in Wgarwal/Ramana, Foundations of E-government, 2007, page 270 et. seq; *Ndou*, E-Government for Developing Countries, Opportunities and Challenges, DJISDC 2004, 18, page 1 et seq.

[13] See for example: *Molla*, The Impact of eReadingness on eCommerce Success in Developing Countries, 2004.

[14] See for example: *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 et seq.

[15] See for example: *Aggarwal,* Role of e-Learning in A Developing Country Like India, Proceedings of the 3rd National Conference, INDIA, Com 2009.

[16] *ITU*, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February 2009, 2009, available at: www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%20&%20Cybersecurity.pdf.

[17] Regarding the possibilities of low-cost access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in developing countries, available at: http://www2007.org/workshops/paper_106.pdf.

[18] Regarding the number of users of free-or-charge e-mail services, see: *Graham*, Email carriers deliver gifts of ninety features to lure, keep users, USA Today, 16.04.2008, available at: www.usatoday.com/tech/products/2008-04-15-google-gmail-webmail_N.htm. The article mentions that the four biggest webmail providers have several hundred million users – Microsoft (256 million), Yahoo (254 million), Google (91 million) and AOL (48 million). For an overview on e-mail statistics, see: *Brownlow*, e-mail and web statistics, April 2008, available at: www.email-marketing-reports.com/metrics/email-statistics.htm.

[19] www.wikipedia.org

[20] Regarding the use of free-of-charge services in criminal activities, see for example: Symantec Press Release, Symantec Reports Malicious Web Attacks Are on the Rise, 13.05.2008, available at: www.symantec.com/business/resources/articles/article.jsp?aid=20080513_symantec_reports_malicious_web_attacks_are_on_the_rise.

[21] Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[22] See for example: Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Challenges for the European Information Society beyond 2005, page 3, available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf.

[23] Regarding the impact of ICT on the development of the society, see: *Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Yang*, Between Democracy and Development: The impact of new information technologies on civil societies in China, available at: http://programs.ssrc.org/itic/publications/civsocandgov/yangpolicyrevised.pdf; *White*, Citizen Electronic: Marx and Gilder on Information Technology and Democracy, Journal of Information Technology impact, 1999, Vol. 1, page 20, available at: www.jiti.com/v1n1/white.pdf.

[24] Regarding the extent of integration of ICTs into the daily lives and the related threats, see: § 3.2.1 below, as well as *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[25] See UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211, page 1; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, page 212; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[26] See *Suter*, A Generic National Framework For Critical Information Infrastructure Protection, 2007, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

[27] *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[28] See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, page 1; *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf.

[29] Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf. Regarding the attacks against major online companies in the United States in 2000, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

[30] The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 219 million incidents were reported in one month (November 2010). Source: www.hackerwatch.org. Regarding the necessary differentiation between port scans and possible attempts to break into a computer system, see:

Panjwani/Tan/Jarrin/Cukier, An Experimental Evaluation to Determine if Port Scans are Precursors to an Attacks, available at: www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf.

[31] See *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[32] CRS Report for Congress on the Economic Impact of Cyber-Attacks, April 2004, page 10, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[33] See: *O'Connell*, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882.

[34] Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014.

[35] IBM survey, published 14.05.2006, available at: www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

[36] *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf. For more information on the economic impact of cybercrime, see below: § 2.4.

[37] Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[38] Cyber Security Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

[39] *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

[40] UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[41] The term "Cybersecurity" is used to summarize various activities and ITU-T Recommendation X.1205 "Overview of cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberenvironment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: *ITU*, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

[42] With regard to development related to developing countries, see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[43] See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cybersecurity, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[44] For more information, references and links, see: the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009), 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[45] For more information, see: *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1

[46] See: *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, available at: www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf; see also: Pillar One of the ITU Global Cybersecurity Agenda, available at:

www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html. With regard to the elements of an anti-cybercrime strategy, see below: §4.

47 See in this context: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

48 For more information on the World Summit on the Information Society (WSIS), see: www.itu.int/wsis/

49 The WSIS Tunis Agenda for the Information Society, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

50 The WSIS Geneva Plan of Action, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0

51 For more information on WSIS Action Line C5: Building confidence and security in the use of ICTs, see: www.itu.int/wsis/c5/

52 For more information on the Global Cybersecurity Agenda (GCA), see: www.itu.int/cybersecurity/gca/

53 For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

54 For an overview of the most important instruments in the fight against cybercrime, see below: § 6.5.

55 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

56 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 *et seq.*

57 For an overview of cybercrime-related legislation and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html..

58 See below: § 6.2.

59 See below: § 6.5.

60 For an overview of the most relevant challenges in the fight against cybercrime, see below: § 3.2.

61 One possibility to mask the identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Design, 2005.

62 Regarding legal responses to the challenges of anonymous communication, see below: § 6.5.12 and § 6.5.13.

63 Regarding the transnational dimension of cybercrime, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

64 Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management, 2005.

65 Regarding the need for international cooperation in the fight against cybercrime, see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

66 See below: § 6.5.

67 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141.

68 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international

conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf; *Plachta*, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 *et seq.*, available at: www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

69 See below: § 5.5. See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

70 The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Council of Europe Convention on Cybercrime, but addressed in an additional protocol. See below: § 5.2.1.

71 With regard to the different national approaches towards the criminalization of child pornography, see for example: *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

72 Regarding network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

73 The most important communication protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks, 2002; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006.

74 Regarding technical standardization, see: OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: www.itu.int/dms_pub/itu-t/oth/06/15/T061500000A0015PDFE.pdf. Regarding the importance of single technical as well as single legal standards, see: *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

75 Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189), available at: www.conventions.coe.int.

76 Since parties participating in the negotiation could not agree on a common position on the criminalization of the dissemination of xenophobic material, provisions related to this topic were integrated into a First Protocol to the Council of Europe Convention on Cybercrime.

77 See: *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.,* available at: http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

78 This was discussed for example within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: www.juriscom.net/en/uni/doc/yahoo/poullet.htm; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

79 A possibility to circumvent geo-targeting strategies is the use of proxy servers that are located abroad..

80 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

81 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

82 See below:§ 4.

83 See, with regard to the costs of technical protection measures required to fight against spam: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at www.oecd.org/dataoecd/5/47/34935342.pdf.

84 Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

85 One example is spam. The term "spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: "ITU Survey on Anti-Spam Legislation Worldwide 2005", page 5, available at:

www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialized countries. See: OECD, Spam Issue in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[86] For more details about the elements of an anti-cybercrime strategy, see below:§ 4.

2. Le phénomène de la cybercriminalité

2.1 Définitions

Bibliography (selected):

Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et seq., *Chawki*, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Forst*, Cybercrime: Appellate Court Interpretations, 1999, page 1; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No.2, page 144; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at:

www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

La plupart des rapports, guides et publications sur la cybercriminalité commencent par une définition des termes[87] « délit assisté par ordinateur » et « cyberdélit »[88]. Différentes approches ont ainsi été adoptées ces dernières décennies pour élaborer une définition précise de ces deux termes[89]. Avant d'offrir un aperçu du débat et d'évaluer les différentes approches, il est utile de déterminer la relation existant entre le « cyberdélit » et le « délit assisté par ordinateur »[90]. Sans entrer dans les détails à ce stade, le terme « cyberdélit » est plus précis que le « crime informatique », en ce sens qu'il doit impliquer un réseau informatique. Le terme « délit assisté par ordinateur » désigne également les infractions qui n'impliquent aucune relation avec un réseau, mais affectent uniquement des systèmes informatiques autonomes.

Durant le 10e Congrès des Nations Unies pour la Prévention du crime et le traitement des délinquants, deux définitions ont été élaborées dans le cadre d'un atelier organisé autour du même thème[91]. Le terme « cyberdélit » au sens strict (délit informatique) désigne tout comportement illicite mené au moyen d'activités électroniques visant la sécurité de systèmes informatiques et des données qu'ils traitent. Au sens plus large, le cyberdélit (ou délit assisté par ordinateur) recouvre tout comportement illicite réalisé au moyen ou vis-à-vis d'un système informatique ou d'un réseau, y compris les délits tels que la détention illicite et l'offre ou la distribution d'informations par le biais d'un système ou d'un réseau informatique[92].

Selon une acceptation courante, un cyberdélit désigne toute activité mettant en jeu des ordinateurs ou des réseaux en tant qu'outil, cible ou lieu d'une infraction[93]. Cette définition assez large pose quelques problèmes. En effet, elle recouvre également les délits traditionnels tels que le meurtre, dans la mesure où l'auteur a utilisé un clavier pour frapper et tuer sa victime. Autre exemple de définition plus large, l'article 1.1 du projet de convention internationale visant à renforcer la protection contre la cybercriminalité et le terrorisme (le « Projet de Stanford »)[94]. Cet article souligne que le terme « cyberdélit » fait référence à des actes qui concernent des cybersystèmes[95].

Certaines définitions, tentant de prendre en compte les objectifs ou les intentions de l'auteur de l'infraction, donnent une définition plus précise du cyberdélit[96] telle que la suivante : « toute activité assistée par ordinateur qui est *illégale ou considérée comme illicite* par certaines parties et peut être menée *en utilisant les réseaux électroniques mondiaux* »[97]. Le risque existe que ces définitions plus précises, qui excluent les cas où du matériel est utilisé pour commettre des infractions courantes, ne recouvrent pas les infractions considérées comme des cyberdélits dans certains accords internationaux, notamment la loi type du

Commonwealth sur la criminalité informatique et liée à l'informatique ou la Convention sur la cybercriminalité du Conseil de l'Europe[98]. Le fait, par exemple, de créer un dispositif USB[99] contenant un logiciel malveillant destiné à détruire des données sur les ordinateurs auxquels le dispositif serait connecté est une infraction au titre de la définition énoncée à l'article 4 de la Convention sur la cybercriminalité[100]. Pourtant, l'action consistant à détruire des données via un dispositif matériel conçu pour copier un programme malveillant, étant donné qu'elle n'est pas réalisée en utilisant les réseaux électroniques mondiaux, ne pourrait être qualifiée de cyberdélit au sens de la définition étroite mentionnée ci-dessus. Seule une définition reposant sur une description plus large, qui engloberait des actes tels que l'atteinte illégale à l'intégrité des données, permettrait de qualifier une telle action de cyberdélit.

Il ressort de ce qui précède qu'il est extrêmement difficile de définir les termes « délit assisté par ordinateur » et « cyberdélit »[101]. Ce dernier est en effet utilisé pour décrire des délits très variés, des infractions informatiques traditionnelles, aux infractions contre les réseaux. Etant donné les nombreuses différences que présentent ces infractions, il est difficile de ne retenir qu'un critère, susceptible d'englober tous les actes, tout en excluant les infractions traditionnelles uniquement commises au moyen de dispositifs matériels. Cette absence de définition unique du « cyberdélit » ne porte cependant pas à conséquence dès lors que ce vocable n'est pas utilisé comme un terme juridique[102]. Les chapitres suivants reposent sur une approche typologique, plutôt que de faire référence à une définition spécifique.

2.2 Typologie du cyberdélit

Bibliography: Big Data for Development: Challenges & Opportunities, UN Global Pulse, 2012; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf; *Hartmann/Steup,* The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment, published in Podins/Stinissen/Maybaum, 5th International Conference on Cyber Conflicts, 2013; *Kim/Wampler/Goppert/Hwang/Aldridge,* Cyber attack vulnerabilities analysis for unmanned aerial vehicles, American Institute of Aeronautics and Astronautics, 2012; *Sircar*, Big Data: Countering Tomorrow's Challenges, Infosys Labs Briefings, Vol. 11, No. 1, 2013; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004.

Le terme « cyberdélit » étant utilisé pour décrire une grande variété d'infractions[103], il est difficile d'élaborer une typologie ou un système de classification pour ce type de délit[104]. A noter cependant, une tentative intéressante: le système proposé par la Convention du Conseil de l'Europe sur la cybercriminalité[105], qui distingue quatre types d'infractions[106]:

1. les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques; [107]
2. les infractions informatiques;[108]
3. les infractions se rapportant au contenu;[109] et
4. les infractions liées aux atteintes à la propriété intellectuelle.[110]

Cette typologie n'est pas totalement cohérente, car elle ne repose pas sur un critère unique, qui permettrait de différentier les catégories. Trois catégories visent ainsi l'objet de la protection juridique (« infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques » [111]; infractions se rapportant au contenu[112]; et infractions liées aux atteintes à la propriété intellectuelle[113]), alors que la quatrième (« infractions informatiques[114] ») vise la méthode. Du fait de cette incohérence, les catégories se chevauchent.

De plus, certains termes (« cyberterrorisme »[115] ou « hameçonnage »[116]) recouvrent des infractions qui correspondent à plusieurs catégories. Cette classification reste toutefois une bonne base de travail pour étudier le phénomène de la cybercriminalité.

2.3 Évolution des délits assistés par ordinateur et des cyberdélits

Depuis les toutes premières années, l'utilisation abusive des technologies de l'information et les réponses juridiques nécessaires font l'objet de débats. Diverses solutions ont été mises en œuvre au niveau national et régional ces cinquante dernières années, mais, étant donné les progrès technologiques constants et l'évolution des modalités de commission des infractions, cet aspect demeure problématique.

2.3.1 Les années 60

Dans les années 60, l'introduction des systèmes informatiques à transistors, plus compacts et moins coûteux que les machines basées sur les tubes à vide, entraîne une augmentation de l'utilisation de la technologie informatique[117]. Dès les premières années, les infractions visent principalement à détériorer physiquement les systèmes informatiques et les données stockées[118]. De tels incidents sont notamment signalés au Canada, où, en 1969, une manifestation d'étudiants provoque un incendie entraînant la destruction des données informatiques hébergées au sein de l'université[119]. Au milieu des années 60, les Etats-Unis entament des discussions portant sur la création d'une autorité centrale chargée du stockage des données pour l'ensemble des ministères[120]. C'est dans ce contexte que l'utilisation abusive des bases de données[121] et les risques qu'elle présente en termes de respect de la vie privée[122] sont abordés[123].

2.3.2 Les années 70

Dans les années 70, l'utilisation des systèmes et des données informatiques prend de l'ampleur[124]. A la fin de la décennie, le nombre d'ordinateurs centraux utilisés aux Etats-Unis est estimé à 100 000[125]. Avec la baisse des coûts, la technologie informatique est plus largement adoptée au sein de l'administration et des entreprises, tout comme dans les foyers privés. Cette période se caractérise par une évolution des traditionnelles atteintes à la propriété lancées contre les systèmes informatiques[126], qui dominaient dans les années 60, vers de nouvelles formes d'infractions[127]. Tandis que les détériorations matérielles constituent toujours une forme d'infraction conséquente contre les systèmes informatiques[128], de nouvelles formes de délits assistés par ordinateurs voient le jour, dont notamment l'utilisation illicite des systèmes informatiques[129] et la manipulation[130] des données électroniques[131]. Le passage des transactions manuelles aux transactions informatiques engendre une nouvelle forme d'infraction: la fraude assistée par ordinateur[132]. A l'époque, les pertes imputables à des actes frauduleux assistés par ordinateur sont déjà estimées à plusieurs millions de dollars[133]. Ce nouveau type d'infraction constitue un réel problème et les services de répression doivent enquêter sur un nombre d'affaires grandissant[134]. L'application de la législation existante aux cas de délits assistés par ordinateur s'avère difficile[135] et un débat relatif aux solutions juridiques envisageables voit le jour dans diverses parties du monde[136]. Les Etats-Unis élaborent un projet de loi spécifiquement conçu pour répondre à la cybercriminalité[137], tandis qu'Interpol se penche sur le phénomène et sur les différentes réponses juridiques envisageables[138].

2.3.3 Les années 80

Les années 80 voient les ordinateurs personnels gagner en popularité et le nombre de systèmes informatiques (et, par conséquent, celui des cibles potentielles d'infractions) augmenter. Pour la première fois, de nombreuses infrastructures essentielles sont visées[139]. Parmi les principaux effets indésirables de l'évolution des systèmes informatiques, il convient de citer l'augmentation de l'intérêt porté aux logiciels, qui engendre les premières formes de piratage et d'infractions liées à la propriété intellectuelle[140]. L'interconnexion des systèmes informatiques donne également naissance à de nouveaux types d'infractions[141]. En effet, les réseaux permettent désormais aux délinquants de pénétrer à l'intérieur d'un système informatique sans être présents sur la scène du crime[142]. Par ailleurs, en distribuant des logiciels par le biais des réseaux, les délinquants sont en mesure de diffuser des programmes malveillants et de plus en plus de virus informatiques sont découverts[143]. Les différents Etats commencent à mettre à jour leur législation afin de suivre le rythme de l'évolution des infractions[144]. Les organisations internationales s'impliquent aussi dans ce processus. En effet, l'OCDE[145] et le Conseil de l'Europe[146] mettent en place des groupes de travail pour analyser le phénomène et évaluer les réponses juridiques envisageables.

2.3.4 Les années 90

L'arrivée de l'interface graphique (« WWW ») dans les années 90 entraîne une croissance rapide du nombre d'internautes et donne naissance à de nouveaux défis. Des informations légalement disponibles dans un pays sont accessibles partout dans le monde, même dans les pays dans lesquels leur publication est interdite[147]. La rapidité de l'échange d'informations ne fait qu'accroître la complexité des enquêtes relatives aux infractions transnationales liées aux services en ligne[148]. Enfin, la diffusion de contenu pornographique mettant en scène des enfants, qui se limitait auparavant à l'échange de livres et de cassettes, se développe sur les sites Web et au travers de services en ligne[149]. Les délits assistés par ordinateur, jusqu'alors commis à l'échelle locale, profitent d'Internet pour acquérir une dimension transnationale. La communauté internationale se penche alors sur la question avec davantage d'intérêt. La résolution de l'Assemblée générale des Nations unies 45/121 adoptée en 1990[150] et le guide pour la prévention et le contrôle des délits assistés par ordinateur publié en 1994 ne sont que deux exemples de cette nouvelle attention[151].

2.3.5 Le 21ème siècle

Tout comme les décennies précédentes, le 21ème siècle voit naître de nouvelles tendances en matière de délit assisté par ordinateur et de cyberdélit. La première décennie du nouveau millénaire se caractérise par l'utilisation de nouvelles méthodes hautement sophistiquées pour commettre des infractions, parmi lesquelles le « hameçonnage »[152] et les « attaques par botnet »[153], et par l'émergence d'une technologie plus complexe, à l'origine de nombreux défis pour les services de répression chargés de prendre en charge et d'enquêter sur les infractions commises, par exemple, au travers des communications par « voix sur IP » (VoIP) »[154] et de « l'informatique en nuage »[155]. L'impact des infractions évolue tout autant. La possibilité pour les délinquants d'automatiser leurs attaques se traduit par une augmentation du nombre d'infractions commises. Les Etats et les organisations régionales et internationales tentent de relever ces défis de plus en plus conséquents et proposent des solutions à la hauteur du fort degré de priorité accordé à la cybercriminalité. Les nouveautés comme les "big data[156]", les "drones[157]" et les "wearables" (technologies à porter sur soi) constituent des domaines qui attireront probablement encore plus l'attention des délinquants à l'avenir.

2.4 Ampleur et impact des cyberdélits

Bibliography (selected): Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Hyde-Bales/Morris/Charlton, The police recording of computer crime, UK Home Office Development and Practice Report, 2004; Maguire in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 et seq., available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf; Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Osborne/Wernicke, Introduction to Crime Analysis, 2003, page 1 et seq. available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

Les universitaires et les législateurs peuvent utiliser les statistiques relatives aux infractions en tant que base de discussion et dans le cadre du processus de prise de décision qui en découle[158]. Un accès à des informations précises concernant l'ampleur réelle de la cybercriminalité pourrait par ailleurs permettre aux services de répression d'améliorer leurs stratégies de lutte contre les cyberdélits, d'empêcher des attaques potentielles et d'appliquer une législation plus appropriée et plus efficace. Il est cependant difficile de quantifier l'impact de la cybercriminalité sur la société en se basant sur le nombre d'infractions commises au cours d'une période donnée[159]. Il est généralement possible d'obtenir ces informations à partir de statistiques et de sondages réalisés à ce sujet[160], mais de telles sources sont assorties d'un certain nombre de difficultés lorsqu'il s'agit de les utiliser pour formuler des recommandations politiques.

2.4.1 Statistiques relatives aux infractions

Les chiffres ci-dessous sont issus de statistiques relatives aux infractions réalisées au niveau national. Comme expliqué plus en détail ci-après, elles ne visent pas à illustrer l'évolution globale de la cybercriminalité ou l'ampleur réelle des cyberdélits au plan national et sont, par conséquent, exclusivement présentées pour offrir un aperçu des informations disponibles dans chaque Etat concerné.

- Pour 2013, l'Internet Complaint Center des Etats-Unis (centre des réclamations relatives aux crimes informatiques) fait état d'une augmentation de 48,8% des pertes signalées par rapport aux chiffres de 2012.[161]
- Selon les statistiques réalisées en Allemagne sur la criminalité, le nombre total d'infractions liées à Internet a augmenté de 12,2% en 2013 par rapport à 2012.[162]

Le caractère représentatif des statistiques est incertain, tout comme le fait qu'elles puissent fournir des informations fiables sur l'ampleur des délits[163]. Certains problèmes se posent lorsqu'il s'agit d'évaluer la menace globale que représente la cybercriminalité sur la base de statistiques relatives aux infractions[164].

En effet, les statistiques relatives aux infractions sont généralement élaborées au plan national et ne reflètent pas l'ampleur internationale du problème. Bien qu'il soit en principe possible de combiner les données disponibles, une telle approche ne peut fournir des informations fiables en raison des disparités réglementaires et des différentes méthodes employées pour comptabiliser les infractions [165]. La combinaison et la comparaison des statistiques relatives aux infractions élaborées au plan national impliquent un certain degré de compatibilité[166], lequel fait défaut lorsqu'il s'agit de cybercriminalité. Même si les données relatives à la cybercriminalité sont enregistrées, elles ne sont pas nécessairement répertoriées en tant que chiffre distinct [167]. En outre, les statistiques répertorient exclusivement les infractions détectées et signalées[168]. En ce qui concerne notamment la cybercriminalité, il est fort probable que le nombre de cas non signalés soit conséquent[169]. Les entreprises peuvent craindre qu'une mauvaise publicité nuise à leur réputation[170]. En annonçant que des pirates ont accédé à ses serveurs, une entreprise risque en effet de perdre la confiance de ses clients, tandis que les coûts et les conséquences peuvent s'avérer plus importants que les pertes causées par l'attaque elle-même. D'autre part, si les auteurs ne sont pas identifiés et poursuivis, ils sont susceptibles de récidiver. Les victimes peuvent douter du fait que les services de répression soient en mesure d'identifier les auteurs des infractions[171]. Si l'on compare le nombre important de cyberdélits au nombre limité d'enquêtes ayant porté leurs fruits, il est probable que les victimes sous-estiment l'importance de leur signalement [172]. Etant donné que les techniques d'automatisation permettent aux délinquants de faire d'importants profits en lançant de nombreuses attaques qui visent des montants minimes (c'est le cas notamment de la fraude aux avances sur commission[173]), il est fort probable que l'impact potentiel des infractions non signalées soit important. Les victimes d'infractions concernant de faibles montants préfèreront sans doute s'épargner une procédure de signalement chronophage. Les cas signalés impliquent généralement des sommes d'argent très conséquentes[174].

En résumé, les informations statistiques sont utiles pour favoriser la prise de conscience quant à l'importance persistante et grandissante du problème, tout comme elles sont nécessaires pour souligner le fait que l'un des principaux défis liés à la cybercriminalité reste l'absence d'informations fiables concernant l'ampleur du problème, les arrestations, les poursuites en justice et les condamnations. Comme expliqué précédemment, les statistiques relatives aux infractions ne répertorient généralement pas les délits distinctement, tandis que les données disponibles en ce qui concerne l'impact de la cybercriminalité ne peuvent généralement pas fournir aux législateurs des informations suffisamment fiables et précises quant au niveau ou à l'ampleur des infractions[175]. En l'absence de telles informations, il s'avère difficile de quantifier l'effet de la cybercriminalité sur la société et d'élaborer des stratégies visant à résoudre le problème[176]. Cela étant, les statistiques peuvent offrir une base de travail pour déterminer des tendances, lesquelles peuvent être mises au jour en examinant les résultats portant sur plusieurs années, puis servir de guide dans le cadre du processus de signalement des cyberdélits[177].

2.4.2 Les enquêtes

Les chiffres ci-dessous ont été extraits de différentes enquêtes. Comme expliqué plus en détail ci-après, ils ne sont pas nécessairement représentatifs et, par conséquent, sont exclusivement présentés pour offrir un aperçu des conclusions de ces enquêtes.

- Les informations relatives aux cartes de crédit et aux comptes bancaires sont parmi les informations les plus populaires proposées dans le cadre de services de l'économie souterraine. Les prix vont de 0,85 USD-30 USD (informations relatives à une seule carte de crédit) à 15 USD-850 USD (informations relatives à un seul compte bancaire).[178]
- En 2007, la fraude aux enchères était l'une des plus grandes arnaques Internet aux Etats-Unis, avec une perte moyenne de plus de 1 000 USD par infraction.[179]
- En 2005, les pertes résultant de délits liés à l'identité commis aux Etats-Unis totalisaient 56,6 milliards USD.[180]
- Les conséquences financières et personnelles de la cybercriminalité varient considérablement d'un incident à l'autre en Irlande et impliquent au total des coûts de plus de 250 000 EUR.[181]
- Une société de sécurité informatique a créé plus de 450 000 nouvelles signatures de codes malveillants en un seul trimestre.[182]
- Un quart des entreprises ayant répondu à un questionnaire en 2010 signale des pertes opérationnelles imputables à la cybercriminalité.[183]
- Le nombre d'attaques par refus de service et virus informatiques signalées par les professionnels de la sécurité entre 2004 et 2008 a baissé.[184]
- En 2009, les Etats-Unis, la Chine, le Brésil, l'Allemagne et l'Inde figuraient parmi les pays signalant le plus grand nombre d'activités malveillantes.[185]
- En 2014, on estimait que les pertes annuelles mondiales imputables à la cybercriminalité étaient comprises entre 375 et 575 milliards USD.[186]
- Avec une perte estimée à l'équivalent de 1,6% de son PIB total, l'Allemagne est le pays le plus touché par la cybercriminalité.[187] Les pertes sont estimées à 0,64% du PIB aux Etats-Unis, à 0,32% du PIB au Brésil et à 0,01% du PIB au Kenya.[188]
- Le coût moyen des vols de données est de 136 USD par habitant.[189] Suite à une attaque unique visant une base de données de clients, l'entreprise Sony a dû faire face à des coûts directs de près de 170 000 000 USD. [190]

Plusieurs problèmes se posent quant à l'utilisation de ces enquêtes pour déterminer l'ampleur et l'effet de la cybercriminalité sur la société.

Il est extrêmement difficile d'estimer avec précision les pertes financières. Selon certaines sources, les pertes enregistrées par les entreprises et les institutions aux Etats-Unis[191] du fait de la cybercriminalité pourraient atteindre 67 milliards USD en une seule année. Il est cependant difficile de savoir si l'extrapolation des résultats des sondages donne des chiffres fiables[192]. Cette critique méthodologique s'applique aux pertes ainsi qu'au nombre d'infractions reconnues.

Parmi les autres difficultés liées aux informations statistiques, notons que, la plupart du temps, des informations peu fiables ou non vérifiables sont citées de manière répétitive. C'est notamment le cas des informations statistiques concernant les aspects commerciaux de la pornographie en ligne mettant en scène des enfants. Selon plusieurs analyses, TopTenReviews estime que la pornographie sur Internet mettant en scène des enfants génère chaque année 2,5 milliards USD à travers le monde[193]. Pourtant, TenReviews ne fournit aucune information historique quant à la méthode employée pour réaliser cette étude. Compte tenu des déclarations de la société sur son site Internet: « *nous offrons les informations dont vous avez besoin pour faire un achat judicieux. Nous formulons une recommandation pour le meilleur produit de chaque catégorie. Grâce à nos graphiques comparatifs parallèles, aux nouvelles, aux articles et aux vidéos, nous simplifions le processus d'achat pour nos clients* », l'on est en droit de remettre en question

l'utilisation de telles données. Un autre exemple de chiffres cités sans référence vérifiable a été mis au jour en 2006 par le Wall Street Journal [194]. Après avoir enquêté sur une affirmation selon laquelle la pédopornographie représentait un marché de plusieurs milliards de dollars (20 milliards USD chaque année), un journaliste a déclaré que deux des principaux documents faisant état de profits allant de 3 milliards USD à 20 milliards USD – une publication du NCMEC et une du Conseil de l'Europe – faisaient référence à des institutions n'ayant pas confirmé ces chiffres.

Les enquêtes se limitent généralement à répertorier les incidents, sans fournir de plus amples informations ou détails. Il est donc très difficile d'en tirer des conclusions en matière de tendances. On peut citer, à titre d'exemple, l'étude *Computer Crime and Security Survey 2007*, réalisée par l'institut américain CSI[195], qui analyse, entre autres tendances, le nombre d'infractions informatiques[196]. Cette étude repose sur les réponses fournies par 494 professionnels de la sécurité informatique travaillant dans des entreprises, des organismes publics et des établissements financiers aux Etats-Unis[197]. L'étude fournit des informations sur le nombre d'infractions signalées entre 2000 et 2007 par les organismes interrogés. Elle montre que, depuis 2001, la proportion des organismes ayant subi ou noté des attaques par virus ou des accès non autorisés à des données (ou une introduction dans des systèmes par des personnes externes) a diminué, sans toutefois en donner la raison.

Les statistiques sur la cybercriminalité ne peuvent pas fournir d'informations fiables sur le niveau ou l'ampleur des infractions [198]. L'incertitude concernant la proportion de victimes ayant signalé des infractions[199] ainsi que l'absence d'explications concernant la réduction du nombre de cyberdélits rendent ces statistiques sujettes à interprétation. En conséquence, les données actuellement disponibles sont insuffisantes pour prévoir les tendances et les évolutions futures.

2.5 Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Bibliography (selected): Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; Hackworth, Spyware, Cybercrime & Security, IIA-4; Kabay, A Brief History of Computer Crime: An Introduction for Students, 2008; Ollmann, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; Paxson, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; Sieber, Council of Europe Organised Crime Report 2004; Szor, The Art of Computer Virus Research and Defence, 2005; Urbas/Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.250; Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 et seq.

Toutes les infractions classées dans cette catégorie portent atteinte à (au moins) l'un des trois principes juridiques que sont la confidentialité, l'intégrité et la disponibilité. Les systèmes et les données informatiques sont apparus il y a environ soixante ans[200]. Contrairement aux délits traditionnels (vols, meurtres, etc.), qui entrent dans le champ d'application du droit pénal depuis des siècles, les infractions informatiques sont donc relativement récentes. Pour pouvoir engager des poursuites contre les auteurs de ces actes, il est nécessaire que le droit pénal en vigueur contienne des dispositions visant à protéger les objets tangibles et les documents matériels contre la manipulation, mais aussi que ces dispositions englobent les nouveaux principes juridiques susmentionnés[201]. Cette section fournit une vue d'ensemble des infractions les plus courantes classées dans cette catégorie.

2.5.1 Accès illégal (piratage, craquage)[202]

Le « piratage » (*hacking*) désigne l'accès illégal à un ordinateur[203]. C'est l'une des infractions informatiques les plus anciennes[204]. Avec le développement des réseaux informatiques (notamment d'Internet), cette infraction est devenue un phénomène de masse[205]. Certaines organisations bien connues ont été victimes de piratage, par exemple la NASA (*United States National Aeronautics and Space Administration*), l'armée de l'air des Etats-Unis, le Pentagone, Yahoo!, Google, Ebay et l'administration allemande[206].

Parmi les exemples illustrant quelques infractions entrant dans la catégorie du piratage, on peut citer le craquage d'un mot de passe ou de sites Internet protégés par mot de passe[207] et le contournement d'une protection par mot de passe sur un ordinateur. On peut également citer quelques exemples d'actes préparatoires relevant du « piratage », tels que l'exploitation d'une faille logicielle ou matérielle pour obtenir illégalement un mot de passe permettant d'entrer dans un système informatique[208], la création de sites Internet d'espionnage (*spoofing*) conçus pour amener les utilisateurs à révéler leur mot de passe[209] et l'installation de matériels ou de logiciels d'enregistrement de frappe (par exemple, « enregistreurs de frappe » ou *keyloggers*), qui enregistrent toutes les frappes au clavier et, par conséquent, tous les mots de passe saisis sur l'ordinateur et/ou le dispositif[210].

Tous les auteurs d'infraction n'ont pas les mêmes motivations. Certains contournent des mesures de sécurité dans l'unique but de montrer ce dont ils sont capables[211]. D'autres ont des motivations politiques (c'est ce que l'on appelle « l'activisme » ou piratage militant[212]), à l'exemple des pirates qui ont récemment attaqué le site Internet principal des Nations Unies[213]. Dans la plupart des cas, l'auteur de l'infraction n'est pas seulement motivé par un accès illicite au système informatique, mais par l'exploitation de cet accès dans le but de commettre d'autres types d'infraction: espionnage ou manipulation de données, attaques par refus de service (DoS)[214]. Ainsi, en règle générale, l'accès illicite au système n'est-il qu'une indispensable première étape[215].

De nombreux analystes le reconnaissent, les tentatives d'accès illicite aux systèmes informatiques sont en augmentation, avec plus de 250 millions d'incidents enregistrés dans le monde pendant le seul mois d'août 2007[216]. Trois facteurs principaux expliquent ce phénomène: la protection inadaptée et insuffisante des systèmes informatiques ; le développement d'outils logiciels d'automatisation des attaques ; et le rôle grandissant des ordinateurs privés dans les stratégies de piratage.

La protection inadaptée et insuffisante des systèmes informatiques

Sur les centaines de millions d'ordinateurs connectés à Internet, nombreux sont ceux qui ne disposent pas d'une protection adaptée contre les accès illicites[217]. Or, des analyses menées par l'Université du Maryland semblent indiquer qu'un système informatique non protégé risque de subir une attaque dans la minute qui suit sa connexion à Internet[218]. On notera cependant que les dispositifs de protection, s'ils peuvent réduire les risques, ne sont pas infaillibles. En témoignent certaines attaques réussies contre des systèmes informatiques pourtant bien protégés[219].

Le développement d'outils logiciels d'automatisation des attaques

Depuis peu, des outils logiciels sont utilisés pour automatiser les attaques[220]. Un même pirate peut, à l'aide de certains logiciels et grâce à des attaques dites « de préinstallation », attaquer des milliers de systèmes informatiques dans une même journée à partir d'un seul ordinateur[221]. Si, en plus, il a accès à d'autres ordinateurs – via un botnet[222] –, il peut encore augmenter la portée de son attaque. Etant donné que ces outils logiciels mettent en œuvre des méthodes prédéfinies, toutes les attaques ne sont pas couronnées de succès. Ainsi, les utilisateurs qui mettent régulièrement à jour leur système d'exploitation et leurs applications logicielles diminuent-ils le risque d'être victimes de ces attaques de grande ampleur, étant donné que les sociétés spécialisées dans le développement d'antivirus analysent les programmes de piratage et se préparent ainsi à contrer les attaques standard.

Les attaques massives reposent souvent sur des attaques élémentaires de conception individualisée. La plupart du temps, leur succès ne tient pas à l'utilisation de méthodes extrêmement sophistiquées, mais au nombre de systèmes informatiques pris pour cibles. Il est très facile de se procurer sur Internet les outils permettant de réaliser ces attaques standard[223], si certains sont gratuits, les plus efficaces se vendent

couramment quelques milliers de dollars[224]. On peut citer l'exemple des logiciels qui permettent de rechercher les ports non protégés de tous les ordinateurs correspondant à une plage d'adresses IP, préalablement définie par le pirate (par exemple de 111.2.0.0 à 111.9.253.253)[225].

Le rôle grandissant des ordinateurs privés dans les stratégies de piratage

En général, l'objectif premier d'une attaque n'est pas d'obtenir l'accès à un système informatique[226]. Les ordinateurs professionnels résistent mieux aux attaques utilisant des outils logiciels préconfigurés car ils sont généralement mieux protégés que les ordinateurs privés[227]. C'est donc sur ces derniers que les pirates concentrent de plus en plus leurs attaques depuis quelques années, d'autant plus qu'ils contiennent souvent des informations sensibles (numéros de carte de crédit, coordonnées bancaires, etc.). Par ailleurs, après une attaque réussie, les pirates peuvent intégrer l'ordinateur privé dans leur botnet et l'utiliser pour commettre des infractions ultérieures, raison supplémentaire pour privilégier ce type de cible[228].

L'accès illégal à un système informatique, que l'on peut comparer à l'accès illégal à un bâtiment, est considéré dans de nombreux pays comme une infraction pénale[229]. L'analyse des différentes façons d'envisager la pénalisation des accès aux systèmes informatiques montre que certaines légalisations confondent parfois l'accès illégal avec les infractions qui sont commises à la suite de cet accès, alors que d'autres ne pénalisent l'accès illégal qu'en cas de violation grave. Certaines dispositions sanctionnent l'accès initial, d'autres approches restreignent l'infraction pénale aux cas suivants: le système violé est protégé par des mesures de sécurité[230] ou l'auteur de l'infraction a l'intention de nuire[231] ou les données ont été collectées, modifiées ou corrompues. D'autres systèmes juridiques ne sanctionnent pas l'accès en tant que tel, mais s'attachent avant tout aux infractions qui sont commises ultérieurement[232].

D'après une analyse plus récente, la tendance est à la perpétration d'attaques plus sophistiquées et ciblées, en plus des importantes attaques à grande échelle qui ont prévalu ces dernières décennies.[233] Alors que les attaques à grande échelle suivent une approche opportuniste et sont plus faciles à mener, les attaques ciblées demandent au pirate plus d'efforts mais sont largement plus efficaces et portent davantage préjudice[234] à la victime.[235]

2.5.2 Acquisition illégale de données (espionnage de données)

Les systèmes informatiques contiennent souvent des données sensibles. Si le système est connecté à Internet, un pirate peut essayer de récupérer ces données par le réseau, et ce, où qu'il se trouve sur la planète (ou presque)[236]. Ainsi Internet est-il de plus en plus utilisé pour dérober des données commerciales confidentielles[237]. La valeur des données sensibles et la possibilité d'y accéder à distance font de l'espionnage de données une activité hautement rentable. Dans les années 80, plusieurs pirates allemands ont réussi à entrer dans les systèmes informatiques de l'administration et de l'armée des Etats-Unis, à dérober des données confidentielles et à les vendre à des agents d'autres pays[238].

Pour entrer dans les systèmes informatiques de leurs victimes, les pirates utilisent diverses techniques[239], notamment: l'utilisation de logiciels conçus pour rechercher les ports non protégés[240] ou pour contourner les mesures de protection[241], ou encore « l'ingénierie sociale »[242]. Cette dernière approche, en particulier, ne repose pas sur des moyens techniques et est, à ce titre, très intéressante. Elle désigne une méthode d'intrusion, non technique, qui repose largement sur le facteur humain et consiste souvent à amener d'autres personnes, en les trompant, à enfreindre les procédures normales de sécurité[243]. Dans le contexte de l'accès illégal, elle désigne aussi la manipulation des personnes dans le but d'accéder à des systèmes informatiques[244]. L'ingénierie sociale est généralement très efficace, car les utilisateurs sont souvent le maillon faible de la sécurité informatique. Le hameçonnage (*phishing*), par exemple, est récemment devenu une infraction majeure dans le cyberespace[245]. Il désigne la tentative de s'approprier frauduleusement des données sensibles (mots de passe par exemple) en se faisant passer pour une personne ou une entreprise digne de confiance (un établissement financier par exemple) dans une communication électronique d'apparence officielle.

Le facteur humain joue dans les deux sens. D'un côté, la vulnérabilité des personnes ouvre la voie aux escroqueries; de l'autre, les utilisateurs bien formés ne sont pas des victimes faciles. C'est pourquoi la formation des utilisateurs est un élément essentiel de toute stratégie de lutte contre la cybercriminalité[246].

Par ailleurs, des mesures techniques peuvent être mises en œuvre pour prévenir l'accès illégal. A cet égard, l'OCDE met en avant l'importance de la cryptographie au niveau de l'utilisateur comme moyen supplémentaire de protection des données[247]. Quiconque – personne ou organisation – souhaitant prendre des mesures adaptées pour protéger ses données trouvera dans la cryptographie une méthode plus efficace que toute autre protection matérielle[248]. Le succès des attaques visant à dérober des données sensibles s'explique souvent par l'absence de mesures de protection. Les systèmes informatiques contiennent de plus en plus souvent des données sensibles. Il est donc essentiel d'évaluer l'efficacité des mesures de protection technique prises par les utilisateurs ou de déterminer s'il y a lieu de mettre en place des protections juridiques supplémentaires pour sanctionner pénalement l'espionnage de données[249].

Si les pirates ciblent généralement les données confidentielles des entreprises, ils s'intéressent de plus en plus souvent aux données stockées sur les ordinateurs privés[250]. En effet, les particuliers stockent souvent leurs coordonnés bancaires et leurs numéros de carte de crédit sur leur ordinateur[251], informations que les pirates utilisent pour leur propre compte (utilisation des coordonnées bancaires pour effectuer des transferts de fonds par exemple) ou revendent à des tiers[252]. Les données relatives à des cartes de crédit peuvent ainsi se vendre jusqu'à 60 USD[253]. Le fait que les actes de piratage portent essentiellement sur des ordinateurs privés est très instructif. Si l'exploitation des données confidentielles d'une entreprise rapporte généralement plus que le vol ou la vente de données de cartes de crédit, il se trouve que l'espionnage des ordinateurs privés, du fait qu'ils sont en général moins bien protégés, a en réalité toutes les chances de rapporter davantage.

Pour collecter des données, deux approches sont envisageables: accéder à un système informatique ou à un dispositif de stockage et extraire les données, ou avoir recours à la manipulation de façon à amener des utilisateurs à dévoiler les données recherchées ou les codes qui permettront ensuite aux pirates d'accéder à ces données (« hameçonnage »).

Les pirates utilisent souvent des outils informatiques installés sur les ordinateurs de leurs victimes ou des logiciels malveillants appelés « logiciels espions » (*spyware*), qui sont chargés de leur transmettre les données recherchées[254]. Plusieurs types de logiciels espions ont été découverts ces dernières années, parmi lesquels les enregistreurs de frappe[255]. Il s'agit de programmes conçus pour enregistrer toutes les frappes effectuées sur le clavier d'un ordinateur infecté[256]. Certains envoient au pirate toutes les données enregistrées dès que l'ordinateur est connecté à Internet. D'autres effectuent un premier tri, analysent les données enregistrées (recherche d'informations évoquant des cartes de crédit par exemple[257]) et ne transmettent que les données pertinentes ainsi trouvées. Il existe aussi des dispositifs matériels fonctionnant sur le même principe. Ces dispositifs sont connectés entre le clavier et l'ordinateur afin d'enregistrer les frappes au clavier. Ce type d'enregistreur de frappe est plus difficile à installer et à détecter, car il requiert un accès physique à l'ordinateur[258]. En revanche, les logiciels anti-virus et anti-logiciels espions traditionnels sont, pour l'essentiel, incapables de les détecter[259].

Il n'est pas nécessaire d'avoir accès à un ordinateur pour dérober des données qui y sont stockées: il peut suffire de manipuler les personnes qui l'utilisent. Certains pirates ont récemment mis au point des méthodes d'escroquerie efficaces afin d'obtenir des informations confidentielles (coordonnées bancaires, données de cartes de crédit, etc.) en manipulant les utilisateurs par des techniques d'ingénierie sociale[260]. Le « hameçonnage » est récemment devenu une infraction majeure dans le cyberespace[261]. Il désigne un type d'infraction caractérisé par la tentative de s'approprier frauduleusement les données sensibles (mots de passe par exemple) en se faisant passer pour une personne ou une entreprise digne de confiance (un établissement financier par exemple) dans une communication électronique d'apparence officielle[262].

Les nouveautés telles que les "big data", qui correspondent à la collecte par les entreprises de grandes quantités de données en vue de la réalisation d'analyses sophistiquées, a fait évoluer la place occupée par les vols de données dans les menaces. Si les pirates accèdent à des bases de données volumineuses contenant des données personnelles de consommateurs, le simple vol des données peut coûter très cher à l'entreprise attaquée, même si les pirates n'utilisent pas les données pour commettre d'autres infractions.[263] Le coût moyen des vols de données est de 136 USD par habitant.[264] Suite à une attaque unique visant une base de données de clients, l'entreprise Sony a dû faire face à des coûts directs de près de 170 000 000 USD[265].

D'après des travaux de recherche publiés en 2014, les données disponibles sur les cybermarchés noirs, obtenues dans le cadre de vols de données, comprennent des justificatifs d'identité concernant jusqu'à 360 millions de comptes.[266]

2.5.3 Interception illégale

Pour obtenir des informations, les pirates peuvent également intercepter des communications [267] (messagerie électronique par exemple) ou des transferts de données (transfert vers un serveur ou accès à un support de stockage externe par le Web [268]). Les pirates sont susceptibles de viser tous les types d'infrastructures de communication (lignes fixes, communications hertziennes, etc.) et tous les types de services Internet (messagerie électronique, discussion en ligne, voix sur IP[269], etc.).

La plupart des transferts de données entre fournisseurs d'infrastructures Internet ou fournisseurs de services Internet sont bien protégés et difficiles à intercepter [270]. Les pirates cherchent cependant à identifier les points faibles du système. Les technologies hertziennes, de plus en plus populaires, ont montré, par le passé, leur vulnérabilité[271]. Aujourd'hui, les hôtels, les restaurants et les bars proposent à leurs clients des accès à Internet via des points d'accès hertziens. Or, les signaux utilisés pour l'échange de données entre un ordinateur et un point d'accès peuvent être captés dans un rayon maximal de 100 mètres[272]. Les pirates souhaitant intercepter un processus d'échange de données peuvent donc se placer n'importe où dans le cercle défini par ce rayon. Même lorsque les communications hertziennes sont chiffrées, ils parviennent parfois à décrypter les données interceptées[273].

Pour avoir accès à des données sensibles, certains pirates créent des points d'accès à proximité des lieux où il y a une forte demande d'accès hertzien[274] (près des bars, des hôtels, etc.). Le point d'accès pirate est souvent nommé de façon à inciter les utilisateurs qui recherchent un accès à Internet à choisir celui-ci plutôt qu'un autre. Les pirates peuvent ainsi aisément intercepter les communications des utilisateurs qui, comptant sur le fournisseur d'accès pour garantir la sécurité de leurs communications, n'ont pas mis en place leurs propres mesures de protection.

L'utilisation de lignes fixes n'empêche pas les pirates d'intercepter les communications [275]. En effet, la transmission de données sur une ligne crée un champ électromagnétique [276] que les pirates peuvent détecter et enregistrer à l'aide d'un équipement approprié[277]. De cette façon, ils peuvent enregistrer les données transférées entre des ordinateurs et le système informatique auxquels ils sont connectés, mais aussi les données transmises à l'intérieur d'un même système[278].

La plupart des pays ont décidé de protéger l'utilisation des services de télécommunication en sanctionnant pénalement l'interception illégale des conversations téléphoniques. Les services reposant sur IP étant de plus en plus prisés, le législateur devra peut-être examiner s'ils doivent bénéficier d'une protection analogue[279].

2.5.4 Atteinte à l'intégrité des données

Les utilisateurs privés, les entreprises et les administrations sont tributaires de l'intégrité et de la disponibilité des données informatiques qui représentent, pour eux, des informations vitales [280]. Tout problème d'accès aux données peut ainsi causer des dommages (financiers) considérables. Les pirates peuvent violer l'intégrité des données et interférer avec celles-ci en les supprimant, en les effaçant ou en les altérant[281]. Le virus informatique est un exemple de programme malveillant qui opère par effacement des données[282]. Depuis les débuts de l'informatique, les virus menacent les utilisateurs qui ne protègent pas suffisamment leur ordinateur [283]. Le nombre de virus informatiques a en outre considérablement augmenté[284]. La méthode de diffusion des virus et leur charge active (*payload*[285]) ont également évolué.

Les virus informatiques étaient autrefois diffusés par le biais de dispositifs de stockage (disquettes, etc.), alors qu'ils sont aujourd'hui, pour l'essentiel, diffusés via Internet à l'intérieur de courriels ou de fichiers téléchargés par les utilisateurs[286]. Du fait de leur efficacité, ces nouvelles méthodes de diffusion ont permis d'accélérer considérablement les infections par virus et d'accroître, dans de grandes proportions, le nombre de systèmes informatiques infectés. On estime par exemple que le ver informatique SQL Slammer[287] a infecté 90 % des ordinateurs vulnérables dans les dix premières minutes de sa diffusion[288]. Les pertes financières dues aux attaques par virus dans la seule année 2000 sont estimées à quelque 17 milliards USD[289]. En 2003, ces pertes s'élevaient encore à plus de 12 milliards USD[290].

La plupart des virus informatiques de première génération étaient conçus pour effacer des données ou afficher des messages. Leur charge utile s'est récemment diversifiée[291]. Ainsi, les virus modernes sont-ils capables d'installer des portes dérobées (*back-doors*), qui permettent aux pirates de prendre le contrôle de l'ordinateur à distance ou de chiffrer certains de ses fichiers et d'en interdire l'accès (la victime doit alors payer pour obtenir la clé de chiffrement)[292].

D'après les rapports publiés par les entreprises de sécurité, le nombre de virus informatiques et autres formes de logiciels malveillants est en constante augmentation, avec jusqu'à 30 millions de nouvelles chaînes de logiciels malveillants chaque année.[293] Kaspersky a indiqué avoir détecté en 2013 plus de 300 000 fichiers malveillants par jour.[294] Ces chiffres étant pour la plupart publiés par des entreprises de sécurité qui vendent des logiciels antivirus, il est sans aucun doute plus difficile de vérifier leur fiabilité. L'évolution montre que plusieurs décennies après la découverte du premier virus informatique, les logiciels malveillants continuent de représenter un problème de taille pour la sécurité sur Internet.

2.5.5 Atteinte à l'intégrité du système

Ce qui a été dit à propos des attaques visant les données informatiques s'applique également aux attaques visant les systèmes informatiques. De plus en plus d'entreprises intègrent des services Internet dans leur processus de production, bénéficiant ainsi d'une disponibilité sur vingt-quatre heures et d'une accessibilité dans le monde entier[295]. Les pirates qui parviennent à déstabiliser le fonctionnement des systèmes informatiques peuvent donc causer de très lourdes pertes[296].

Une façon de mener une attaque est de s'en prendre physiquement au système informatique[297], par destruction du matériel par exemple (sous réserve que les pirates soient en mesure d'accéder au système). Les cas de destruction de matériel à distance ne posent pas de problèmes majeurs à la plupart des systèmes juridiques, car ils sont assimilables à des cas classiques de dégradation ou de destruction de biens. Cela étant, pour les entreprises de commerce électronique florissantes, les pertes financières dues aux attaques menées contre les systèmes informatiques dépassent souvent très largement le seul coût du matériel[298].

Les escroqueries par Internet posent en revanche aux systèmes juridiques davantage de problèmes. Parmi les attaques à distance contre les systèmes informatiques, on peut citer les vers informatiques[299] et les attaques par refus de service (DoS)[300].

Comme les virus, les vers informatiques[301] sont un sous-ensemble des logiciels malveillants. Ils désignent des programmes informatiques auto reproducteurs, qui déstabilisent le réseau en lançant de multiples processus de transfert de données. Ils peuvent influer sur les systèmes informatiques en perturbant le bon fonctionnement de l'ordinateur, en utilisant les ressources système afin de s'autoreproduire sur Internet, ou en augmentant le trafic sur le réseau, ce qui peut rendre certains services (notamment des sites Internet) indisponibles.

Les effets des vers informatiques s'étendent généralement à l'ensemble du réseau, alors que les attaques DoS visent certains systèmes en particulier, rendant les ressources indisponibles aux utilisateurs[302]. En envoyant à un système informatique plus de requêtes qu'il ne peut en gérer, les pirates arrivent à empêcher les utilisateurs d'accéder au système, de relever leurs courriels, de lire les nouvelles, de réserver un billet d'avion ou de télécharger des fichiers. En 2000, en un court laps de temps, plusieurs attaques DoS ont été lancées contre des entreprises connues telles que CNN, eBay et Amazon[303]. Des attaques similaires ont été lancées en 2009 contre des sites du gouvernement et des sites commerciaux aux Etats-Unis et en Corée du Sud[304], rendant certains services indisponibles pendant plusieurs heures, voire plusieurs jours[305].

Etant donné que les attaques par ver informatique ou de type DoS ne comportent pas nécessairement d'atteintes au matériel, la poursuite de leurs auteurs pose à la plupart des systèmes juridiques de grandes difficultés. Outre la nécessité élémentaire de sanctionner pénalement les attaques par Internet[306], la question se pose de savoir si la prévention et la poursuite des attaques visant des infrastructures essentielles requièrent une approche législative distincte. Cette question est en cours d'examen.

En dépit de la mise au point d'outils techniques de prévention et de stratégies d'atténuation, les attaques par refus de service continuent de poser problème aux entreprises et aux institutions publiques. D'après certaines recherches, ces attaques constituent une menace grandissante et les coûts qu'elles engendrent ne cessent d'augmenter.[307]

2.6 Infractions se rapportant au contenu

Bibliography (selected): *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in Governing the Internet Freedom and Regulation in the OSCE Region; *Carr*, Child Abuse, Child Pornography and the Internet, 2004; *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144 *et seq.*; *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Healy*, Child Pornography: An International Perspective, 2004; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001; *Lanning*, Child Molesters: A Behavioral Analysis, 2001; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*; *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/.

Cette catégorie vise les contenus qui sont considérés comme illicites, notamment la pornographie mettant en scène des enfants, la xénophobie et les outrages concernant des symboles religieux[308]. L'élaboration d'instruments juridiques destinés à lutter contre cette catégorie d'infractions relève, pour l'essentiel, d'approches nationales, reposant éventuellement sur des principes culturels et juridiques fondamentaux. En matière de contenu illicite, les systèmes de valeurs et les systèmes juridiques diffèrent considérablement selon les sociétés. Ainsi, la diffusion de contenus xénophobes est illégale dans de nombreux pays européens[309], alors qu'elle peut relever de la liberté d'expression[310] aux Etats-Unis[311]. De même les remarques désobligeantes à l'égard du prophète Mahomet sont érigées en infraction pénale dans de nombreux pays arabes, mais pas dans certains pays européens[312].

Les approches juridiques adoptées pour sanctionner pénalement le contenu illicite ne doivent pas interférer avec la liberté d'expression. Ce droit est notamment défini par le principe 1 (b) des Principes de Johannesburg sur la sécurité nationale et la liberté d'expression[313]. Toutefois, le principe 1 (c) précise que la liberté d'expression peut faire l'objet de restrictions. Tandis que le fait de sanctionner pénalement le contenu illicite n'est par conséquent pas exclu en soi, il doit être strictement limité. Ces restrictions sont notamment abordées eu égard à l'application de sanctions pénales aux cas de diffamation[314]. La déclaration conjointe de 2008 du Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression et d'autres documents soulignent le fait que des notions vagues, telles que la fourniture de communications et la glorification ou la promotion du terrorisme ou de l'extrémisme ne devraient pas faire l'objet de sanctions pénales[315].

Ces problèmes juridiques sont complexes, car toute information, une fois mise en ligne par un internaute dans un pays donné, devient accessible de tout point du globe[316]. Or, si un « délinquant » crée du contenu jugé illicite dans certains pays, mais non dans le pays à partir duquel il opère, il est difficile, voire impossible, d'engager des poursuites à son encontre[317].

Quels contenus doivent être considérés comme illicites ? Dans quelle mesure certains actes doivent-ils être sanctionnés pénalement ? Ces questions ne font pas l'unanimité, loin s'en faut. Parce qu'ils ne partagent pas les points de vue d'autres pays ou qu'il leur est difficile de poursuivre des violations commises à l'extérieur de leur territoire, certains pays sont amenés à bloquer des types de contenu sur Internet. Les Etats qui sont parvenus à un accord pour empêcher l'accès aux sites à contenu illicite hébergés à l'extérieur de leur territoire parviennent à maintenir une législation stricte, à bloquer les sites et à filtrer les contenus[318].

Il existe plusieurs types de systèmes de filtrage. Les fournisseurs d'accès peuvent par exemple installer des programmes qui, après analyse, mettent certains sites visités sur liste noire[319]. Une autre solution consiste à installer un logiciel de filtrage sur l'ordinateur de l'utilisateur (solution qui convient bien au contrôle parental ainsi qu'au contrôle de contenu par les bibliothèques et les terminaux publics d'accès à Internet)[320].

Les tentatives de contrôle de contenu sur Internet ne concernent pas uniquement les contenus généralement reconnus comme illicites. Certains pays utilisent en effet les technologies de filtrage pour restreindre l'accès aux sites traitant de sujets politiques. Les rapports de l'OpenNet Initiative[321] signalent à cet égard qu'une vingtaine de pays environ pratiquent la censure[322].

2.6.1 Contenus érotiques ou pornographiques (à l'exclusion de la pédopornographie)

Les contenus à caractère sexuel ont été parmi les premiers contenus commercialisés sur Internet. Ce médium offre en effet aux distributeurs de contenu érotique et pornographique plusieurs avantages, notamment:

- échange de médias (images, films, retransmissions en direct, etc.) sans avoir à payer de frais de port élevés;[323]
- accès mondial[324] permettant d'atteindre un nombre de clients très supérieur à ce que peuvent réaliser des magasins de détail;
- Internet est souvent (à tort[325]) considéré comme un médium anonyme, caractéristique que les consommateurs de pornographie apprécient compte tenu des opinions sociales prédominantes.

De récentes études ont recensé pas moins de 4,2 millions de sites pornographiques potentiellement disponibles à tout moment sur Internet[326]. Outre les sites Internet, d'autres supports permettent de diffuser du contenu pornographique, par exemple les systèmes de partage de fichiers[327] et les salons privés de discussion en ligne.

Le degré de pénalisation des contenus érotiques et pornographiques diffère selon les pays. Certains, cherchant à protéger les mineurs[328], autorisent l'échange de contenu pornographique entre adultes et ne sanctionnent que les cas où des mineurs ont eu accès à ce type de contenu[329]. Selon certaines études, l'accès, par des enfants, à du contenu pornographique pourrait avoir sur leur développement des effets indésirables[330]. Pour se conformer aux diverses législations, les sites Internet ont mis en place des « systèmes de vérification de l'âge »[331]. D'autres pays sanctionnent pénalement tout échange de contenu pornographique, même entre adultes[332], sans viser spécifiquement certains groupes (les mineurs par exemple).

Les pays qui érigent en infraction pénale toute interaction avec du contenu pornographique rencontrent de réelles difficultés à prévenir l'accès à ce type de contenu. En dehors d'Internet, les autorités parviennent souvent à détecter les violations des dispositions visant à interdire le contenu pornographique et à poursuivre en justice leurs auteurs. Sur Internet en revanche, où ce type de contenu est souvent proposé par des serveurs hébergés à l'étranger, la répression est plus difficile. Même lorsqu'elles parviennent à identifier précisément les sites à caractère pornographique, les autorités n'ont pas toujours le pouvoir d'imposer le retrait de ce type de contenu qu'elles jugent offensant.

En vertu du principe de *souveraineté nationale,* un pays ne peut généralement pas mener d'enquêtes sur le territoire d'un autre pays sans la permission des autorités locales[333]. De plus, le principe de « double incrimination »[334] peut entraver l'instruction et la prise de sanctions pénales, quand bien même les

autorités cherchent à obtenir le soutien des pays où sont hébergés les sites Internet incriminés. Pour empêcher l'accès aux contenus pornographiques, les pays dotés d'une législation exceptionnellement stricte doivent donc souvent se contenter de mesures de prévention visant à limiter l'accès à certains sites (technologies de filtrage[335] par exemple)[336].

2.6.2 Pornographie mettant en scène des enfants (pédopornographie)

Internet est devenu un canal privilégié pour la distribution de pornographie mettant en scène des enfants. Dans les années 70 et 80, les délinquants impliqués dans l'échange de contenu pédopornographique font face à des menaces sérieuses[337]. Le marché de la pédopornographie se concentre alors principalement sur l'Europe et les Etats-Unis[338], le contenu est produit localement, coûteux et difficile d'accès[339]. Les tentatives d'achat ou de vente de contenu pédopornographique impliquaient à l'époque plusieurs risques qui sont désormais considérablement limités, voire inexistants. Par le passé, les producteurs n'étaient pas en mesure de développer des photographies ou des films[340]. Ils devaient recourir aux services d'entreprises spécialisées et s'exposer au risque d'une identification du contenu pédopornographique par les services de répression au travers des rapports produits par les entreprises concernées[341]. Cette situation a évolué pour la première fois avec l'arrivée des caméras vidéo[342]. Cela étant, les risques ne se limitaient pas à la production. L'accès au contenu pédopornographique présentait tout autant de risques pour les délinquants qui passaient leurs commandes en répondant à des petites annonces publiées dans des journaux[343]. Les moyens de communication entre le vendeur et l'acheteur, et, par conséquent, le marché lui-même, restaient limités[344]. Jusqu'au milieu des années 90, le contenu pédopornographique était principalement échangé par le biais des services postaux, ce qui permettait aux enquêteurs de parvenir à détecter un nombre conséquent d'auteurs d'infractions[345]. Selon les experts, les services de répression étaient alors en mesure de faire face aux défis rencontrés[346].

L'arrivée des applications d'échange de données sur Internet bouleverse cette situation. Jusqu'alors confrontés à un contenu analogique, les services de répression découvrent désormais, dans la plupart des cas, du matériel au format numérique[347]. Depuis le milieu des années 90, les délinquants ont de plus en plus recours aux services du réseau pour distribuer ce type de contenu[348], ce qui ne fait qu'accroître la complexité de la détection et de l'investigation des affaires de pédopornographie[349]. Internet est aujourd'hui le principal moyen d'échange de contenu pornographique ordinaire[350] et pédopornographique[351].

Le passage de la distribution analogique à la distribution numérique peut s'expliquer de différentes manières. Internet offre aux utilisateurs les moins aguerris en termes de technologie l'impression qu'ils peuvent agir en toute transparence vis-à-vis des autres. Si l'auteur d'une infraction n'emploie pas de technologie de communication anonyme, cette impression est fausse. Cela étant, le fait que l'utilisation de moyens sophistiqués de communication anonyme peut empêcher l'identification de l'auteur est une source de problèmes en ce qui concerne l'échange de contenu pédopornographique en ligne[352]. D'autre part, cette évolution a bénéficié de la baisse des prix des dispositifs techniques et des services utilisés pour produire et commercialiser les contenus pédopornographiques, notamment l'équipement d'enregistrement et les services d'hébergement[353]. Les sites Web et les services Internet étant ouverts à près de deux milliards d'internautes, le nombre de clients potentiels s'est également développé[354]. Le fait que l'accès simplifié séduise des individus qui, en dehors d'Internet, n'auraient pas pris le risque d'être démasqués en tentant d'obtenir du contenu pédopornographique pose question[355]. Avec la transition de l'analogique au numérique, un nombre croissant d'images pédopornographiques découvertes au travers d'enquêtes a été signalé[356]. Cette évolution est aussi probablement favorisée par le fait que les informations numériques peuvent, en général, être copiées sans perte de qualité[357]. Par le passé, les amateurs de pédopornographie souhaitant copier et vendre du contenu étaient en effet limités par la perte de qualité inhérente au processus de duplication. Aujourd'hui, un fichier téléchargé peut devenir la source de nouvelles copies. En conséquence, même si l'auteur qui produit le contenu en premier lieu est arrêté et ses fichiers confisqués, il est difficile de « supprimer » ces fichiers une fois échangés sur Internet[358].

Si les avis concernant la pornographie mettant en scène des adultes divergent, la pornographie mettant en scène des enfants est largement condamnée et beaucoup considèrent que les infractions qui y sont liées sont des actes criminels[359]. Plusieurs organisations internationales sont engagées dans la lutte contre la

diffusion en ligne de ce type de pornographie[360]. A noter, entre autres, plusieurs initiatives juridiques internationales: la Convention des Nations Unies relative aux droits de l'enfant de 1989[361], la Décision-cadre du Conseil de l'Union européenne relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie de 2003[362] et la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels de 2007[363].

Malheureusement, s'agissant du contrôle de la pornographique en ligne, ces initiatives se sont révélées peu dissuasives à l'encontre des délinquants qui utilisent Internet dans le but de communiquer et d'échanger des contenus pornographiques mettant en scène des enfants[364]. A noter, par ailleurs, que l'augmentation de la bande passante contribue à l'échange de films et d'archives d'images.

Selon des études portant sur le comportement des délinquants adeptes de pédopornographie, 15 % des personnes arrêtées en possession de contenus pédopornographiques liés à Internet possédaient plus de 1 000 images sur leur ordinateur, 80 % détenaient des images d'enfants âgés de six à douze ans[365], 19 % des images d'enfants âgés de moins de trois ans[366] et 21 % des images d'actes de violence[367].

La vente de contenu pédopornographique est très rentable[368], les personnes intéressées étant prêtes à payer de fortes sommes pour des films et des images montrant des enfants dans un contexte sexuel[369]. Les moteurs de recherche permettent de trouver ce type de contenu très rapidement[370]. La plupart des contenus sont échangés dans des forums privés protégés par mot de passe, auxquels l'utilisateur lambda et les services de répression ont rarement accès. La lutte contre la pédopornographie passe donc nécessairement par des opérations d'infiltration[371].

L'utilisation des TIC complique les investigations concernant ce type d'infraction, et ce pour deux raisons principales:

1 Le recours aux monnaies virtuelles et aux paiements anonymes[372]

Le paiement en liquide permettant aux acheteurs de certains types de produits de cacher leur identité, il prédomine dans de nombreuses activités commerciales criminelles. La demande de moyens de paiements anonymes a conduit au développement de systèmes de paiement virtuel et à la mise en place des monnaies virtuelles[373]. Les paiements en monnaie virtuelle ne passent pas nécessairement par un processus d'identification et de validation, ce qui empêche les services de répression de déterminer l'origine des flux d'argent et de remonter jusqu'aux malfaiteurs. Récemment cependant, dans plusieurs affaires de pédopornographie, les enquêteurs sont parvenus à identifier les criminels en exploitant les traces laissées par les paiements effectués par ces derniers[374]. Il n'en reste pas moins que les personnes qui effectuent des paiements anonymes sont difficiles à dépister[375]. Lorsque les délinquants utilisent ces monnaies anonymes, ils limitent la possibilité pour les services de répression de les identifier à l'aide du suivi des transferts d'argent[376]. C'est notamment le cas pour les affaires impliquant la vente de contenu pédopornographique[377].

2 L'utilisation de techniques de chiffrement[378]

Les délinquants chiffrent de plus en plus souvent leurs messages. De plus, selon les instances de répression, ils protègent aussi les données stockées sur leurs disques durs grâce à des techniques de chiffrement[379], ce qui complique considérablement les enquêtes[380].

Outre la pénalisation généralisée des actes de pédopornographie, d'autres approches sont actuellement envisagées, notamment l'obligation pour les fournisseurs de services en ligne de procéder à une inscription des utilisateurs ou de bloquer ou filtrer l'accès aux sites de pornographie mettant en scène des enfants[381].

2.6.3 Racisme, discours de haine et apologie de la violence

Pour faire leur propagande, les groupements radicaux utilisent des moyens de communication de masse, notamment Internet[382]. On observe depuis peu une augmentation du nombre de sites Web présentant un contenu raciste et des discours de haine[383]. Une étude menée en 2005 avance une augmentation de 25% entre 2004 et 2005 du nombre de pages Web faisant la promotion de la haine raciale, de la violence et de la xénophobie[384]. On dénombrait, en 2006, plus de 6 000 sites de ce type sur Internet[385].

La diffusion sur Internet présente pour les délinquants plusieurs avantages, notamment les faibles coûts de diffusion, la possibilité d'utiliser un équipement non professionnel et l'accès à une audience mondiale. Exemple d'incitation à la haine, les instructions fournies par certains sites sur la façon de fabriquer des bombes[386]. Internet n'est pas seulement un moyen de propagande, c'est aussi un marché pour certains types de produit (objets se rapportant au nazisme par exemple, tels que drapeaux à croix gammée, uniformes et livres). On peut facilement les acheter sur des plates-formes d'enchères et dans des boutiques en ligne spécialisées[387]. Internet est aussi utilisé pour transmettre du courrier électronique, envoyer des bulletins d'information et diffuser des clips vidéo et des programmes télévisés via des sites d'archivage bien connus (YouTube, etc.).

Tous les pays ne sanctionnent pas ces infractions[388], ce type de contenu étant parfois protégé au nom de la liberté d'expression[389]. La question de savoir jusqu'où ce principe peut s'appliquer en ce qui concerne certains sujets fait débat et les désaccords sont souvent un obstacle aux enquêtes internationales. L'affaire qui a opposé la France au fournisseur d'accès Yahoo! en 2001 est un bon exemple de conflit de lois. Un tribunal français avait ordonné au fournisseur (installé aux Etats-Unis) de bloquer l'accès des utilisateurs français à tous les contenus se rapportant au nazisme[390]. Or, en vertu du premier amendement de la Constitution des Etats-Unis, la vente de tels matériels est conforme au droit américain. Un tribunal américain a donc décidé, en raison de cet amendement, que l'ordonnance émise par le tribunal français à l'encontre de Yahoo! n'était pas applicable aux Etats-Unis[391].

Ces différences de points de vue entre les pays sont apparues au grand jour lors de l'élaboration de la Convention du Conseil de l'Europe sur la cybercriminalité. Cette convention vise à harmoniser les législations relatives à la cybercriminalité afin de garantir que les enquêtes internationales ne sont pas gênées par les conflits de lois[392]. Etant donné que les parties engagées dans les négociations n'ont pu adopter une position commune sur la pénalisation de la diffusion de matériel xénophobe, ce sujet a été totalement exclu de la convention et traité dans un document distinct, le premier Protocole[393]. Certains pays, notamment les Etats-Unis, auraient pu, sans cela, se trouver dans l'incapacité de signer la convention.

2.6.4 Infractions à motivation religieuse

Un nombre grandissant[394] de sites Internet présentent des contenus qui, dans certains pays, entrent dans le champ des dispositions juridiques relatives aux infractions à motivation religieuse, au nombre desquelles figurent les déclarations écrites contre la religion[395]. Même si certains contenus ne font que documenter des tendances et des faits réels (le déclin de la fréquentation des églises en Europe par exemple), certaines juridictions peuvent juger ce type d'information illégal. A titre d'exemple, on peut également citer la diffamation des religions et la publication de dessins humoristiques.

Les personnes qui souhaitent discuter ou traiter de façon critique d'un sujet trouvent dans le réseau Internet de multiples avantages. Elles peuvent laisser des commentaires, envoyer du contenu ou écrire des articles sans avoir à révéler leur identité. De nombreux groupes de discussion, mais aussi des portails conçus spécifiquement pour recevoir du contenu généré par l'utilisateur, reposent sur la liberté d'expression[396], facteur fondamental de la réussite d'Internet[397]. Même s'il est essentiel de protéger ce principe, il convient de rappeler qu'il est soumis à des conditions et à des lois qui régissent son application, et ce, même dans les pays les plus libéraux.

La disparité des normes juridiques en matière de contenu illicite traduit les difficultés que rencontrent les législateurs. Un contenu dont la publication est protégée par des dispositions relatives à la liberté d'expression dans le pays où il est mis à disposition peut être accessible dans des pays où les réglementations sont plus strictes. En 2005, la publication de douze dessins dans le journal danois Jyllands-Posten a déclenché de vastes protestations dans l'ensemble du monde musulman[398].

La diffusion de certaines informations ou matériels est, dans certains pays, passible de poursuites pénales au même titre que la diffusion de contenus illicites. Mais la protection des religions et des symboles religieux diffère selon les pays. Par exemple, certains sanctionnent les remarques désobligeantes à l'encontre du prophète Mahomet[399] ou la profanation du Coran[400], alors que d'autres, adoptant une approche plus libérale, ne sanctionnent pas de tels actes.

2.6.5 Paris et jeux en ligne illégaux

Les paris et les jeux en ligne constituent l'un des domaines d'activité sur Internet dont l'expansion est la plus rapide[401]. Selon la société Linden Labs, le nombre d'inscriptions au jeu en ligne Second Life[402], dont elle est l'inventeur, atteindrait les dix millions[403]. Certaines études montrent que de tels jeux ont été utilisés pour commettre des infractions, notamment[404] l'échange et l'affichage de contenus pornographiques mettant en scène des enfants[405], la fraude[406], les paris dans les cybercasinos[407], et la diffamation (diffusion de messages calomnieux par exemple).

Certaines estimations prévoient une augmentation des recettes liées aux paris en ligne, qui passeraient de 3,1 milliards USD en 2001 à 24 milliards USD en 2010[408] (à noter cependant qu'en regard des recettes générées par les jeux traditionnels, ces estimations restent relativement faibles[409]). On s'attend pour 2015 à des recettes de 28 milliards USD.[410]

Les règlementations relatives aux jeux en ligne et hors ligne varient selon les pays[411]. Les délinquants, mais aussi les commerces et les casinos qui opèrent en toute légalité, ont su exploiter cette faille. Les effets de ces disparités réglementaires apparaissent clairement à Macao. Après avoir été rendue à la Chine par le Portugal en 1999, Macao est devenue l'une des destinations les plus prisées au monde pour les jeux de hasard. Avec des recettes annuelles estimées à 6,8 milliards USD en 2006, Macao est passée devant Las Vegas (6,6 milliards USD)[412]. Ce succès tient au fait que, le jeu étant illégal en Chine[413], des milliers de joueurs font le voyage depuis le continent chinois pour assouvir leur passion.

Grâce à Internet, les joueurs peuvent contourner les restrictions concernant les jeux[414]. Les cybercasinos, sites très répandus, sont, pour la plupart, hébergés dans des pays qui sont dotés de législations libérales ou qui ne réglementent pas le jeu en ligne. Ils offrent aux internautes la possibilité d'ouvrir un compte, de transférer des fonds et de jouer à des jeux de hasard[415]. Les cybercasinos interviennent également dans les activités de blanchiment de capitaux et de financement du terrorisme[416]. Lorsque les délinquants parient dans les cybercasinos pendant la phase de blanchiment dite « d'empilage » (phase pendant laquelle les données ne sont pas consignées) ou qu'ils se trouvent dans des pays qui ne sanctionnent pas le blanchiment d'argent, les services de répression ont le plus grand mal à déterminer l'origine des fonds.

Les pays qui ont mis en place des restrictions concernant les jeux ont des difficultés à contrôler les accès aux cybercasinos et les activités de ces sites. Ainsi Internet vient-il compromettre les dispositions juridiques de lutte contre les jeux[417]. Plusieurs pays ont essayé d'interdire, par la loi, la participation aux jeux en ligne[418]. On peut citer l'*Internet Gambling Prohibition Enforcement Act* de 2006 (loi d'application de l'interdiction du jeu sur Internet) aux Etats-Unis, qui vise à limiter les jeux illégaux en poursuivant les prestataires de services financiers qui acceptent d'effectuer des transactions liées à des de tels jeux[419].

2.6.6 Diffamation et fausses informations

Si Internet permet de diffuser de vraies informations, il permet d'en répandre de fausses tout aussi facilement[420]. On peut trouver, sur les sites Internet, des informations fausses ou diffamatoires, notamment dans les forums et les salons de discussion qui ne sont pas contrôlés par des modérateurs[421]. Les mineurs utilisent de plus en plus les forums et les sites de réseau social, qui sont aussi des vecteurs de fausses informations[422]. Parmi les actes répréhensibles[423], on peut citer la diffusion de photographies intimes et la publication de fausses informations concernant les comportements sexuels[424].

La plupart des délinquants profitent du fait que les services de publication en ligne gratuits ou bons marché n'imposent généralement pas aux auteurs de s'identifier ou ne vérifient pas correctement les identités[425]. Ce mode de fonctionnement complique l'identification des délinquants. Il arrive en outre que les modérateurs ne contrôlent pas suffisamment – ou pas du tout – les contenus envoyés sur les forums. Ces avantages (anonymat, absence de contrôle du contenu) n'ont cependant pas empêché le développement de projets de grande valeur, qui sont régis par des procédures strictes de réglementation du contenu, parmi lesquels Wikipedia[426], encyclopédie en ligne alimentée par ses utilisateurs. Cela étant, les délinquants utilisent ces mêmes avantages pour diffuser de fausses informations (sur des concurrents par exemple)[427] ou révéler des informations confidentielles (en diffusant des secrets d'Etat ou des informations commerciales sensibles par exemple).

Il est essentiel de souligner les risques grandissants que présentent les fausses informations ou les informations trompeuses. De fait, les déclarations en ligne étant accessibles par un très large public dans le monde entier, les actes de diffamation peuvent très gravement porter atteinte à la réputation et à la dignité des victimes. Dès lors qu'une information est publiée sur Internet, son ou ses auteurs en perdent généralement le contrôle. Quand bien même elle serait corrigée ou effacée peu de temps après sa publication, le risque existe qu'elle ait déjà été dupliquée (sites « miroirs ») et publiée par une personne qui refuse de la démentir ou de la retirer. Dans ce cas, l'information est toujours disponible en ligne, même si elle a été retirée ou corrigée par son auteur[428]. On peut citer, à titre d'exemple, le cas des « courriels incontrôlables », qui sont transmis à des millions de personnes et contiennent des informations salaces, trompeuses ou fausses sur des individus ou des organisations, dont la réputation ne sera peut-être jamais restaurée, et ce, indépendamment du bien-fondé du courriel d'origine. Pour prévenir les risques de diffamation, il est donc indispensable de trouver un compromis entre liberté d'expression[429] d'une part et protection des victimes d'autre part[430].

2.6.7 Spam et risques connexes

Le spam désigne un message non sollicité envoyé en masse[431]. Parmi les différentes méthodes d'escroquerie, celle qui utilise la messagerie électronique est la plus courante. Elle consiste à envoyer des millions de courriels, souvent à des fins publicitaires pour proposer des services ou des produits. Ces courriels contiennent aussi fréquemment des logiciels malveillants. Depuis l'envoi du premier courriel de spam en 1978[432], le phénomène n'a fait qu'augmenter, pour atteindre aujourd'hui des proportions considérables[433]. Selon les prestataires de messagerie électroniques, le spam représenterait jusqu'à 85 à 90 % de l'ensemble des courriels[434]. En 2007, les principales sources de spam par courriel étaient les Etats-Unis (19,6 % du spam recensé), la République populaire de Chine (8,4 %) et la République de Corée (6,5 %)[435]. Six ans après, les trois principales sources de spam restaient identiques: République populaire de Chine (22,97 % du spam recensé), États-Unis (17,6 %) et République de Corée (12,67 %).[436]

La plupart des fournisseurs de courriel ont réagi à l'augmentation du spam en installant des filtres anti-spam, qui repèrent les courriels incriminés à l'aide de mots-clés ou de listes noires contenant les adresses IP des spammeurs[437]. Malgré l'évolution des technologies de filtrage, les spammeurs parviennent à contourner les systèmes de protection, notamment en évitant d'utiliser des mots-clés. Ils ont par exemple imaginé de multiples façons de décrire le Viagra – l'un des produits les plus couramment proposés dans des spams – sans utiliser le nom de la marque[438].

La capacité à détecter le spam dépend des techniques de diffusion et de leurs évolutions. De nombreux spammeurs n'envoient pas leurs courriels à partir d'un unique serveur de messagerie (ce qui, d'un point de vue technique, faciliterait le travail d'investigation des fournisseurs de messagerie électronique du fait du nombre limité de sources[439]), mais en utilisant des botnets[440]. Chaque ordinateur du botnet – qui en contient des milliers[441] – n'envoie que quelques centaines de messages. Cette technique de diffusion complique le travail des fournisseurs de messagerie électronique qui cherchent à détecter les messages pollués en analysant les informations concernant les émetteurs, ainsi que le travail des services de répression qui tentent de remonter jusqu'aux spammeurs.

Comme il est possible d'envoyer des milliards de courriels pour une somme modique, l'envoi de spam est une activité très rentable. L'utilisation de botnets permet encore de réduire les coûts[442]. Certains experts avancent ainsi que la seule solution pour lutter contre le spam serait d'augmenter les coûts d'émission des courriels[443]. Selon une analyse des coûts et des profits du spam envoyé par courriel publiée en 2007, le coût d'envoi de 20 millions de courriels s'élève à environ 500 USD[444]. L'envoi de spam est donc une technique très rentable, notamment pour ceux qui envoient les courriels par milliards, tel ce spammeur néerlandais, qui déclarait avoir dégagé un bénéfice de 50 000 USD en envoyant au moins 9 milliards de courriels pollués[445].

En 2005, l'OCDE a analysé, dans un rapport, les effets du spam sur les pays en développement[446]. Ces pays déclarent souvent que leurs internautes subissent davantage les effets du spam et des pratiques frauduleuses sur Internet. En effet, la bande passante et l'accès à Internet sont pour eux des ressources précieuses, plus limitées et plus onéreuses que dans les pays industrialisés[447]. L'envoi de spam consommant inutilement des ressources et du temps, les pays en développement sont donc particulièrement touchés.

2.6.8 Extorsion

L'extorsion n'est pas considérée comme relevant de la cybercriminalité type, mais de la délinquance traditionnelle. Toutefois, l'utilisation de plus en plus courante des TIC a ouvert la voie à des attaques souvent appelée « cyberextorsion ».[448] Ces dernières années, aussi bien les grandes entreprises que les jeunes entreprises de petite taille ont été visées par de telles attaques.[449] Les pirates se servent de plus en plus souvent de plusieurs avantages que présentent les TIC par rapport aux méthodes traditionnellement utilisées pour commettre de telles infractions. En plus d'utiliser des technologies de communication permettant de conserver l'anonymat pour perpétrer les infractions, les pirates sont de plus en plus nombreux à utiliser des monnaies virtuelles à place des paiements au comptant par virement.[450] Les travaux de recherche font apparaitre que les entreprises sous-estiment toujours la menace d'extorsion.[451]

Une forme plus automatisée d'extorsion est constituée par ce que l'on appelle le « logiciel de demande de rançon » : un logiciel malveillant infecte un système informatique, le bloque et affiche un message indiquant que l'ordinateur ne sera débloqué qu'après paiement d'une rançon par la victime. Ce phénomène inquiète de plus en plus.[452] Pour se montrer plus persuasifs, les auteurs des infractions font souvent croire que l'ordinateur a été bloqué par un organisme chargé de faire respecter la loi en raison d'activités illégales menées par l'utilisateur.[453]

2.6.9 Autres formes de contenu illicite

Internet n'est pas seulement un moyen de lancer des attaques directes, c'est aussi une plate-forme qui permet de solliciter, de proposer et d'encourager la commission d'infractions[454], de vendre illégalement des produits et de diffuser des informations et des instructions permettant de commettre des actes illicites (mode d'emploi pour fabriquer des explosifs par exemple).

De nombreux pays ont pris des dispositions pour réglementer la vente de certains produits. Les législations et les restrictions commerciales (concernant le matériel militaire par exemple) varient d'un pays à l'autre[455]. C'est le cas notamment de la vente de médicaments: tel médicament en vente libre dans un pays et seulement prescrit sur ordonnance dans un autre[456]. Par ailleurs, du fait de la mondialisation des échanges commerciaux, il est parfois difficile de garantir que l'accès à certains produits est bien limité à une zone précise[457]. Avec la popularité grandissante d'Internet, ce problème prend de l'ampleur. En effet, certaines boutiques en ligne peuvent vendre des produits autorisés sur leur sol à des pays qui ont mis en place des mesures restrictives, lesquelles se trouvent du coup menacées.

Avant Internet, il était difficile pour le citoyen lambda d'obtenir des informations sur la fabrication des armes. Certes, ces informations étaient disponibles (dans des ouvrages sur la chimie des explosifs par exemple), mais les trouver prenait du temps. Aujourd'hui disponibles sur Internet[458] elles sont plus faciles à obtenir, ce qui augmente les risques d'attaque armée.

2.7 Infractions se rapportant aux atteintes à la propriété intellectuelle et aux marques commerciales

Bibliography (selected): Androutsellis-Theotokis/Spinellis, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; Bakken, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf; Clarke/Sandberg/Wiley/Hong, Freenet: a distributed anonymous information storage and retrieval system, 2001; Cunard/Hill/Barlas, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; Fischer, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002; Johnson/McGuire/Willey, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf; Lohmann, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; Penn, Copyright Law:

Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2; Rayburn, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001; Schoder/Fischbach/Schmitt, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Sifferd, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93.

L'une des fonctions essentielles d'Internet est la diffusion d'informations. Les entreprises, par exemple, utilisent Internet pour diffuser des informations sur leurs services et leurs produits. S'agissant du piratage, elles courent sur Internet les mêmes risques qu'en dehors du réseau: leur image de marque et leur charte graphique peuvent être utilisées pour la vente de produits de contrefaçon. Les contrefacteurs copient les logos et les produits, certains tentent de faire enregistrer le domaine Internet des sociétés qu'ils visent. En outre, les sociétés qui vendent directement sur Internet[459] peuvent être poursuivies pour violation de droits d'auteur si les produits qu'elles proposent sont téléchargés, copiés et redistribués.

2.7.1 Infractions se rapportant aux atteintes à la propriété intellectuelle

L'industrie du divertissement a profité du passage de l'analogique au numérique[460] pour numériser[461] les supports afin d'enrichir les fonctionnalités et les services. Les DVD intègrent aujourd'hui des doublages en plusieurs langues, des sous-titres, des bandes annonces, des bonus, etc. Les CD et DVD sont en outre plus durables que les disques et les vidéocassettes[462].

Mais en offrant la possibilité de reproduire une œuvre rapidement et avec précision, la numérisation a ouvert la voie à de nouvelles atteintes à la propriété intellectuelle. Avant la numérisation, la copie d'un disque ou d'une vidéocassette s'accompagnait nécessairement d'une perte de qualité. Aujourd'hui, il est possible de dupliquer des sources numériques sans perte de qualité et, partant, d'effectuer des reproductions à partir de n'importe quelle copie. Parmi les atteintes à la propriété intellectuelle les plus courantes, on peut citer l'échange de musique, de logiciels protégés et de fichiers par le biais de systèmes de partage de fichiers[463] ou de services d'hébergement partagé, ou le fait de contourner les systèmes de gestion des droits numériques (DRM)[464].

Les systèmes de partage de fichiers sont des services en réseau reposant sur le *peer-to-peer*[465], qui permettent aux utilisateurs de partager des fichiers[466], souvent avec des millions d'autres utilisateurs[467]. Après avoir installé le logiciel de partage, l'utilisateur peut choisir les fichiers qu'il souhaite partager et rechercher des fichiers mis à disposition par des centaines d'autres utilisateurs. Avant le développement des systèmes de partage de fichiers, les cassettes et les disques étaient déjà copiés et échangés. Le partage de fichier a permis de multiplier les sources d'échange.

La technologie *peer-to-peer* (P2P) joue un rôle essentiel sur Internet. Plus de 50 % du trafic généré par les internautes provient de réseaux *peer-to-peer*[468] et le nombre d'utilisateurs de ces réseaux est en constante augmentation. Selon un rapport publié par l'OCDE, 30 % des internautes français auraient téléchargé de la musique ou des fichiers via des systèmes de partage[469], les autres pays de l'OCDE affichant une tendance analogue[470].Ces systèmes permettent d'échanger tout type de données informatiques: musique, films, logiciels, etc.[471] Autrefois principalement utilisé pour échanger de la musique, le partage de fichiers sert aujourd'hui de plus en plus à télécharger des vidéos[472].

Les services de partage de fichiers utilisent une technologie très sophistiquée, qui permet d'échanger de gros fichiers sur de courtes périodes de temps[473]. Ceux de la première génération reposant sur un serveur central chargé de communiquer aux utilisateurs la liste des fichiers disponibles, les agences de répression avaient les moyens d'intervenir contre le partage de fichiers illégal au sein du réseau Napster[474]. Les systèmes de deuxième génération ne reposent plus sur un serveur central[475]: ils sont décentralisés. Il est donc plus difficile de les bloquer. Néanmoins, le fait que les communications soient directes permet de remonter jusqu'aux utilisateurs à partir de leur adresse IP[476]. Si les enquêtes visant à dépister les atteintes à la propriété intellectuelle dans les systèmes de partage de fichiers ont parfois porté leurs fruits, des versions plus récentes de ces systèmes, qui autorisent certaines formes de communication anonyme devraient, à l'avenir, compliquer les enquêtes[477].

Les internautes ordinaires et les délinquants ne sont pas les seuls utilisateurs des technologies de partage de fichiers. Les entreprises en ont également l'utilité[478]. Aussi, tous les fichiers échangés dans un tel système ne portent-ils nécessairement pas atteinte à la propriété intellectuelle. L'échange de copies autorisées ou d'œuvres d'art du domaine public est un exemple d'utilisation parfaitement légitime[479].

Cela étant, les systèmes de partage de fichiers posent à l'industrie du divertissement divers problèmes[480]. Il est par exemple difficile de savoir dans quelle mesure la diminution des ventes de CD/DVD et de billets de cinéma est due à l'échange de titres dans les systèmes de partage de fichiers. Quoi qu'il en soit, d'après les études réalisées, les utilisateurs de ces systèmes se comptent par millions[481], et les fichiers téléchargés par milliards[482]. On trouve même des copies de films avant leur sortie officielle en salle[483], d'où un manque à gagner pour les détenteurs de droits d'auteur. L'apparition récente de systèmes de partage anonymes va compliquer la tâche des ayants droit et des services de répression[484].

L'industrie du divertissement a réagi en utilisant des technologies conçues pour empêcher les utilisateurs de faire des copies de CD et de DVD, notamment le système d'embrouillage de contenu (CSS)[485], qui consiste à chiffrer les DVD au niveau de leur contenu pour en empêcher la copie[486]. Ces technologies sont une composante essentielle des nouveaux modèles économiques, qui visent à définir plus précisément les droits d'accès des utilisateurs. La gestion des droits numériques (DRM)[487] désigne la mise en œuvre de technologies permettant aux détenteurs de droits d'auteur de limiter l'utilisation des médias numériques, modèle dans lequel les consommateurs achètent des droits d'utilisation limités (par exemple, le droit de diffuser un titre de musique au cours d'une soirée uniquement). Les DRM offrent la possibilité de mettre en place de nouveaux modèles économiques, qui reflètent mieux les intérêts des ayants droit et des utilisateurs. Ils pourraient permettre d'inverser la tendance et de rétablir les profits.

Mais ces technologies présentent un problème majeur: il est possible de contourner les protections[488]. Les pirates ont en effet développé des outils logiciels permettant aux utilisateurs de diffuser sur Internet des fichiers protégés contre la copie[489], et ce pour une somme modique, voire gratuitement. Une fois la protection DRM retirée, un fichier peut être copié et lu sans limitation aucune.

Les industries de la musique et du cinéma ne sont pas les seules à déployer des efforts pour protéger leurs produits. Certaines chaînes de télévision (en particulier les chaînes à péage) chiffrent les contenus afin de s'assurer que seuls les abonnés peuvent recevoir leurs programmes. Malgré des techniques de protection sophistiquées, les pirates parviennent à falsifier les dispositifs matériels de contrôle d'accès ou à briser les codes de chiffrement à l'aide d'outils logiciels[490].

Sans les outils logiciels nécessaires, les utilisateurs ordinaires ont plus de difficultés à commettre ces infractions. C'est pourquoi les études sur la pénalisation des atteintes à la propriété intellectuelle ne portent pas seulement sur les systèmes de partage et sur le fait de contourner les protections techniques, mais aussi sur la fabrication, la vente et la détention de « dispositifs illégaux » ou d'outils destinés à permettre aux utilisateurs de passer outre les droits d'auteur[491].

2.7.2 Infractions se rapportant aux marques commerciales

Les infractions se rapportant aux marques commerciales, bien connues du commerce international, ressemblent aux infractions contre le droit à la propriété intellectuelle. Elles sont passées dans le cyberespace et sont sanctionnées différemment selon les pays [492] . Les infractions les plus graves comprennent l'utilisation de marques commerciales dans le but de tromper et les infractions se rapportant au nom ou domaine.

Pour une société, bonne réputation et marque commerciale sont souvent directement liées. Certains types d'activités délictueuses reposent donc sur l'utilisation frauduleuse des noms de marques et des marques commerciales. On peut citer le hameçonnage[493], technique consistant à envoyer des millions de courriels falsifiés (en y insérant des noms de marque par exemple) afin de persuader les destinataires qu'ils proviennent de sociétés reconnues pour légitimes[494].

Parmi les infractions se rapportant à des marques commerciales, on compte aussi celles qui visent les domaines Internet[495], telles que le cybersquattage[496], pratique abusive consistant à faire enregistrer le nom de la marque commerciale d'un produit ou d'une société ou un nom approchant[497]. La plupart du temps,

les malfaiteurs cherchent à revendre au prix fort le nom de domaine à la société prise pour victime[498] ou à utiliser ce domaine pour vendre des produits ou des services en mettant en avant un prétendu rapport avec la marque commerciale afin de tromper les internautes[499]. On peut également citer le « détournement de domaine » et l'enregistrement de noms de domaines ayant expiré par mégarde[500].

2.8 Infractions informatiques

Bibliography (selected): *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*; *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf; *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005; *Gercke*, Internet-related Identity Theft, 2007; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270; *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004; *Paget*, Identity Theft – McAfee White Paper, page 10, 2007; *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1; *Sieber*, Council of Europe Organised Crime Report 2004; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*

Cette catégorie regroupe plusieurs types d'infractions, qui sont nécessairement commises à l'aide d'un système informatique. Contrairement aux catégories précédentes, ces infractions, moins spécifiques, ne concernent pas aussi strictement la violation de principes juridiques. Elles comprennent la fraude informatique, la falsification informatique, le hameçonnage et le vol d'identité, ainsi que l'utilisation abusive de dispositifs.

2.8.1 Fraude et fraude informatique

La fraude informatique est l'un des délits les plus courants sur Internet[501], car elle peut être automatisée[502] et réalisée avec des logiciels permettant au fraudeur de cacher son identité.

Grâce à l'automatisation, les malfaiteurs peuvent tirer de grands bénéfices d'un petit nombre d'actions[503]. Une stratégie consiste à veiller à ce que les pertes financières supportées par chaque victime restent en deçà d'une certaine limite. En effet, les victimes sont alors moins tentées d'investir du temps et de l'énergie pour signaler ces infractions et entamer des recherches[504]. Dans cette catégorie d'escroquerie, on peut citer la fraude aux avances sur commission, notamment la « lettre nigériane »[505].

Bien que ces infractions soient commises à l'aide de technologies informatiques, la plupart des systèmes juridiques de droit pénal ne les classent pas sous la catégorie « infractions informatiques » mais « fraude ordinaire »[506], le critère étant la cible de l'infraction. Si les malfaiteurs cherchent à influencer une personne, l'infraction est généralement qualifiée de fraude. Si la cible est un ordinateur ou un système de traitement de données, l'infraction est souvent qualifiée de fraude informatique. Cela étant, les systèmes juridiques qui reconnaissent la fraude mais pas encore la manipulation de systèmes informatiques à des fins frauduleuses permettent, en règle générale, de poursuivre les infractions susmentionnées. Les escroqueries de type « fraude » les plus fréquentes comprennent la fraude aux enchères en ligne et la fraude aux avances sur commission.

La fraude aux enchères en ligne [507]

Les enchères en ligne sont aujourd'hui l'un des services de commerce électronique les plus populaires. En 2006 déjà, des biens pour une valeur totale dépassant 20 milliards USD ont été vendus sur eBay, plus grand site d'enchères au monde[508]. Les acheteurs ont accès à des produits du monde entier, aussi variés que

spécialisés; les vendeurs, de leur côté, bénéficient d'une clientèle à l'échelle mondiale, ce qui stimule la demande et fait grimper les prix.

Les auteurs d'infraction sur les plates-formes d'enchères exploitent l'absence de contact en face à face entre les acheteurs et les vendeurs[509]. Comme il est difficile de faire la distinction entre un utilisateur honnête et un malfaiteur, la fraude aux enchères est devenue l'un des cyberdélits les plus fréquents[510]. Les deux escroqueries les plus courantes consistent[511] à proposer à la vente des produits qui n'existent pas et à exiger des acheteurs le paiement avant livraison[512] et à faire un achat et à demander d'être livré, avec l'intention de ne pas payer.

Pour lutter contre ces escroqueries, les responsables de ces sites ont mis au point des systèmes de protection, notamment le système de feed-back/commentaires. Après chaque transaction, les acheteurs et les vendeurs laissent un commentaire[513], qui fournit aux autres utilisateurs une information neutre sur la fiabilité des vendeurs/acheteurs. Selon ce principe – qui pourrait se résumer ainsi: « tout repose sur la réputation » – il est plus difficile, sans un nombre suffisant de commentaires positifs, de persuader les victimes potentielles de payer pour des produits qui n'existent pas ou, inversement, d'accepter d'envoyer des produits avant réception du paiement. Mais les malfaiteurs ont réagi en contournant cette protection par le biais de comptes utilisateurs appartenant à des tiers[514]. Dans cette escroquerie appelée « piratage de compte »[515], les malfaiteurs tentent, pour masquer leur identité et compliquer les recherches, d'obtenir les noms et les mots de passe d'utilisateurs honnêtes afin de vendre ou d'acheter frauduleusement des produits.

La fraude aux avances sur commission [516]

La fraude aux avances sur commission consiste à envoyer des courriels qui sollicitent l'aide du destinataire pour transférer de grosses sommes d'argent vers des tiers. Le message précise que le destinataire recevra un pourcentage s'il accepte de faire transférer l'argent par son compte personnel[517]. Il lui est également demandé d'envoyer une somme modique afin de valider ses coordonnées bancaires (les personnes qui répondent, percevant des similitudes avec les jeux de loterie, acceptent de perdre une somme minime en échange d'un gain important bien que peu probable). Une fois l'argent envoyé, la victime n'entend plus jamais parler du malfaiteur. Il est parfois demandé au destinataire d'envoyer directement ses coordonnées bancaires, que les malfaiteurs utilisent pour commettre des actes frauduleux. D'après les informations dont on dispose, des milliers de victimes répondraient à ce type de courriel[518]. En dépit des diverses initiatives et campagnes d'information, il ressort des études en cours que la fraude aux avances sur commission progresse toujours, que ce soit par le nombre de victimes ou par le total des pertes financières[519].

2.8.2 Falsification informatique

La falsification informatique désigne la manipulation de documents numériques[520], notamment la création d'un document qui semble provenir d'une institution digne de confiance, la manipulation d'images électroniques (par exemple, d'images utilisées comme éléments de preuve devant les tribunaux) et l'altération de documents contenant du texte.

La falsification des courriels comprend notamment l'escroquerie dite du « hameçonnage », problème majeur pour les services de répression dans le monde entier[521]. L'objectif du hameçonnage est d'amener la victime à révéler des informations personnelles ou confidentielles[522]. La plupart du temps, le malfaiteur envoie des courriels qui ressemblent à des messages provenant d'établissements financiers légitimes avec lesquels la victime a l'habitude de traiter[523]. Le courriel est rédigé de telle façon qu'il est difficile pour la victime de déceler la supercherie[524]. Dans le message, il est demandé au destinataire de révéler et/ou de vérifier certaines informations sensibles. De nombreuses victimes s'exécutent et divulguent les informations demandées, permettant ainsi aux malfaiteurs d'effectuer des transferts en ligne et d'autres opérations frauduleuses[525].

Par le passé, les poursuites pour falsification informatique étaient rares, car la plupart des documents faisant foi étaient des documents sur papier. Les documents numériques jouent aujourd'hui un rôle toujours plus important et sont de plus en plus utilisés. Le remplacement des documents classiques par des

documents numériques est d'ailleurs conforté par la loi. On notera à ce propos les dispositions juridiques qui reconnaissent la validité des signatures numériques.

De tout temps, les malfaiteurs ont essayé de manipuler les documents. Il est aujourd'hui possible de copier des documents numériques sans perte de qualité et de les modifier sans difficulté. A moins qu'un dispositif technique[526] visant à protéger un document n'ait été falsifié, les experts de la police scientifique ont généralement du mal à apporter la preuve que le document a subi des manipulations numériques[527].

2.8.3 Vol d'identité

Le terme « vol d'identité » – qui n'est ni défini ni employé de façon cohérente – désigne le fait d'obtenir et d'utiliser frauduleusement l'identité d'une autre personne[528]. Cet acte peut être effectué sans l'aide de moyens techniques[529], mais aussi en ligne grâce à la technologie Internet[530].

D'après la couverture médiatique dont elles font l'objet[531], les résultats de différentes études analysant l'ampleur du vol d'identité et les préjudices qui en découlent[532] et les nombreuses analyses techniques et juridiques[533] publiées ces dernières années, on pourrait facilement estimer que les infractions liées à l'identité sont un phénomène spécifique au 21ème siècle[534]. Ce n'est toutefois pas le cas, puisque les infractions liées à l'usurpation d'identité ou à la falsification et à l'utilisation frauduleuse des documents d'identité existent depuis plus d'un siècle[535]. Dès les années 80, la presse fait régulièrement état de cas d'utilisation frauduleuse d'informations relatives à l'identité [536]. L'utilisation des pièces d'identité numériques et des technologies de l'information n'a fait que modifier les méthodes employées par les malfaiteurs, ainsi que leurs cibles[537]. L'utilisation de plus en plus courante des informations numériques a offert aux malfaiteurs de nouvelles possibilités d'accéder à des informations liées à l'identité[538]. Ainsi, le processus de transformation des nations industrialisées en sociétés de l'information [539] a-t-il eu une influence considérable sur l'émergence de nouvelles infractions liées au vol d'identité. Néanmoins, malgré le nombre conséquent d'affaires liées au vol d'identité sur Internet, la numérisation n'a pas fondamentalement modifié l'essence même de l'infraction, mais elle a créé de nouvelles cibles et facilité l'élaboration de nouvelles méthodes[540]. Il semble que l'effet de l'utilisation croissante de la technologie Internet soit surestimé. Selon les résultats d'une analyse des méthodes employées pour commettre des infractions liées à l'identité, le vol d'identité reste, dans une grande mesure, une infraction commise en dehors de toute connexion à l'Internet[541]. En 2007, 20% des infractions commises aux Etats-Unis [542] impliquaient des escroqueries en ligne et des vols de données[543]. En dépit des évolutions récentes, le vol d'identité en dehors du cadre de l'Internet reste très pratiqué. Il est surprenant de constater que le nombre d'infractions commises en dehors de toute connexion à l'Internet reste conséquent, la numérisation et la mondialisation des services basés sur Internet ayant conduit à une augmentation de l'utilisation des informations numériques liées à l'identité[544]. Ces informations sont de plus en plus importantes, aussi bien au sein de l'économie qu'en termes d'interaction sociale. Par le passé, une « réputation » et des relations personnelles bien placées dominaient le monde des affaires tout comme les transactions quotidiennes[545]. Avec l'adoption du commerce électronique, l'identification en face à face devient pratiquement impossible et, partant, les données d'identification personnelle prennent une importance majeure pour les individus qui participent aux interactions sociales et économiques [546]. Ce processus peut être assimilé à une instrumentalisation[547], où l'identité est traduite en données d'identification personnelle quantifiables. Ce processus, associé à la distinction entre l'aspect plus philosophique du terme « identité » (défini[548] comme étant la collecte de caractéristiques personnelles) et les données d'identification personnelle qui permettent de reconnaître une personne, revêt une importance cruciale. Cette transformation ne concerne pas uniquement les caractéristiques Internet du vol d'identité, puisque l'effet de cette évolution s'étend bien au-delà des réseaux informatiques. Aujourd'hui, les exigences imposées par les transactions distantes, telles que la confiance et la sécurité[549], dominent l'économie au sens large et ne se limitent pas aux activités du commerce électronique. On peut citer, à titre d'exemple, l'utilisation de cartes de paiement assorties d'un code d'identification personnel pour l'achat de biens dans un supermarché.

En règle générale, les infractions désignées sous le terme de « vol d'identité » se déroulent en trois phases[550]. Dans une première phase, le malfaiteur obtient des informations se rapportant à l'identité de la victime, par exemple au moyen d'un logiciel malveillant ou par des attaques de type hameçonnage. La deuxième phase se caractérise par divers échanges mettant en jeu les informations d'identité recueillies[551].

Dans cette phase, les informations ne sont pas encore directement utilisées mais elles peuvent par exemple être vendues[552]. Des données relatives à des cartes de crédit peuvent par exemple se vendre jusqu'à 60 USD[553]. La troisième phase correspond à l'utilisation des informations dans le cadre d'une infraction. Dans la plupart des cas, l'accès à des données d'identification personnelle permet au malfaiteur de commettre de nouvelles infractions[554]. Il ne s'intéresse donc pas aux données elles-mêmes, mais à la possibilité qu'elles offrent de commettre des infractions, par exemple la falsification de documents d'identification ou des fraudes à la carte de crédit[555].

Dans la première phase, les méthodes utilisées pour obtenir des données sont très nombreuses. Les méthodes dites « matérielles » consistent à dérober des dispositifs de stockage informatique contenant des données d'identité, à fouiller les poubelles (« *dumpster diving* »[556]), à voler du courrier[557], etc. Il est aussi possible d'utiliser des moteurs de recherche. On parle dans ce cas de « *Googlehacking* » (piratage par Google) et de « *googledorks* » (pirates utilisant Google) pour faire référence à l'utilisation de requêtes complexes sur des moteurs de recherche dans le but de filtrer de grandes quantités de résultats, à la recherche d'informations mettant en évidence des problèmes de sécurité dans les systèmes informatiques ainsi que d'informations personnelles utilisables dans des escroqueries reposant sur le vol d'identité. Tel malfaiteur cherchera par exemple à identifier des systèmes dont la protection par mot de passe est insuffisante dans le but d'y dérober des informations[558]. Des études soulignent d'ailleurs les risques que peut présenter l'utilisation de moteurs de recherche à des fins illicites[559]. Des problèmes analogues ont été signalés avec les systèmes de partage de fichiers. Le Congrès américain a récemment examiné la question de l'utilisation de ces systèmes dans le but d'obtenir des données personnelles à des fins d'usurpation d'identité[560]. Outre cette possibilité, les malfaiteurs peuvent aussi recourir à des personnes internes ayant accès à des données d'identité. D'après l'étude *Computer Crime and Security Survey 2007*[561], réalisée par l'institut américain CSI, plus de 35% des personnes ayant répondu estiment que le pourcentage des pertes de leur organisation dues à des personnes internes est supérieur à 20%. En 2013, une enquête a montré que 23 % des infractions électroniques étaient commises par des personnes internes ; 53% des personnes interrogées étaient d'avis que les attaques de l'intérieur étaient plus préjudiciables que les attaques de l'extérieur.[562] Enfin, on a vu apparaître ces dernières années des méthodes d'escroquerie efficaces utilisant des techniques d'ingénierie sociale pour persuader les victimes de divulguer des informations personnelles ou confidentielles (coordonnées bancaires, données de cartes de crédit, etc.)[563].

Les données recherchées sont de plusieurs types[564]. Les plus courantes sont le numéro de Sécurité Sociale et le numéro de passeport, la date de naissance, l'adresse et les numéros de téléphone, et les mots de passe.

Numéro de Sécurité Sociale ou numéro de passeport

Le numéro de sécurité sociale tel que celui utilisé aux Etats-Unis est un exemple classique de données d'identité recherchées par les malfaiteurs. Créé à l'origine pour suivre précisément les gains des personnes à des fins fiscales, il est en effet très fréquemment utilisé comme moyen d'identification[565]. Les malfaiteurs utilisent les numéros de sécurité sociale ou de passeport pour ouvrir des comptes bancaires, prendre le contrôle de comptes existants, ouvrir des crédits ou accumuler des dettes[566].

Date de naissance, adresse et numéros de téléphone

Ces données ne peuvent en général servir à commettre des vols d'identité que lorsqu'elles sont combinées à d'autres éléments d'information (par exemple, le numéro de sécurité sociale)[567]. La connaissance d'informations supplémentaires telles que la date de naissance ou l'adresse permet au malfaiteur de contourner les processus de vérification. L'un des plus grands risques liés à ce type de données tient au fait qu'elles sont largement disponibles en ligne, qu'elles aient été publiées volontairement dans l'un des très nombreux forums nominatifs[568] ou saisies sur des sites comme preuve d'identité en vertu d'obligations légales[569].

Mots de passe de comptes non financiers

La connaissance d'un mot de passe permet au malfaiteur de modifier les paramètres d'un compte afin de l'utiliser pour ses propres besoins[570]. Il peut par exemple prendre le contrôle d'un compte de messagerie

électronique dans le but d'envoyer des messages illicites. Il peut aussi s'approprier le compte d'un utilisateur de plate-forme d'enchères pour vendre des produits volés[571].

Mots de passe de comptes financiers

A l'instar du numéro de sécurité sociale, les données concernant des comptes financiers sont une cible fréquente de vol d'identité. Comptes chèques, comptes d'épargne, cartes de crédit, cartes de débit, données de planification financière, autant d'informations qu'un voleur d'identité peut utiliser pour commettre des cyberdélits financiers.

Le vol d'identité est un problème grave et de plus en plus pressant[572]. Au premier semestre 2004, 3% des ménages américains ont été victimes de vol[573]. En 2012, le Bureau des statistiques judiciaires a annoncé que 7% des personnes âgées de 16 ans ou plus aux Etats-Unis avaient été victimes au moins une fois de vol d'identité en 2012.[574] Au Royaume-Uni, le coût du vol d'identité pour l'économie britannique a été estimé à 1,3 milliard de livres par an[575]. Les estimations concernant les pertes dues au vol d'identité en Australie sont comprises entre moins d'un milliard USD et plus de 3 milliards USD par an[576]. L'*Identity Fraud Survey 2006* (étude sur la fraude à l'identité 2006) estime les pertes en 2005 aux Etats-Unis à 56,6 milliards USD[577]. Dans l'édition de 2013 du même rapport, on estime les pertes à 20,9 milliards USD pour 2012. Outre l'aspect financier, il convient également de mentionner les atteintes à la réputation[578]. Dans les faits, de nombreuses victimes ne signalent pas ces infractions et les établissements financiers se font rarement l'écho des mauvaises expériences de leurs clients. Aussi est-il probable que l'incidence réelle du vol d'identité dépasse largement le nombre de signalements[579].

L'usurpation d'identité en ligne est possible car, sur Internet, il existe peu de mécanismes de vérification d'identité. Il est plus facile d'identifier les personnes dans le monde réel que sur Internet, où les méthodes d'identification sont généralement plus complexes. Les outils d'identification sophistiqués (au moyen de données biométriques par exemple) sont coûteux et peu utilisés. Les contrôles sur Internet étant peu développés, le vol d'identité est une activité simple et rentable[580].

Un phénomène étroitement lié à l'essor des "big data" est la prolifération des informations relatives à l'identité que l'on peut se procurer sur les "marchés noirs". Si les auteurs d'infraction piratent des bases de données contenant des millions de fichiers clients, une grande partie de ces fichiers pourra être vendue par la suite. Ainsi, d'après des travaux de recherche publiés en 2014, les informations relatives à l'identité obtenues dans le cadre de vols de données et disponibles sur les cybermarchés noirs comprennent des justificatifs d'identité concernant jusqu'à 360 millions de comptes.[581]

2.8.4 Utilisation abusive de dispositifs

Pour commettre une infraction sur Internet, un équipement relativement élémentaire suffit[582]. Certaines infractions, telles que la diffamation ou la fraude en ligne, ne nécessitent qu'un ordinateur et un accès au réseau, et peuvent donc être commises dans un cybercafé. Les infractions plus sophistiquées nécessitent l'utilisation d'outils logiciels spécialisés.

Il est facile de se procurer sur Internet des outils permettant de commettre des infractions complexes[583]. Si les plus simples sont souvent gratuits, les plus sophistiqués peuvent coûter plusieurs milliers de dollars[584]. Grâce à ces outils, les malfaiteurs peuvent attaquer des systèmes informatiques en un simple clic. Les attaques standard sont aujourd'hui moins efficaces, car les sociétés spécialisées dans la sécurité informatique analysent ces outils et se préparent à contrer les attaques. Les attaques massives reposent souvent sur une conception individualisée en vue d'atteindre des cibles bien spécifiques[585]. On trouve ainsi des outils pour[586] mener des attaques de type DoS[587], créer des virus informatiques, décrypter une communication chiffrée ou accéder illégalement à un système informatique.

Grâce aux outils logiciels de deuxième génération, qui permettent d'automatiser de nombreux cyberdélits, les pirates peuvent déclencher de multiples attaques sur une courte durée. D'utilisation de plus en plus simple, ces outils offrent en outre à des utilisateurs moins expérimentés la possibilité de commettre des cyberdélits. On peut citer les boîtes à outils permettant à quiconque, ou presque, d'envoyer des courriels de hameçonnage[588] ou encore les programmes de transfert de fichiers vers des serveurs de partage ou depuis ces serveurs. Etant donné qu'il est de plus en plus facile de se procurer ces outils informatiques, le

nombre de cyberdélinquants potentiels a considérablement augmenté. Les initiatives juridiques nationales et internationales contre ces logiciels se multiplient. Elles visent notamment à sanctionner pénalement la production, la vente ou la possession de tels outils[589].

2.9 Infractions combinées

Bibliography (selected): *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001; *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf; *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006; *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001); *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45, page 1033 *et seq.*; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996; *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007; *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27; *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008; *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010; *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

Plusieurs termes servent à décrire des escroqueries complexes relevant de plusieurs types d'infractions. On peut citer le cyberterrorisme, le cyberblanchiment et le hameçonnage.

2.9.1 Cyberterrorisme

Dans les années 90, les attaques par le réseau visant les infrastructures essentielles telles que les transports et les systèmes d'approvisionnement en énergie (« cyberterrorisme ») et l'utilisation des technologies de l'information dans les conflits armés (guerre numérique ou « cyberguerre ») étaient au cœur du débat sur l'utilisation du réseau par les organisations terroristes[590]. Le succès des attaques par virus et par botnet l'a clairement démontré, la sécurité des réseaux n'est pas parfaite. Les terroristes réussissent, on le sait, à mener des attaques via Internet[591], mais il est difficile d'évaluer le niveau de la menace[592]. A noter en outre que le degré d'interconnexion était, à l'époque, faible en regard de ce qu'il est actuellement, ce qui explique très probablement pourquoi si peu d'incidents de ce type étaient signalés (si ce n'est l'intérêt des Etats à ne pas divulguer les attaques qui avaient réussi). A cette époque, les arbres représentaient pour les infrastructures électriques une menace plus sérieuse que les cyberattaques[593].

A la suite des attentats du 11 septembre, la situation a changé. C'est à cette époque qu'ont débuté les discussions intensives sur l'utilisation des TIC par les terroristes[594], sur fond de rapports[595] indiquant qu'Internet avait été utilisé pour préparer les attaques[596]. Il ne s'agissait pas à proprement parler de cyberattaques – étant donné que le groupe responsable des attentats n'avait pas lancé d'attaque sur Internet – mais le réseau avait joué un rôle dans la préparation de l'offensive[597]. Dans ce contexte, les enquêteurs ont mis au jour les différentes façons dont les organisations terroristes utilisent Internet[598]. On sait aujourd'hui que les terroristes utilisent les TIC et Internet pour:

- faire de la propagande
- collecter des informations

- préparer des attaques dans le monde réel
- publier du matériel de formation
- communiquer
- financer le terrorisme
- lancer des attaques contre des infrastructures essentielles.

Cette réorientation du débat a eu un effet positif sur la recherche concernant le cyberterrorisme en cela qu'elle a mis en avant des domaines d'activités terroristes relativement inconnus jusqu'alors. Cela étant, s'il importe assurément d'adopter une démarche exhaustive, les menaces liées aux cyberattaques visant des infrastructures essentielles doivent rester au centre du débat. En effet, étant donné la vulnérabilité des technologies de l'information et la dépendance grandissante[599] à leur égard, il est indispensable d'intégrer cette menace dans les stratégies de prévention et de répression du cyberterrorisme.

Cela étant, malgré des recherches de plus en plus poussées, la lutte contre le cyberterrorisme demeure difficile. Une comparaison des différentes approches nationales fait apparaître de nombreuses similarités[600], ce qui s'explique notamment par le fait que la communauté internationale mesure la nécessité de trouver des solutions mondiales pour lutter contre le terrorisme international[601]. Il est cependant difficile aujourd'hui de savoir si cette approche est satisfaisante ou s'il faut adopter des solutions différentes selon le système juridique et le contexte culturel. Dilemme difficile à trancher, car, mis à part les rapports concernant les incidents majeurs, les analystes scientifiques disposent de très peu de données pour évaluer les différentes solutions. Pour la même raison, il est difficile de déterminer le risque lié à l'utilisation des technologies de l'information par les organisations terroristes. En effet, les rapports étant très souvent classés, seuls les services secrets sont autorisés à les consulter[602]. Pire, il n'existe toujours pas de définition admise par tous du terme « terrorisme »[603]. Ainsi, un rapport du *Congressionnal research Service* (service de recherche du Congrès américain), établi à la demande du Congrès américain, présente l'achat en ligne d'un billet d'avion pour les Etats-Unis par un des terroristes comme une preuve que les terroristes ont utilisé Internet pour préparer leurs attaques[604]. A moins de considérer que tout achat de billet d'avion ne soit un acte lié au terrorisme dès lors qu'il est le fait d'un terroriste, cette explication semble peu solide.

Propagande

En 1998, seules douze des trente organisations terroristes étrangères recensées par le Département d'Etat américain tenaient à jour un site Internet pour informer le public de leurs activités[605]. En 2004, *l'Institute of Peace* (institut pour la paix) des Etats-Unis indiquait que quasiment toutes les organisations terroristes possédaient un site Internet, notamment le Hamas, le Hezbollah, le PKK et Al-Qaïda[606]. Les terroristes ont aussi commencé à utiliser les sites communautaires de partage de vidéos (YouTube par exemple) pour diffuser des messages et faire de la propagande[607]. L'utilisation de sites Internet et autres forums est le signe que, dans leurs rapports avec le public, les groupes subversifs s'orientent de plus en plus vers des méthodes professionnelles[608]. Ils utilisent les sites Internet et autres médias en ligne à des fins diverses: faire de la propagande[609], publier des messages pour justifier leurs activités[610], contacter et recruter[611] des membres, contacter et trouver des donateurs[612]. A noter que les sites Internet ont récemment été utilisés pour diffuser des vidéos d'exécution[613].

Collecte d'informations

Internet regorge d'informations sur des cibles potentielles[614]. Les architectes qui interviennent dans la construction de bâtiments publics mettent souvent les plans des bâtiments en ligne. Plusieurs services Internet offrent aujourd'hui des images satellitaires en haute résolution gratuitement, images que très peu d'institutions militaires dans le monde pouvaient se procurer il y a quelques années[615]. On a en outre découvert des programmes d'apprentissage en ligne expliquant comment fabriquer une bombe et d'autres programmes, sur ce même modèle d'apprentissage, montrant, dans des camps d'entraînement virtuels, comment manier les armes[616]. Par ailleurs, certaines informations sensibles ou confidentielles insuffisamment protégées des robots de recherche sont accessibles via des moteurs de recherche[617]. En 2003, le Département de la Défense américain a été informé qu'un manuel de formation lié à Al-Qaïda

indiquait qu'il était possible de trouver des informations sur des cibles potentielles en utilisant des sources publiques[618]. En 2006, le New York Times signalait que des informations essentielles concernant la construction d'armes nucléaires étaient disponibles sur un site Internet du gouvernement, informations prouvant que l'Irak avait l'intention de développer des armes nucléaires[619]. Un incident analogue a été signalé en Australie: des sites Internet du gouvernement contenaient des informations détaillées sur des cibles potentielles d'attaques terroristes[620]. En 2005, selon la presse allemande, des enquêteurs ont découvert que des manuels sur la fabrication d'explosifs avaient été téléchargés sur les ordinateurs de deux suspects, qui étaient accusés de tentative d'attaque à la bombe artisanale contre les transports publics[621].

Préparation d'attaques dans le monde réel

Les terroristes peuvent utiliser les technologies de l'information pour préparer leurs attaques de différentes façons. On peut citer, à titre d'exemple, l'envoi de courriels ou l'utilisation de forums, méthodes qui sont examinées dans la partie consacrée à la communication. D'autres méthodes plus directes sont visées ici. Les jeux en ligne, par exemple, seraient utilisés pour préparer des attaques terroristes[622]. Plusieurs de ces jeux permettent de simuler le monde réel à l'aide de personnages (avatars) agissant dans un monde virtuel. Ces jeux pourraient, en principe, servir à simuler des attaques, mais il est difficile de savoir si c'est déjà le cas[623].

Publication de matériel de formation

Internet peut être utilisé pour diffuser du matériel de formation, par exemple sur le maniement des armes ou le choix des cibles. Ce type de matériel est très largement disponible en ligne[624]. En 2008, les services secrets occidentaux ont découvert un serveur Internet permettant d'échanger du matériel de formation et de communiquer[625]. On a en outre signalé plusieurs sites mis en place par des organisations terroristes pour coordonner leurs activités[626].

Communication

Les organisations terroristes n'utilisent pas les technologies de l'information uniquement pour créer des sites Internet et faire des recherches dans des bases de données. Il a ainsi été rapporté, dans le contexte des enquêtes menées à la suite des attentats du 11 septembre, que les terroristes avaient communiqué par courriel pour coordonner leurs attaques[627] et, selon la presse, pour échanger des instructions détaillées concernant les cibles et le nombre d'attaquants[628]. A noter par ailleurs que les terroristes ont recours à des technologies de chiffrement et des moyens de communication anonymes, ce qui complique le travail d'identification et de surveillance.

Financement du terrorisme

La plupart des organisations terroristes sont tributaires de ressources financières apportées par des tiers. Depuis les attentats du 11 septembre, l'une des lignes stratégiques majeures de la lutte contre le terrorisme est de déterminer l'origine de ces transactions financières. L'une des principales difficultés tient au fait que les ressources financières requises pour mener les attaques ne sont pas nécessairement élevées[629]. Internet peut être utilisé de diverses façons pour financer le terrorisme. Les organisations terroristes peuvent solliciter des donations en ligne par paiement électronique[630] ou indiquer sur le site les modalités de donation (le site de l'organisation « Hizb al-Tahrir » fournit par exemple les coordonnées d'un compte bancaire à l'usage des donateurs potentiels)[631]. Une autre approche consiste à mettre en place des donations avec paiement en ligne par carte de crédit. L'IRA (*Irish Republican Army*, armée républicaine irlandaise) a été l'une des premières organisations terroristes à proposer ce mode de donation[632]. Ces deux approches présentent cependant le risque que les informations publiées sur les sites ne soient découvertes et utilisées pour déterminer l'origine des transactions. Il est donc vraisemblable que les organisations auront de plus en plus recours aux systèmes de paiement électronique anonymes. Pour ne pas attirer l'attention, elles tentent parfois de dissimuler leurs activités en passant par des intervenants au-dessus de tout soupçon (organisations caritatives par exemple). Autre approche fondée sur Internet, le financement par de fausses boutiques en ligne. De création relativement simple, la boutique en ligne présente l'avantage majeur d'être accessible en tout point du globe. De plus, il est assez difficile de prouver que des transactions financières effectuées sur ces sites ne correspondent pas à des achats ordinaires mais à des donations. En

effet, il faudrait pour cela enquêter sur chaque transaction, ce qui peut se révéler difficile si la boutique est gérée à partir d'un autre pays ou si elle a recours à des systèmes de paiement anonymes[633].

Attaques visant des infrastructures essentielles

Les infrastructures essentielles de l'information, cibles de cyberdélits ordinaires tels que la fraude et le vol d'identité, pourraient aussi devenir la cible des organisations terroristes. Du fait de leur dépendance grandissante à l'égard des technologies de l'information, les infrastructures essentielles sont plus vulnérables aux attaques[634]. C'est tout particulièrement le cas des systèmes interconnectés par des réseaux informatiques et des réseaux de communication[635]. En effet, une attaque perpétrée via un réseau crée des perturbations beaucoup plus étendues que la mise hors service d'un système isolé. Des interruptions de service, même de courte durée, peuvent entraîner de lourdes pertes financières. Les services civils (entreprises de commerce électronique, etc.) ne sont pas les seuls concernés, les infrastructures et les services de l'armée sont aussi en danger[636]. Les enquêtes sur ces attaques, mais aussi leur prévention, présentent des difficultés bien spécifiques[637]. En effet, contrairement aux attaques physiques, les cyberattaques ne nécessitent pas la présence des attaquants sur les lieux qui sont ciblés[638]. De plus, les attaquants peuvent utiliser des moyens de communication anonymes et des technologies de chiffrement pour cacher leur identité[639]. Comme indiqué précédemment, pour enquêter sur de telles attaques, il faut disposer de moyens spéciaux: instruments de procédure, technologies d'investigation, personnel spécialement formé[640].

Les infrastructures essentielles sont, par définition, un élément vital de la durabilité et de la stabilité d'un Etat; il est donc communément admis qu'elles représentent une cible potentielle des attaques terroristes[641]. On appelle infrastructure essentielle une infrastructure dont la mise hors d'usage ou la destruction aurait pour effet de fragiliser la défense ou la sécurité économique d'un Etat[642]. Ces infrastructures comprennent notamment les systèmes d'alimentation en énergie, les systèmes de télécommunication, le transport et les réserves de gaz et de pétrole, le système bancaire et financier, les transports, les systèmes d'alimentation en eau et les services d'urgence. La gravité des perturbations causées par l'interruption des services civils après le passage de l'ouragan Katrina aux Etats-Unis montre bien la dépendance de la société à l'égard de ces services[643]. Le logiciel malveillant « Stuxnet » illustre parfaitement la menace que représentent désormais les attaques menées à l'aide d'Internet qui ciblent les infrastructures essentielles[644]. En 2010, une société biélorusse spécialisée dans la sécurité a découvert un nouveau logiciel malveillant[645]. L'étude des manipulations causées par le logiciel, de son concepteur et de ses motivations se poursuit et tous les faits n'ont pas encore été découverts, loin s'en faut, notamment en ce qui concerne les attributions et les motivations du concepteur[646]. Toutefois, en ce qui concerne plus particulièrement le fonctionnement du logiciel, il semble que l'on dispose désormais d'informations factuelles importantes:

Ce logiciel complexe, doté de plus de 4 000 fonctions[647], semblait cibler les systèmes de contrôle industriels (ICS)[648] – notamment ceux produits par la société technologique Siemens[649]. Il était diffusé par le biais de disques amovibles et utilisait quatre exploits « zero-day » pour infecter les systèmes informatiques[650]. Des ordinateurs infectés ont notamment été signalés en Iran, en Indonésie et au Pakistan, mais également aux Etats-Unis et dans certains pays européens[651]. Bien que le logiciel malveillant soit souvent caractérisé par le recours à une technologie hautement sophistiquée, certaines études remettent en question ce degré de sophistication[652].

Comme indiqué précédemment, déterminer l'attribution ou les motivations du délinquant s'avère encore plus complexe et implique un fort degré d'incertitude. Selon certains médias ou études, le logiciel aurait ciblé les installations d'enrichissement en uranium d'Iran et retardé la mise en œuvre du programme nucléaire du pays[653].

On peut tirer deux principales conclusions de la découverte de ce logiciel malveillant. Premièrement, l'incident souligne le fait que l'infrastructure essentielle dépend fortement de la technologie informatique et que les attaques sont possibles. Ensuite, comme en témoigne la diffusion du logiciel par le biais de disques amovibles, le seul fait de déconnecter un système informatique du réseau ne peut empêcher les attaques.

La dépendance des infrastructures essentielles vis-à-vis des TIC s'étend au-delà de l'industrie de l'énergie et du nucléaire. Les incidents suivants survenus dans le transport aérien, qui, dans la plupart des pays, est également considéré comme une infrastructure essentielle, attestent de cette vulnérabilité aux attaques par le réseau. Les systèmes d'enregistrement peuvent faire l'objet d'une attaque. Ceux de la plupart des aéroports du monde reposent déjà sur des systèmes informatiques interconnectés[654]. En 2004, le ver informatique Sasser[655] a infecté des millions d'ordinateurs dans le monde, notamment ceux de grandes compagnies aériennes, entraînant l'annulation de plusieurs vols[656].

Les systèmes de billetteries en ligne représentent également une cible potentielle. Aujourd'hui, un nombre conséquent de billets sont achetés en ligne. Les compagnies aériennes s'appuient sur les technologies de l'information pour effectuer diverses opérations. Toutes les grandes compagnies aériennes proposent aujourd'hui à leurs clients d'acheter leurs billets en ligne. Au même titre que d'autres activités de commerce électronique, ces opérations en ligne peuvent être la cible de malfaiteurs. L'attaque par refus de service (DoS) est l'une des techniques classiques utilisées par les cyberdélinquants pour perturber les services reposant sur Internet[657]. En 2000, en un court laps de temps, plusieurs attaques DoS ont ainsi été lancées contre des entreprises connues telles que CNN, eBay et Amazon[658], rendant certains services indisponibles pendant plusieurs heures, voire plusieurs jours[659]. Certaines compagnies aériennes ont également été touchées par des attaques DoS. En 2001 par exemple, le site Internet de la Lufthansa a été la cible d'une attaque de ce type[660].

Autre cible potentielle des attaques en ligne contre des infrastructures essentielles du transport aérien, les systèmes informatiques de contrôle des aéroports. La vulnérabilité de ces systèmes a été mise en évidence par une attaque perpétrée contre l'aéroport de Worcester aux Etats-Unis en 1997[661], pendant laquelle l'auteur a réussi à désactiver les services téléphoniques vers la tour de contrôle ainsi que le système de commande des feux de balisage des pistes[662].

2.9.2 Guerre numérique ou « cyberguerre »

Suite aux attaques lancées contre des systèmes informatiques en Estonie en 2007 et en Géorgie en 2008, et à la découverte du virus informatique « Stuxnet »[663], le terme « cyberguerre » a fréquemment été employé pour décrire ce type de situation bien que, comme expliqué ci-dessous, le choix de la terminologie employée reste problématique.

Terminologie et définitions

Il n'existe pas de terminologie cohérente, pas plus qu'une définition largement admise du terme « guerre informatique » (*cyberwarfare*). D'autres termes utilisés recouvrent la guerre de l'information, la guerre électronique, la cyberguerre, la guerre du net, les opérations sur informations[664]. En règle générale, ces termes sont employés pour désigner l'utilisation des TIC et d'Internet pour mener une guerre. Des définitions plus restrictives désignent ces activités comme une mesure de conflit armé axée sur la gestion et l'utilisation des informations sous toutes leurs formes et à tous les niveaux pour obtenir un avantage militaire décisif, notamment au sein d'un environnement conjoint et combiné[665]. D'autres définitions, plus larges, couvrent les conflits électroniques dans le cadre desquels les informations représentent un actif précieux, objet de conquête ou de destruction[666].

Evolution du débat

Depuis des décennies, ce thème est au cœur des débats et des controverses[667]. L'attention portait à l'origine sur la substitution des actes de guerre classiques par des attaques promues ou menées à l'aide du réseau[668]. A cet égard, la capacité de neutraliser un ennemi sans être impliqué dans un combat a toujours occupé une place majeure au sein du débat[669]. En outre, les attaques basées sur le réseau sont généralement moins coûteuses que des opérations militaires traditionnelles[670] et sont à la portée des petits Etats comme des grands. En dépit de certains cas concrets fréquemment cités, les principaux aspects du débat restent largement hypothétiques[671]. Les deux exemples les plus fréquemment mentionnés sont les attaques informatiques lancées contre l'Estonie et la Géorgie. La classification d'une attaque en tant qu'acte de guerre nécessite toutefois que certains critères soient satisfaits.

En 2007, l'Estonie a vu naître un débat houleux, y compris des manifestations organisées dans la capitale, concernant le retrait d'un mémorial de la deuxième guerre mondiale[672]. Outre les moyens de protestation traditionnels, l'Estonie a découvert plusieurs vagues d'attaques informatiques lancées contre les sites du gouvernement et des entreprises privées et les services en ligne[673], dont la défiguration de certains sites Web[674], des attaques lancées contre des serveurs de noms de domaines et des attaques par refus de service distribué (DDoS) impliquant l'utilisation de botnets[675]. S'agissant de ces dernières, les experts ont par la suite expliqué que la réussite des attaques contre le site Web officiel des organismes gouvernementaux d'Estonie[676] ne peut s'expliquer que par l'inadéquation des mesures de protection[677]. L'impact de ces attaques, ainsi que leur origine, ont par la suite fait l'objet d'une controverse. Tandis que d'après les journaux[678] et les revues spécialisées[679] les attaques ont failli mettre hors service l'infrastructure numérique du pays, des études plus fiables révèlent que l'impact des attaques est resté limité aussi bien en termes de nombre d'ordinateurs concernés que de durée de l'indisponibilité des services[680]. Un débat analogue a pris place quant à l'origine des attaques. Si, durant l'attaque, on a rapporté que le territoire de la Fédération russe était l'origine des faits[681], une analyse des attaques a révélé qu'elles impliquaient en réalité plus de 170 pays[682]. Même lorsque les motivations sont d'ordre politique, une attaque ne constitue pas nécessairement un acte de guerre. Le cas de l'Estonie doit donc être exclu de la liste. Bien qu'il s'agisse d'attaques informatiques lancées contre les sites du gouvernement et des entreprises privés et les services en ligne[683], y compris la défiguration de certains sites[684], et d'attaques par refus de service distribué (DDoS)[685], elles ne peuvent être qualifiées de guerres électroniques, puisqu'elles n'impliquent pas un acte de force et n'interviennent pas pendant un conflit entre deux Etats souverains.

Des deux attaques mentionnées précédemment, celle de 2008 ciblant les systèmes informatiques de Géorgie est celle qui se rapproche le plus des actes de guerre. Dans le contexte d'un conflit armé traditionnel[686] entre la Fédération russe et la Géorgie, plusieurs attaques informatiques ciblant les sites Web du gouvernement et des entreprises[687] (y compris par le biais de la défiguration de certains sites et d'attaques par refus de service distribué) ont été découvertes[688]. A l'instar des incidents survenus en Estonie, l'origine de l'attaque contre la Géorgie a provoqué par la suite de nombreux débats. Bien que certains journaux[689] semblent être en mesure de révéler l'origine géographique de l'attaque, les études technologiques soulignent l'utilisation de botnets, des dispositifs qui compliquent la détermination d'une telle origine[690]. Cette incertitude, associée au fait que les actes découverts diffèrent considérablement des actes de guerre traditionnels, permet difficilement de les qualifier de guerres électroniques.

Bien que l'importance du débat entourant ce phénomène soit difficilement contestable, il convient de noter que ces attaques ne constituent pas un phénomène sans précédent. La propagande est diffusée par Internet et les attaques contre les systèmes informatiques des alliances militaires sont monnaie courante. Pendant la guerre de Yougoslavie, des attaques contre les systèmes informatiques de l'OTAN, provenant de Serbie, ont été découvertes[691]. En réponse, les Etats membres de l'OTAN auraient été impliqués dans des attaques de même nature, lancées contre des systèmes informatiques de Serbie[692]. D'autres activités de propagande sur Internet et d'autres formes d'actions psychologiques (PSYOPS) conçues pour influencer l'ennemi ont été largement utilisées[693].

Importance de la distinction

Les actes liés à l'état de guerre présentent de nombreuses similitudes avec d'autres formes d'abus des TIC, telles que la cybercriminalité et l'utilisation d'Internet à des fins terroristes. Par conséquent, les termes « cybercriminalité », « utilisation d'Internet à des fins terroristes » et « guerre de l'information » sont souvent utilisés de manière interchangeable. Mais, puisque les cadres juridiques applicables diffèrent de façon significative, il est très important de faire une distinction entre ces termes. Alors que la cybercriminalité est généralement traitée par des actes juridiques visant à pénaliser ces comportements, les règles et les procédures ayant trait à la guerre de l'information sont largement réglementées par le droit international, et en particulier par la Charte des Nations Unies.

2.9.3 Cyberblanchiment

En 2013, l'arrêt des activités du fournisseur de monnaie électronique "Liberty Reserve" a fait les gros titres.[694] Avec un montant estimé à 6 milliards USD, il pourrait s'agir de la plus grosse affaire de

cyberblanchiment de tous les temps.[695] En 2013, le département du Trésor des États-Unis a publié les conclusions détaillées relatives à cette affaire.[696] Internet est en train de transformer le blanchiment de capitaux. Si les techniques traditionnelles de blanchiment présentent toujours un certain intérêt pour les sommes importantes, Internet apporte plusieurs avantages. Les services financiers en ligne offrent la possibilité d'effectuer des transactions financières multiples dans le monde entier très rapidement. Internet a contribué à surmonter la dépendance envers les opérations monétaires physiques. Première étape dans la suppression de la dépendance physique à l'argent, les virements bancaires ont remplacé le transport d'argent liquide, mais des règlementations plus strictes pour détecter les transferts suspects ont poussé les délinquants à élaborer de nouvelles techniques. La détection des transactions suspectes dans la lutte contre le blanchiment d'argent est basée sur des obligations imposées aux institutions financières impliquées dans les transferts. [697]

Le blanchiment de capitaux s'effectue généralement en trois phases: le placement, l'empilage et l'intégration.

S'agissant du placement d'importantes sommes en liquide, l'utilisation d'Internet ne présente peut-être pas tant d'avantages concrets.[698] Toutefois, le recours à Internet est surtout intéressant pendant la phase d'empilage (masquage). Dans ce contexte, la suspicion de blanchiment d'argent est particulièrement difficile lorsque les blanchisseurs de capitaux utilisent des cybercasinos pour l'empilage.[699]

La réglementation des transactions financières est aujourd'hui relativement limitée et Internet offre aux délinquants la possibilité d'effectuer, pour un coût modique, des virements non imposables entre plusieurs pays. Les difficultés actuelles pour enquêter sur les techniques de blanchiment d'argent basées sur Internet découlent souvent de l'utilisation de monnaies virtuelles et de cybercasinos.

Utilisation des monnaies virtuelles

L'un des moteurs clés du développement des monnaies virtuelles a été les micropaiements (pour le téléchargement d'articles en ligne coûtant moins de 0,10 USD par exemple), pour lesquels l'utilisation des cartes de crédit est problématique. Face à la demande croissante de micropaiements, des monnaies virtuelles, y compris des monnaies virtuelles « or », ont été mises en place. Les monnaies virtuelles « or » sont des systèmes de paiement reposant sur des comptes dont la valeur est gagée sur des réserves d'or. L'ouverture de comptes *e-gold* s'effectue en ligne, souvent sans inscription préalable. Certains prestataires proposent même des services de virement en *peer-to-peer* (de personne à personne) et de retrait en liquide.[700] Les cyberdélinquants peuvent ouvrir des comptes *e-gold* dans plusieurs pays et les associer, brouillant ainsi les instruments financiers servant au blanchiment de capitaux et au financement du terrorisme. Par ailleurs, certains délinquants ouvrent des comptes en fournissant des renseignements inexacts de façon à masquer leur identité.[701]

Outre les monnaies virtuelles simples, il existe également des monnaies qui combinent le caractère virtuel et l'anonymat. À titre d'exemple on peut citer le *Bitcoin*, une monnaie virtuelle utilisant la technologie peer-to-peer.[702] Bien qu'il s'agisse de systèmes décentralisés ne nécessitant aucun intermédiaire central pour garantir la validité des autorités de transactions, les attaques réussies commises au cours de l'année 2011 démontrent la vulnérabilité/les risques liés à ces monnaies virtuelles décentralisées.[703] Lorsque ce genre de monnaie anonyme est utilisée par des criminels, cela limite la capacité d'identification des suspects par les agences de répression en suivant les transferts d'argent[704] – par exemple dans des cas ayant trait à la pédopornographie commerciale.[705]

Utilisation des casinos en ligne

La création d'un casino en ligne ne nécessite pas, contrairement à la création d'un casino réel, de gros investissements financiers.[706] De plus, les réglementations relatives aux casinos en ligne et hors ligne diffèrent souvent selon les pays.[707] Déterminer l'origine des virements et prouver que certains fonds ne sont pas des gains de jeux, mais correspondent en réalité à des capitaux blanchis, n'est possible que si les casinos consignent leurs transactions et les communiquent aux services de répression.

Les réglementations juridiques actuelles relatives aux services financiers en ligne ne sont pas aussi strictes que les réglementations financières traditionnelles. Outre les lacunes législatives, les difficultés de

réglementation s'expliquent par la difficulté à contrôler l'identité des clients, car la fiabilité de la vérification peut être compromise si le prestataire de services financiers et le client ne se rencontrent jamais.[708] Par ailleurs, l'absence de contact en face à face rend difficile l'application des procédures traditionnelles, qui reposent sur la connaissance du client. En outre, les transferts par Internet impliquent souvent la participation transfrontalière de prestataires situés dans différents pays. Enfin, le contrôle des transactions s'avère particulièrement difficile lorsque les prestataires autorisent leurs clients à effectuer des transferts de valeurs selon un modèle *peer-to-peer*.

2.9.4 Hameçonnage

Pour obtenir des informations personnelles sur les utilisateurs, les cyberdélinquants ont mis au point différentes techniques, qui vont des logiciels espions [709] aux attaques par « hameçonnage ». [710] L'« hameçonnage » décrit les actes commis dans le but d'amener les victimes à révéler des informations personnelles ou confidentielles.[711] On distingue plusieurs types d'attaques par hameçonnage,[712] dont l'hameçonnage par courriel, qui comprend trois grandes phases. Au cours de la première phase, les cyberdélinquants identifient des sociétés légitimes qui proposent des services en ligne et communiquent par voie électronique avec des clients ciblés, par exemple des institutions financières. Ils créent ensuite des sites Internet qui ressemblent aux sites légitimes de ces sociétés. Ces sites demandent aux victimes de s'identifier de manière classique et collectent, ce faisant, des informations personnelles sur les clients (numéros de compte, mots de passe pour les opérations bancaires en ligne, etc.).

Pour les orienter vers ces sites d'espionnage, les cyberdélinquants envoient aux internautes des courriels qui ressemblent à ceux normalement émis par les sociétés légitimes,[713] commettant souvent par là même une violation de la marque commerciale.[714] Dans le faux courriel, il est demandé au destinataire de se connecter au site pour des motifs de mise à jour ou de contrôle de sécurité, quelquefois assorti de menaces s'il refuse de coopérer (fermeture de compte par exemple). Pour orienter la victime vers le site d'espionnage, ce faux courriel contient généralement un lien sur lequel la victime doit cliquer, et ce, afin d'éviter qu'elle ne saisisse manuellement l'adresse Internet correcte de l'établissement. Les cyberdélinquants ont mis au point des techniques sophistiquées afin de s'assurer que l'utilisateur ne réalise pas qu'il n'est pas connecté au site authentique.[715]

Dès que les données personnelles sont divulguées, les cyberdélinquants se connectent au compte de la victime et effectuent des opérations frauduleuses telles que des virements, des demandes de passeport ou d'ouverture de compte, etc. Le nombre croissant d'attaques réussies montre bien le potentiel de cette technique.[716] Plus de 55 000 sites d'hameçonnage ont été signalés à l'APWG [717] en avril 2007.[718] En janvier 2014, le nombre de sites d'hameçonnage détectés est passé à près de 43 000. [719] Les techniques d'hameçonnage ne servent pas uniquement à se procurer des mots de passe pour effectuer des opérations bancaires en ligne, mais aussi à obtenir des codes d'accès à des systèmes informatiques ou à des plates-formes d'enchères ainsi que des numéros de sécurité sociale, éléments d'identification particulièrement importants aux États-Unis, qui peuvent servir à commettre des infractions de type « vol d'identité ».[720]

[87] Other terminology used includes information technology crime and high-tech crime. See, in this context: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No. 2, page 144.

[88] Regarding approaches to define and categorize cybercrime, see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the Council of Europe Convention on Cybercrime, No. 8; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf; Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at: www.aph.gov.au/Senate/Committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1.

[89] *Nhan/Bachmann* in Maguire/Okada (eds), Critical Issues in Crime and Justice, 2011, page 166

[90] Regarding this relationship, see also: *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004, page 86.

[91] Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

[92] With regard to the definition, see also: *Kumar*, Cyber Law, A view to social security, 2009, page 29.

[93] See, for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 *et seq.*; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

[94] The Stanford Draft International Convention was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Stanford Draft is published in: The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[95] *Arti*cle 1, Definitions and Use of Terms,

For the purposes of this Convention:

1. "cyber crime" means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;

[...]

[96] See: *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[97] *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

[98] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on

Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq.*

[99] Universal serial bus (USB)

[100] Article 4 – Data Interference:

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

[101] For difficulties related to the application of a cybercrime definition to real-world crimes, see: *Brenner*, Cybercrime Metrics: Old Wine, New Bottles?, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

[102] In civil law countries, the use of such a legal term could lead to conflicts with the principle of certainty..

[103] Some of the most well-known cybercrime offences are illegal access, illegal interception of computer data, data interference, computer-related fraud, computer-related forgery, dissemination of child pornography. For an overview see: *Sieber*, Council of Europe Organised Crime Report 2004; ABA International Guide to Combating Cybercrime, 2002; *Williams*, Cybercrime, 2005, in Miller, Encyclopaedia of Criminology.

[104] *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

[105] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. Regarding the Convention on Cybercrime see: *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[106] The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[107] Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences, see below: § 6.2.

[108] Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences, see below: § 6.2.

[109] Art. 9 (Offences related to child pornography). For more information about the offences, see below: § 6.2.

[110] Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences, see below: § 6.2.

[111] See below: § 2.5.

[112] See below: § 2.6.

[113] See below: § 2.7.

[114] See below: § 2.8.

[115] See below: § 2.9.1

[116] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

[117] Regarding the related challenges, see: *Slivka/Darrow*; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, page 217 *et seq.*

[118] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[119] See: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[120] *Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman*, Report of the Committee on the Preservation and Use of Economic Data, 1965, available at: www.archive.org/details/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965.

[121] *Miller*, The Assault on Privacy-Computers, 1971.

[122] *Westin/Baker*, Data Banks in a Free Society, 1972.

[123] For an overview about the debate in the US and Europe, see: *Sieber*, Computer Crime and Criminal Law, 1977.

[124] *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 48.

[125] *Stevens*, Identifying and Charging Computer Crimes in the Military, Military Law Review, Vol. 110, 1985, page 59.

[126] *Gemignani*, Computer Crime: The Law in '80, Indiana Law Review, Vol. 13, 1980, page 681.

[127] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[128] For an overview about cases see: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[129] *Freed*, Materials and cases on computer and law, 1971, page 65.

[130] *Bequai*, The Electronic Criminals – How and why computer crime pays, Barrister, Vol. 4, 1977, page 8 *et seq.*

[131] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, page 225 *et seq.*; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

[132] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Bequai*, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, page 22.

[133] *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 527.

[134] Regarding the number of the cases in early cybercrime investigations, see: *Schjolberg*, Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, page 6, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

[135] *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 58, Notes – A Suggested Legislative Approach to the Problem of Computer Crime, Washington and Lee Law Review, 1981, page 1173.

[136] *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976.

[137] Federal Computer Systems Protection Act of 1977. For more information, see: *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 2, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf; *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 531.

[138] Third Interpol Symposium on International Fraud, France 1979.

[139] Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, page 73.

[140] *BloomBecker*, The Trial of Computer Crime, Jurimetrics Journal, Vol. 21, 1981, page 428; *Schmidt*, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, Vol. 21, 1981, 345 *et seq.*; *Denning*,

Some Aspects of Theft of Computer Software, Auckland University Law Review, Vol. 4, 1980, 273 *et seq.*; *Weiss*, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983, page 1 *et seq.*; *Bigelow*, The Challenge of Computer Law, Western England Law Review, Vol. 7, 1985, page 401; *Thackeray*, Computer-Related Crimes, Jurimetrics Journal, 1984, page 300 *et seq.*

141 *Andrews*, The Legal Challenge Posed by the new Technology, Jurismetrics Journal, 1983, page 43 *et seq.*

142 *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

143 *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

144 *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 4, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

145 Computer-related criminality: Analysis of Legal Politics in the OECD Area, 1986.

146 Computer-related crime: Recommendation No. R. (89) 9.

147 Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

148 Regarding the impact of the speed of data exchange on cybercrime investigation, see: § 3.2.10.

149 Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

150 A/RES/45/121 adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm

151 UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at: www.uncjin.org/Documents/EighthCongress.html.

152 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. For more information, see: § 2.9.4.

153 Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

154 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006.

155 *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

156 See for example: Big Data for Development: Challenges & Opportunities, UN Global Pulse, 2012; *Sircar*, Big Data: Countering Tomorrow's Challenges, Infosys Labs Briefings, Vol. 11, No. 1, 2013;

157 *Hartmann/Steup,* The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment, published in Podins/Stinissen/Maybaum, 5th International Conference on Cyber Conflicts, 2013; *Kim/Wampler/Goppert/Hwang/Aldridge,* Cyber attack vulnerabilities analysis for unanned areal vehicles, American Institute of Aeronautics and Astronautics, 2012.

158 *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

159 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

160 Regarding the emerging importance of crime statistics, see: *Osborne/Wernicke*, Introduction to Crime Analysis, 2003, page 1 *et seq.*, available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

161 2013 Internet Crime Report , Internet Crime Complaint Center, 2014, available at: www.ic3.gov/media/annualreport/2013_IC3Report.pdf.

162 German Crime Statistics 2013, available at www.bka.de. As this number also includes traditional crimes that involved Internet technology at any stage of the offence, the increase of cases cannot necessarily be used to determine the specific development in the typology-based crime fields.

[163] Regarding the related difficulties, see: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 229, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[164] Regarding challenges related to crime statistics in general, see: *Maguire* in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 *et seq.* available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf.

[165] See in this context: Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009, page 9, available at: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

[166] *Alvazzi del Frate*, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

[167] Computer Crime, Parliamentary Office of Science and Technology, Postnote No. 271, Oct. 2006, page 3.

[168] Regarding the related challenges, see: *Kabay*, Understanding Studies and Surveys of Computer Crime, 2009, available at: www.mekabay.com/methodology/crime_stats_methods.pdf.

[169] The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, – available at: www.heise-security.co.uk/news/80152. See also: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, page 660.

[170] See *Mitchison/Urry*, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[171] See *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; *Smith*, Investigating Cybercrime: Barriers and Solutions, 2003, page 2, available at: www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

[172] In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp.

[173] See SOCA, International crackdown on mass marketing fraud revealed, 2007, available at: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[174] In the 2006 NW3C Internet Crime report, only 1.7 per cent of the reported total USD losses were related to the Nigerian Letter Fraud, but those cases that were reported had an average loss of USD 5 100 each. The number of reported offences is very low, while the average loss of those offences is the high.

[175] With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29..

[176] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[177] See in this context: *Hyde-Bales/Morris/Charlton*, The police recording of computer crime, UK Home Office Development and Practice Report, 2004.

[178] Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport, page 15.

[179] National Fraud Information Center, 2007 Internet Fraud Statistics, 2008, available at: www.fraud.org/internet/intstat.htm.

[180] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report.

[181] 2nd ISSA/UCD Irish Cybercrime Survey, 2008, available at: www.issaireland.org/2nd%20ISSA%20UCD%20Irish%20Cybercrime%20Survey%20-%20Results%2017DEC08.pdf.

[182] Symantec Intelligence Quarterly, April-June 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport.

[183] 2010 CSO CyberSecurity Watch Survey, 2010.

[184] 2008 CSI Computer Crime and Security Survey, 2009, page 15.

[185] Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at: www.symantec.com/business/theme.jsp?themeid=threatreport, page 7,

[186] Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 2.

[187] Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 8.

[188] Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 8.

[189] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

[190] Goodin, PlayStation Network breach will cost Sony $ 171m, The Register, 24.05.2011, available at: www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/.

[191] See 2005 FBI Computer Crime Survey, page 10.

[192] See: § 2.4.

[193] *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62; ECPAT, Violence against Children in Cyberspace, 2005, page 54; Council of Europe Organized Crime Situation Report 2005, Focus on Cybercrime, page 41.

[194] *Bialik*, Measuring the Child-Porn Trade, The Wall Street Journal, 18.04.2006.

[195] Computer Security Institute (CSI), United States.

[196] The CSI Computer Crime and Security Survey 2007 is available at: www.gocsi.com/

[197] See CSI Computer Crime and Security Survey 2007, page 1, available at: www.gocsi.com/. Having regard to the composition of the respondents, the survey is likely to be relevant for the United States only.

[198] With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22, available at: www.gao.gov/new.items/d07705.pdf. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[199] See below: § 2.4.

[200] Regarding the development of computer systems, see: *Hashagen*, The first Computers – History and Architectures.

[201] See in this context, for example, the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

[202] From a legal perspective, there is no real need to differentiate between "computer hackers" and "computer crackers" as – in the context of illegal access – both terms are used to describe persons who enter a computer system without right. The main difference is the motivation. The term "hacker" is used to describe a person who enjoys exploring the details of programmable systems, without breaking the law. The term "cracker" is used to describe a person who breaks into computer systems in general by violating the law.

[203] In the early years of IT development, the term "hacking" was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term "hacking" was often used to describe a constructive activity.

[204] See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61; *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*.

[205] See the statistics provided by HackerWatch. The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported; *Biegel,* Beyond our Control? The Limits

of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.* in the month of August 2007. Source: www.hackerwatch.org.

206 For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 *et seq.*; Regarding the impact, see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.*

207 *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

208 *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

209 *Sieber*, Council of Europe Organised Crime Report 2004, page 66.

210 *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

211 Hacking into a computer system and modifying information on the first page to prove the ability of the offender can – depending on the legislation in place – be prosecuted as illegal access and data interference. For more information, see below: § 6.2.1 and § 6.2.4.

212 The term "hacktivism" combines the words hack and activism. It describes hacking activities performed to promote a political ideology. For more information, see: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf. Regarding cases of political attacks, see: *Vatis*, cyberattacks during the war on terrorism: a predictive analysis, available at: www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

213 A hacker left messages on the website that accused the United States and Israel of killing children. For more information, see BBC News, "UN's website breached by hackers", available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm

214 The abuse of hacked computer systems often causes difficulties for law-enforcement agencies, as electronic traces do not often lead directly to the offender, but first of all to the abused computer systems.

215 Regarding different motivations and possible follow-up acts, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1;

216 The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: www.hackerwatch.org.

217 Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.

218 See Heise News, Online-Computer werden alle 39 Sekunden angegriffen, 13.02.2007, available at: www.heise.de/newsticker/meldung/85229. The report is based on an analysis from Professor Cukier..

219 For an overview of examples of successful hacking attacks, see http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

220 Regarding threats from Cybercrime toolkits, see Opening Remarks by ITU Secretary-General, 2nd Facilitation Meeting for WSIS Action Line C5, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/sg-opening-remarks-14-may-2007.pdf. See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 29, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

221 For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

222 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

223 Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

224 For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[225] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9, available at: www.212cafe.com/download/e-book/A.pdf.

[226] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

[227] For an overview of the tools used to perform high-level attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; *Erickson*, Hacking: The Art of Exploitation, 2003.

[228] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: § 3.2.9.

[229] See *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[230] See in this context Art. 2, sentence 2, Convention on Cybercrime.

[231] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

[232] One example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a) until 2007, when the provision was changed. The following text is taken from the old version of Section 202a – Data Espionage:

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

[233] With regard to targeted attacks see for example: *Sood/Enbody*, Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, 2010. With regard to trends towards targeted attack see: Blurring Boundaries, Trend Micro Security Predictions for 2014 and Beyond, Trend Micro, 2014.

[234] With regard to details related to the damage of targeted attacks see: *Kaspersky*, IT Security Risks Survey 2014.

[235] Targeted Cyber Attacks, GFI White Paper, 2009, page 5.

[236] For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq.*; *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[237] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

[238] For more information about that case, see: *Stoll*, Stalking the wily hacker, available at: http://pdf.textfiles.com/academics/wilyhacker.pdf; *Stoll*, The Cuckoo's Egg, 1998.

[239] See *Sieber*, Council of Europe Organised Crime Report 2004, page 88 *et seq.*; *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[240] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

[241] Examples are software tools that are able to break passwords. Another example is a software tool that records keystrokes (keylogger). Keyloggers are available as software solutions or hardware solutions.

[242] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[243] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[244] For more information, see *Mitnick/Simon/Wozniak*, The Art of Deception: Controlling the Human Element of Security.

[245] See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See: *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at:

www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

246 Regarding the elements of an Anti-Cybercrime Strategy, see below: § 4.

247 "Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems" – See OECD Guidelines for Cryptography Policy, V 2, available at: www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

248 Physical research proves that it can take a very long time to break encryption, if proper technology is used. See *Schneier*, Applied Cryptography, page 185. For more information regarding the challenge of investigating cybercrime cases that involve encryption technology, see below: § 3.2.14.

249 The Council of Europe Convention on Cybercrime contains no provision criminalizing data espionage.

250 Regarding the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq.*

251 Regarding the impact of this behaviour for identity theft, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

252 *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

253 See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

254 See *Hackworth*, Sypware, Cybercrime & Security, IIA-4. Regarding user reactions to the threat of spyware, see: *Jaeger/ Clarke*, The Awareness and Perception of Spyware amongst Home PC Computer Users, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Jaeger%20Clarke%20-%20The%20Awareness%20and%20Perception%20of%20Spyware%20amongst%20Home%20PC%20Computer%20Users.pdf

255 See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

256 For further information about keyloggers, see: http://en.wikipedia.org/wiki/Keylogger; Netadmintools Keylogging, available at: www.netadmintools.com/part215.html

257 It is easy to identify credit-card numbers, as they in general contain 16 digits. By excluding phone numbers using country codes, offenders can identify credit-card numbers and exclude mistakes to a large extent.

258 One approach to gain access to a computer system in order to install a keylogger is, for example, to gain access to the building where the computer is located using social engineering techniques, e.g. a person wearing a uniform from the fire brigade pretending to check emergency exits has a good chance of gaining access to a building, if more extensive security is not in place. Further approaches can be found in *Mitnick*, The Art of Deception: Controlling the Human Element of Security, 2002.

259 Regular hardware checks are a vital part of any computer security strategy.

260 See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

261 See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606..

262 For more information on the phenomenon of phishing, see below: § 2.9.4.

263 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

264 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

265 Goodin, PlayStation Network breach will cost Sony $ 171m, The Register, 24.05.2011, available at: www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/.

266 *Finkle*, 360 million newly stolen credentials on black market: cybersecurity firm, Reuters, 25.02.2014.

267 *Leprevost*, Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, Development of surveillance technology and risk of abuse of economic information, 2.4, available at: http://cryptome.org/stoa-r3-5.htm.

268 With the fall in price of server storage space, the external storage of information has become more popular. Another advantage of external storage is that information can be accessed from every Internet connection.

269 Regarding the interception of VoIP to assist law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf. Regarding the potential of VoIP and regulatory issues, see: *Braverman*, VoIP: The Future of Telephony is now…if regulation doesn't get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47 *et seq.*, available at: www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

270 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

271 *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

272 The radius depends on the transmitting power of the wireless access point. See http://de.wikipedia.org/wiki/WLAN.

273 With regard to the time necessary for decryption, see below: § 3.2.14.

274 Regarding the difficulties in Cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

275 *Sieber*, Council of Europe Organised Crime Report 2004, page 97.

276 With regard to the interception of electromagnetic emissions, see: Explanatory Report to the Convention on Cybercrime, No. 57.

277 See http://en.wikipedia.org/wiki/Computer_surveillance#Surveillance_techniques.

278 e.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

279 For more details on legal solutions, see below: § 6.2.4.

280 See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

281 *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

282 A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user, to harm the computer system. See *Spafford*, The Internet Worm Program: An Analysis, page 3; *Cohen*, Computer Viruses – Theory and Experiments, available at: http://all.net/books/virus/index.html; *Adleman*, An Abstract Theory of Computer Viruses, Advances in Cryptography – Crypto, Lecture Notes in Computer Science, 1988, page 354 *et seq.* Regarding the economic impact of computer viruses, see: *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12; Symantec Internet Security Threat Report,Trends for July-December 2006, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

283 *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

284 *White/Kephart/Chess*, Computer Viruses: A Global Perspective, available at: www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html

285 Payload describes the function the virus performs after it is installed on victims' computers and activated. Examples of the payload are displaying messages or performing certain activities on computer hardware, such as opening the CD drive or deleting or encrypting files.

286 Regarding the various installation processes, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 21 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

287 See BBC News, Virus-like attack hits web traffic, 25.01.2003, http://news.bbc.co.uk/2/hi/technology/2693925.stm;

288 Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO, 2005 GAO-05-434, page 12, available at: www.gao.gov/new.items/d05434.pdf.

289 *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

290 *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

291 See *Szor*, The Art of Computer Virus Research and Defence, 2005.

292 One example of a virus that encrypts files is the Aids Info Disk or PC Cyborg Trojan. The virus hid directories and encrypted the names of all files on the C-drive. Users were asked to 'renew their licence' and contact PC Cyborg Corporation for payment. For more information, see: *Bates*, "Trojan Horse: AIDS Information Introductory Diskette Version 2.0" in *Wilding/Skulason*, Virus Bulletin, 1990, page 3.

293 Annual Report, Pandalabs, 2013.

294 Kaspersky Press Release, 10.12.2013, available at: www.kaspersky.com/about/news/virus/2013/number-of-the-year .

295 In 2000, a number of well-known United States e-commerce businesses were targeted by denial-of-service attacks. A full list of the attacks business is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

296 Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

297 Examples include: Inserting metal objects in computer devices to cause electrical shorts, blowing hairspray into sensitive devices or cutting cables. For more examples, see *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

298 Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

299 *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

300 A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

301 The term "worm" was used by *Shoch/Hupp*, The 'Worm' Programs – Early Experience with a Distributed Computation, published in 1982. This publication is available for download: http://vx.netlux.org/lib/ajm01.html. With regard to the term 'worm', they refer to the science-fiction novel, "The Shockwave Rider" by John Brunner, which describes a program running loose through a computer network.

302 For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP.

303 See *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

304 July, 2009 South Korea and US DDosc Attacks, Arbor Networks, 2009, available at: www.idcun.com/uploads/pdf/July_KR_US_DDoS_Attacks.pdf.

[305] *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html;

[306] Regarding the different approaches, see below: § 6.2.6.

[307] 2012 Cost of Cyber Crime Study: United States, Ponemon, 2012, page 7.

[308] For reports on cases involving illegal content, see *Sieber*, Council of Europe Organised Crime Report 2004, page 137 *et seq.*

[309] One example of the wide criminalization of illegal content is Sec. 86a German Penal Code. The provision criminalizes the use of symbols of unconstitutional parties: Section 86a: Use of Symbols of Unconstitutional Organizations:

> (1) Whoever: 1. domestically distributes or publicly uses, in a meeting or in writings (Section 11 subsection (3)) disseminated by him, symbols of one of the parties or organizations indicated in Section 86 subsection (1), nos. 1, 2 and 4; or 2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use domestically or abroad, in the manner indicated in number 1, shall be punished with imprisonment for not more than three years or a fine.
>
> (2) Symbols, within the meaning of subsection (1), shall be, in particular, flags, insignia, uniforms, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in sentence 1 shall be deemed to be equivalent thereto.
>
> (3) Section 86 subsections (3) and (4), shall apply accordingly.

[310] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[311] Concerns over freedom of expression (e.g. the First Amendment to the United States Constitution) explain why certain acts of racism were not made illegal by the Convention on Cybercrime, but their criminalization was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

[312] The 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "in many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues". In 2008 the Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should desist from the further adoption of statements supporting the idea of defamation of religions.

[313] 1996 Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

[314] The 2002 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".

[315] International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, and the ACHPR (African Commission on Human and Peoples Rights) Special Rapporteur on Freedom of Expression and Access to Information, 2008..

[316] See below: §§ 3.2.6 and 3.2.7.

[317] In many cases, the principle of dual criminality hinders international cooperation.

[318] Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/*; Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp;

Enser, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

319 Regarding this approach, see: *Stadler*, Multimedia und Recht 2002, page 343 *et seq.*; *Mankowski*, Multimedia und Recht 2002, page 277 *et seq.*

320 See *Sims*, Why Filters Can't Work, available at: http://censorware.net/essays/whycant_ms.html; *Wallace*, Purchase of blocking software by public libraries is unconstitutional, available at: http://censorware.net/essays/library_jw.html.

321 The OpenNet Initiative is a transatlantic group of academic institutions that reports on internet filtering and surveillance. Harvard Law School and the University of Oxford participate in the network, among others. For more information, see: www.opennet.net.

322 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

323 Depending on the availability of broadband access.

324 Access is in some countries is limited by filter technology. Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches,
see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

325 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: § 6.5.

326 *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

327 About a third of all files downloaded in file-sharing systems contained pornography. *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

328 One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch):

Section 184 Dissemination of Pornographic Writings

(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):

1. offers, gives or makes them accessible to a person under eighteen years of age; […]

329 Regarding this aspect, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

330 See: *Nowara/Pierschke*, Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerterten Modellprojekten, 2008.

331 See *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[332] One example is the 2006 Draft Law, Regulating the protection of Electronic Data and Information and Combating Crimes of Information (Egypt):

Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty.

[333] National sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[334] Regarding the principle of "dual criminality", see below: § 6.6.2.

[335] Regarding technical approaches in the fight against obscenity and indecency on the Internet, see: *Weekes*, Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

[336] Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

[337] Regarding the risk of detection with regard to non Internet-related acts, see: *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 63.

[338] *Healy*, Child Pornography: An International Perspective, 2004, page 4.

[339] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006, page, 1.

[340] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8 *et seq.*

[341] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[342] *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 62; Rights of the Child, Commission on Human Rights, 61st session, E/CN.4/2005/78, page 8; *Healy*, Child Pornography: An International Perspective, 2004, page 5; Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 19.

[343] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[344] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[345] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[346] *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 41.

[347] Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17.

[348] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

[349] Vienna Commitment against Child Pornography on the Internet, 1st October 1999; Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 2; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 49.

[350] *Bloxsome/Kuhn/Pope/Voges*, The Pornography and Erotica Industry: Lack of Research and Need for a Research Agenda, Griffith University, Brisbane, Australia: 2007 International Nonprofit and Social Marketing Conference, 27-28 Sep 2007, page 196.

[351] Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 1; *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1. *McCulloch*, Interpol and Crimes against Children – in Quayle/Taylor, Viewing child pornography on the Internet: Understanding the offence, managing the offender, helping the victims, 2005.

[352] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29.

[353] *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29; *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62.

[354] According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[355] *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 7.

[356] See in this context, for example: *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 8.

[357] *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 64.

[358] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 12.

[359] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[360] See, for example, the "G8 Communique", Genoa Summit, 2001, available at: www.g8.gc.ca/genoa/july-22-01-1-e.asp.

[361] United Nations Convention on the Right of the Child, A/RES/44/25, available at: www.hrweb.org/legal/child.html. Regarding the importance of cybercrime legislation see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 35, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[362] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[363] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http://conventions.coe.int.

[364] *Sieber*, Council of Europe Organised Crime Report 2004, page 135. Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[365] See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[366] See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[367] For more information, see: Child Pornography: Model Legislation & Global Review, 2010, page 3, available at: www.icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf.

[368] See *Walden*, Computer Crimes and Digital Investigations, 2007, page 66.

[369] It is possible to make big profits in a rather short period of time by offering child pornography – this is one way how terrorist cells can finance their activities, without depending on donations.

[370] Police authorities and search engines forms alliance to beat child pornography, available at: http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/; "Google accused of profiting from child porn", available at: www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

[371] See ABA, International Guide to Combating Cybercrime, page 73.

[372] Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, Harvard Journal of Law & Technology, Volume 11, page 840 *et seq.*

[373] For more information, see: *Wilson*, Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond., (1997) 30 Creighton Law Review 671 at 690.

[374] *Smith*, Child pornography operation occasions scrutiny of millions of credit card transactions, available at: www.heise.de/english/newsticker/news/print/83427.

[375] With regard to the concept see for example: *Nakamoto* (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

[376] Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

[377] Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at:

[378] See below: § 3.2.14.

[379] Based on the "National Juvenile Online Victimization Study", 12 per cent of arrested possessors of Internet-related child pornography used encryption technology to prevent access to their files. *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[380] See below: § 3.2.14.

[381] For an overview of the different obligations of Internet service providers that are already implemented or under discussion, see: *Gercke*, Obligations of Internet Service Providers with regard to child pornography: legal issue, 2009, available at www.coe.int/cybercrime.

[382] Radical groups in the United States recognized the advantages of the Internet for furthering their agenda at an early stage. See: *Markoff*, Some computer conversation is changing human contact, NY-Times, 13.05.1990.

[383] *Sieber*, Council of Europe Organised Crime Report 2004, page 138.

[384] *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in "Governing the Internet Freedom and Regulation in the OSCE Region", page 91, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[385] See: Digital Terrorism & Hate 2006, available at: www.wiesenthal.com.

[386] *Whine*, Online Propaganda and the Commission of Hate Crime, available at: www.osce.org/documents/cio/2004/06/3162_en.pdf

[387] See: ABA International Guide to Combating Cybercrime, page 53.

[388] Regarding the criminalization in the United States, see: *Tsesis*, Prohibiting Incitement on the Internet, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.

[389] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[390] See: *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 *et seq.*; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 *et seq.*; Development in the Law, The Law of Media, Harvard Law Review, Vol. 120, page 1041.

391 See: Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=213138298941949941944938934938 9379615191991.

392 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144.

393 See: Explanatory Report to the First Additional Protocol, No. 4.

394 See: *Barkham*, Religious hatred flourishes on web, The Guardian, 11.05.2004, available at: www.guardian.co.uk/religion/Story/0,,1213727,00.html.

395 Regarding legislative approaches in the United Kingdom see *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.192.

396 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman,* Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

397 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

398 For more information on the "cartoon dispute", see: the Times Online, 70.000 gather for violent Pakistan cartoons protest, available at: www.timesonline.co.uk/tol/news/world/asia/article731005.ece; *Anderson*, Cartoons of Prophet Met With Outrage, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/01/30/AR2006013001316.html; *Rose*, Why I published those cartoons, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/02/17/AR2006021702499.html.

399 Sec. 295-C of the Pakistan Penal Code:

295-C. Use of derogatory remarks, etc., in respect of the Holy Prophet: Whoever by words, either spoken or written, or by visible representation or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Mohammed (Peace be Upon Him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

400 Sec. 295-B of the Pakistan Penal Code:

295-B. Defiling, etc., of Holy Qur'an: Whoever wilfully defiles, damages or desecrates a copy of the Holy Qur'an or of an extract there from or uses it in any derogatory manner or for any unlawful purpose shall be punishable with imprisonment for life.

401 Regarding the growing importance of Internet gambling, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf ; *Brown/Raysman*, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 *et seq.* available at: www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

402 www.secondlife.com.

403 The number of accounts published by Linden Lab. See: www.secondlife.com/whatis/. Regarding Second Life in general, see: *Harkin*, Get a (second) life, Financial Times, available at: www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

404 Heise News, 15.11.2006, available at: www.heise.de/newsticker/meldung/81088; DIE ZEIT, 04.01.2007, page 19.

405 BBC News, 09.05.2007 Second Life 'child abuse' claim, available at: http://news.bbc.co.uk/1/hi/technology/6638331.stm.

406 *Leapman*, Second Life world may be haven for terrorists, Sunday Telegraph, 14.05.2007, available at: www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml; *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

407 See: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[408] Christiansen Capital Advisor. See www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

[409] The revenue of United States casinos in 2005 (without Internet gambling) was more than USD 84 billion, from: *Landes*, Layovers And Cargo Ships: "The Prohibition Of Internet Gambling And A Proposed System Of Regulation", page 915, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

[410] Statista, Statistic Portal, Global Online Gambling Gross Win from 2006-2015, available at: www.statista.com/statistics/208456/global-interactive-gambling-gross-win/.

[411] See, for example, GAO, "Internet Gambling – An Overview of the Issues", available at: www.gao.gov/new.items/d0389.pdf. Regarding the WTO Proceedings "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; Article 21.5 panel concluded that the United States had failed to comply with the recommendations and rulings of the DSB.

[412] For more information, see: BBC News, Tiny Macau overtakes Las Vegas, at: http://news.bbc.co.uk/2/hi/business/6083624.stm.

[413] See Art. 300 China Criminal Code:

Whoever, for the purpose of reaping profits, assembles a crew to engage in gambling, opens a gambling house, or makes an occupation of gambling, is to be sentenced to not more than three years of fixed-term imprisonment, criminal detention, or control, in addition to a fine.

[414] Besides gambling in Macau, Chinese have started to use Internet gambling intensively. See: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[415] For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

[416] See: OSCE Report on Money Laundering Typologies 2000 – 2001, page 3, available at: www.oecd.org/dataoecd/29/36/34038090.pdf; *Coates*, Online casinos used to launder cash, available at: www.timesonline.co.uk/tol/news/politics/article620834.ece?print=yes&randnum=1187529372681

[417] See, for example, Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[418] For an overview of the early United States legislation, see: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[419] See § 5367 Internet Gambling Prohibition Enforcement Act.

[420] See *Reder/O'Brien*, Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking The Identity Of Anonymous Employee Internet Posters, Mich. Telecomm. Tech. L. Rev. 195, 2002, page 196, available at www.mttlr.org/voleight/Reder.pdf.

[421] Regarding the situation in blogs, see*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[422] Regarding the privacy concerns related to social networks, see: *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available at: www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[423] Regarding the controversial discussion about the criminalization of defamation, see: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf.

[424] See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

[425] With regard to the challenges of investigating offences linked to anonymous services see below: § 3.2.l2.

[426] See: www.wikipedia.org

[427] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

[428] Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as www.archive.org.

[429] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[430] See in this context*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[431] For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[432] *Tempelton*, Reaction to the DEC Spam of 1978, available at: www.templetons.com/brad/spamreact.html.

[433] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[434] The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. The provider Postini published a report in 2007 identifying up to 75 per cent spam e-mail, see www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mail, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. Article in The Sydney Morning Herald, 2006: The year we were spammed a lot, 16 December 2006; www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html.

[435] 2007 Sophos Report on Spam-relaying countries, available at: www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

[436] Kaspersky Security Bulletin. Spam Evolution 2013.

[437] For more information about the technology used to identify spam e-mails, see: *Hernan/Cutler/Harris*, Email Spamming Countermeasures: Detection and Prevention of Email Spamming, available at: www.ciac.org/ciac/bulletins/i-005c.shtml. For an overview on different approaches, see: BIAC ICC Discussion Paper on SPAM, 2004, available at: www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf.

[438] *Lui/Stamm*, Fighting Unicode-Obfuscated Spam, 2007, page 1, available at: www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

[439] Regarding the filter technologies available, see: *Goodman*, Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam, ConsumerPerspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[440] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

[441] Current analyses suggest that up to a quarter of all computer systems may have been recruited to act as part of botnets, see: *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

[442] Regarding international approaches in the fight against botnets, see: ITU Botnet Mitigation Toolkit, Background Information, ICT Application and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

443 See: *Allmann*, The Economics of Spam, available at: http://acmqueue.org/modules.php?name=Content&pa=showpage&pid=108; *Prince*, ITU Discussion Paper "Countering Spam: How to Craft an Effective Anti-Spam Law", page 3 with further references, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

444 Bulk discounts for spam, Heise News, 23.10.2007, available at: www.heise-security.co.uk/news/97803.

445 *Thorhallsson*, A User Perspective on Spam and Phishing, in Governing the Internet Freedom and Regulation in the OSCE Region, page 208, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

446 Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

447 See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

448 Regarding the terminology see: *Sulkowski*, Cyber-Extortion, Journal of Law, Technology & Policy, 2007, page 101 et seq.

449 *Perlroth/Wortham*, Tech Start-Ups Are Targets of Ransom Cyberattacks, NYT, 03.04.2014; *Perlroth*, Tally of Cyber Extortion Attacks on Tech Companies Grows, NYT, 19.07.2014.

450 *Ross*, BItcoin used for extortion demands, Examiner.com, 20.07.2014.

451 KPMG E-Crime Study 2013, page 7.

452 *O'Gorman/MCDonald*, Ransomware: A Growing Menace, Symantec Security Response.

453 *Wang/Ajjan*, Ransomware: Hijacking Your Data, Sophos, 2013; *Sancho/Hacquebord*, The "Police Trojan", An In-Depth Analysis, Trend Micro Research Paper, 2012.

454 See *Sieber*, Council of Europe Organised Crime Report 2004, page 140.

455 See for example the United States International Traffic in Arms Regulation or the Wassenaar Agreement, which is a convention on arms control. 40 countries already participate in the agreement. For more information, see: www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement.

456 See in this context: Council of Europe, Resolution ResAP(2007)2 on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

457 See for example *Henney*, Cyberpharmacies and the role of the US Food And Drug Administration, available at: https://tspace.library.utoronto.ca/html/1807/4602/jmir.html; *De Clippele*, Legal aspects of online pharmacies, Acta Chir Belg, 2004, 104, page 364, available at: www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, What's a Legal System to Do? The Problem of Regulating Internet Pharmacies, available at: www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

458 See: See *Conway*, Terrorist Uses of the Internet and Fighting Back, Information and Security, 2006, page 16, United States Department of Justice 1997 Report on the availability of bomb-making information, available at: www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.

459 E.g. by offering the download of files containing music, movies or books.

460 Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

461 See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, 2004, page 34 *et seq.*

462 Besides these improvements, digitization has speeded up the production of copies and lowered the costs that were one of the key drivers for the industry to perform the transition to digital-based technologies.

463 *Sieber*, Council of Europe Organised Crime Report 2004, page 148.

464 Digital Rights Management describes access control technology used to limit the usage of digital media. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; *Baesler*, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

465 Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schroder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer

Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

466 GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement, available at: www.gao.gov/new.items/d04503.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. United States Federal Trade Commission, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, page 3, available at: www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

467 In 2005, 1.8 million users used Gnutella. See *Mennecke*, eDonkey2000 Nearly Double the Size of FastTrack, available at: www.slyck.com/news.php?story=814.

468 See: Cisco, Global IP Traffic Forecast and Methodology, 2006-2011, 2007, page 4, available at: www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd806a81aa.pdf.

469 See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

470 One example is Germany, where a regularly updated report of the Federation of the phonographic businesses pointed out that, in 2006, 5.1 million users in Germany downloaded music in file-sharing systems. The report is available at: www.ifpi.de/wirtschaft/brennerstudie2007.pdf. Regarding the United States, see: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

471 Apart from music, videos and software, even sensitive personal documents are often found in file-sharing systems. See: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

472 While in 2002, music files made up more than 60 per cent of all files exchanged in file-sharing systems in OECD countries, this proportion dropped in 2003 to less than 50 per cent. See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

473 *Schoder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005, page 11, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Cope*, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: www.computerworld.com/networkingtopics/networking/story/0,10801,69883,00.html; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

474 Regarding Napster and the legal response, see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html; *Penn*, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol7/issue2/penn.pdf.

475 Regarding the underlying technology, see: *Fischer*, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue3/v7i3_a07-Fisher.pdf; *Sifferd*, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Herndon*, Who's watching the kids? – The use of peer-to-peer programs to Cyberstalk children, Oklahoma Journal of Law and Technology, Vol. 12, 2004, available at: www.okjolt.org/pdf/2004okjoltrev12.pdf; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

476 For more information on investigations in peer-to-peer networks, see: Investigations Involving the Internet and Computer Networks, NIJ Special Report, 2007, page 49 *et seq.*, available at: www.ncjrs.gov/pdffiles1/nij/210798.pdf.

477 *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

478 Regarding the motivation of users of peer-to-peer technology, see: *Belzley*, Grokster and Efficiency in Music, Virginia Journal of Law and Technology, Vol. 10, Issue 10, 2005, available at: www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

479 For more examples, see: Supreme Court of the United States, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, I. B., available at: http://fairuse.stanford.edu/MGM_v_Grokster.pdf.

[480] Regarding the economic impact, see: *Liebowitz*, File-Sharing: Creative Destruction or Just Plain Destruction, Journal of Law and Economics, 2006, Vol. 49, page 1 *et seq.*

[481] The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80 per cent of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

[482] The Recording Industry 2006 Privacy Report, page 4, available at: www.ifpi.org/content/library/piracy-report2006.pdf.

[483] One example is the movie "Star Wars – Episode 3" that appeared in file-sharing systems hours before the official premiere. See: www.heise.de/newsticker/meldung/59762 drawing on a MPAA press release.

[484] Regarding anonymous file-sharing systems, see: *Wiley/ Hong*, Freenet: A distributed anonymous information storage and retrieval system, in Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability, 2000.

[485] Content scrambling systems (CSS) is a digital rights management system that is used is most DVD video discs. For details about the encryption used, see: *Stevenson*, Cryptanalysis of Contents Scrambling System, available at: www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

[486] Regarding further responses of the entertainment industry (especially lawsuits against Internet users), see: *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[487] Digital rights management describes access control technology used to limit the usage of digital media. For more information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[488] *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, Copy Protection for DVD Videos, IV 2, available at: www.adastral.ucl.ac.uk/~icox/papers/1999/ProcIEEE1999b.pdf.

[489] *Siebel*, Council of Europe Organised Crime Report 2004, page 152.

[490] See: www.golem.de/0112/17243.html.

[491] Regarding the similar discussion with regard to tools used to design viruses, see below: § 2.8.4.

[492] See *Bakke*, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Regarding trademark violations as a consequence of online-criticism, see: *Prince*, Cyber-Criticism and the Federal Trademark Dilution act: Redefining the Noncommercial use Exemption, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf.

[493] The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions. See *Gecko*, The criminalization of Phishing and Identity Theft, Computer und Resht, 2005, 606; *Ullman*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: § 2.9.4.

[494] For an overview about what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

[495] Regarding the connection with trademark-related offences, see for example: Explanatory Report to the Convention on Cybercrime, No. 42.

[496] Another term used to describe the phenomenon is "domain grabbing". Regarding cybersquatting, see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from cybersquatters, Virginia Journal of Law and Technology, Vol. 10, Issue 6; *Binomial*, Cyberspace Technological Standardization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 *et seq.*; *Struve/Wagner*, Real space Sovereignty in Cyberspace: Problems with the Ant cybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 *et seq.*; *Travis*, The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003.

[497] See: *Lipton*, Beyond cybersquatting: taking domain name disputes past trademark policy, 2005, available at: www.law.wfu.edu/prebuilt/w08-lipton.pdf.

[498] This happens especially with the introduction of new top-level-domains. To avoid cybersquatting, the introduction of a new first-level domain is often accompanied by a period where only parties with trademarks can register a domain name. At the end of this phase (often called the "sunrise period"), other users can register their domain.

[499] For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 112.

[500] For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 113.

[501] In 2006, the United States Federal Trade Commission received nearly 205 000 Internet-related fraud complaints. See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[502] Regarding the related challenges, see below.

[503] In 2006, Nearly 50 per cent of all fraud complaints reported to the United States Federal Trade Commission were related to amounts paid between 0-25 US Dollars See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[504] Regarding the related automation process: § 3.2.8.

[505] The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237.

[506] For more information, see below: § 6.2.14.

[507] The term auction fraud describes fraudulent activities involving electronic auction platforms over the Internet. Regarding auction fraud, see: *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*, available at: www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*; *Chau/Faloutsos*, Fraud Detection in Electronic Auction, available at: www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf; *Dolan*, Internet Auction Fraud: The Silent Victims, Journal of Economic Crime Management, Vol. 2, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

[508] See www.ebay.com.

[509] See *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1.

[510] The United States Internet Crime Complaint Centre (IC3) (a partnership between the FBI and the National White Collar Crime Centre) reported that around 45 per cent of complaints refer to Auction Fraud. See: IC3 Internet Crime Report 2006, available at: www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

[511] Law Enforcement Efforts to combat Internet Auction Fraud, Federal Trade Commission, 2000, page 1, available at: www.ftc.gov/bcp/reports/int-auction.pdf.

[512] See: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[513] For more information, see for example: http://pages.ebay.com/help/feedback/feedback.html.

[514] Regarding the criminalization of "account takeovers", see: *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

[515] See Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[516] The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[517] Advance Fee Fraud, Foreign & Commonwealth Office, available at: www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.

[518] For an overview of estimated losses, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 3 *et seq.*

[519] For more information, see: the Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.

[520] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[521] Regarding phishing, see: *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister

of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

522 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und REcht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

523 "Phishing" scams show a number of similarities to spam e-mails. It is likely that those organized crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: § 2.6.7.

524 Regarding related trademark violations, see above: § 2.7.2.

525 For more information about phishing scams, see below: § 2.9.4.

526 One technical solution to ensure the integrity of data is the use of digital signatures.

527 For case studies, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 94.

528 *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding the different definitions of identity theft, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

529 One of the classic examples is the search for personal or secret information in trash or garbage bins ("dumpster diving"). For more information about the relation to identity theft, see: Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

530 Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15 per cent obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

531 See for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006; *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007.

532 See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

533 See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000.

534 *Hoar*, Identity Theft: The Crime of the New Millennium, Oregon Law Review, Vol. 80, 2001, page 1421 *et seq.*; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, British Journal of Criminology, 2008, page 8.

535 See: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, page 5.

536 See *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003, page 1.

537 Identity Fraud, Prevalence and Links to Alien Illegal Activities, GAO, 2002, GAO-02-830T, page 6; *Paget,* Identity Theft, McAfee White Paper, 2007, page 6. For an overview of Internet-related phishing, see: *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, page 8 *et seq.*

[538] *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270.

[539] Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[540] *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 51.

[541] 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 5.

[542] 35 per cent of the overall number of cases.

[543] 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 6.

[544] Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07_935T, page 4.

[545] *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf..

[546] See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 555.

[547] *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science Technology Society, 2007, Vol. 27, 2008, page 20.

[548] See Encyclopaedia Britannica 2007.

[549] *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, 533.

[550] *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[551] In some cases perpetrators used the data they obtained to hide their real identity. Regarding this aspect, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[552] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[553] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

[554] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[555] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[556] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

[557] This method is not considered as an Internet-related approach.

[558] For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

[559] See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

[560] See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.

[561] The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of cybercrime businesses. It is based on the responses of 494 computer security practitioners from in US corporations, government agencies and financial institutions. The survey is available at: www.gocsi.com/

[562] 2013 US State of Cybercrime Survey, How Bad is the Insider Threat, Carnegie Mellon University, 2013.

[563] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[564] For more details, see: *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

[565] *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[566] See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[567] *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005, page 6; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[568] Examples is the online community Facebook, available at www.facebook.com.

[569] See for example Art. 5 of the Directive 2000/31/Ec Of The European Parliament And Of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[570] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[571] Regarding forensic analysis of e-mail communication, see: *Gupta*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[572] Identity Theft, Prevalence and Cost Appear to be Growing, GAO-02-363.

[573] United States Bureau of Justice Statistics, 2004, available at www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

[574] Press release from the Bureau of Justice Statistics, 12.12.2013, available at: www.bjs.gov/content/pub/press/vit12pr.cfm.

[575] See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.

[576] *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

[577] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.

[578] See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[579] The United States Federal Bureau of Investigation (FBI) requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. The Head of the FBI office in New York is quoted as saying: "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack". See: Heise News, available at: www.heise-security.co.uk/news/80152.

[580] See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[581] *Finkle*, 360 million newly stolen credentials on black market: cybersecurity firm, Reuters, 25.02.2014.

[582] The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: § 3.2.3.

[583] Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at:

www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

584 For an overview about the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (USD 200-500), see: *Paget*, Identity Theft, White Paper, McAfee, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

585 See above: § 2.5.1.

586 For more examples, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 23 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law-enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

587 DoS is an acronym for denial-of-service attack. For more information, see above: § 2.5.5.

588 These generally contain two elements: Software that automates the process of sending out e-mails by avoiding techniques that enable e-mail providers to identify spam e-mails and a database with thousands or even millions of e-mail addresses. For more information, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 25, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

589 For more details, see below: § 6.2.14.

590 *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*

591 *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 10, available at: www.fas.org/sgp/crs/terror/RL33123.pdf.

592 The CIA pointed out in 2002 that attacks against critical infrastructure in the United States will become an option for terrorists. Regarding the CIA position, see: *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 13, available at: www.fas.org/sgp/crs/terror/RL33123.pdf. However, the FBI has stated that there is presently a lack of capability to mount a significant cyberterrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, A Framework for Understanding Terrorist Use of the Internet, 2006, available at: www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp.

593 See: Report of the National Security Telecommunications Advisory Committee – Information Assurance Task Force – Electric Power Risk Assessment, available at: www.aci.net/kalliste/electric.htm.

594 See: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 et seq.; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

595 See: *Roetzer*, Telepolis News, 4.11.2001, available at: www.heise.de/tp/r4/artikel/9/9717/1.html.

596 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; *Zeller*, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position ;

597 CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html.

598 For an overview, see: *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*.

[599] *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[600] Regarding different international approaches as well as national solutions, see: *Sieber* in Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

[601] One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.

[602] Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyberattacks During the War on Terrorism, page 14ff.; *Clark*, Computer Security Officials Discount Chances of "Digital Pearl Harbour", 2003; USIP Report, Cyberterrorism, How real is the threat, 2004, page 2; *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003..

[603] See, for example: *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.

[604] *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

[605] ADL, Terrorism Update 1998, available at: www.adl.org/terror/focus/16_focus_a.asp.

[606] *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes, see also: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

[607] Regarding the use of YouTube by terrorist organizations, see: Heise News, news from 11.10.2006, available at: www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

[608] *Zanini/Edwards*, The Networking of Terror in the Information Age, in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

[609] United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

[610] Regarding the justification, see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

[611] *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 *et seq.*

[612] See: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16.

[613] Videos showing the execution of American citizens Berg and Pearl were made available on websites. See *Weimann* in the USIP Report: How Terrorists use the Internet, 2004, page 5.

[614] Regarding the related challenges, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.

[615] *Levine*, Global Security, 27.06.2006, available at: www.globalsecurity.org/org/news/2006/060627-google-earth.htm. Regarding the discovery of a secret submarine on a satellite picture provided by a free-of-charge Internet service, see: Der Standard Online, Google Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: www.derstandard.at/?url/?id=2952935.

[616] For further reference, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.

[617] For more information regarding the search for secret information with the help of search engines, see: *Long, Skoudis, van Eijkelenborg*, Google Hacking for Penetration Testers.

[618] "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy." For further information, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information & Security, 2006, page 17.

[619] See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.

[620] *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18.

[621] See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

[622] See US Commission on Security and Cooperation in Europe Briefing, 15.05.2008, available at: http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecordType=B&CFID=18849146&CFTOKEN=53; *O'Brian*, Virtual Terrorists, The Australian, 31.07.2007, available at:

www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html*; O'Hear*, Second Life a terrorist camp?, ZDNet.

623 Regarding other terrorist related activities in online games, see: *Chen/Thoms*, Cyberextremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 *et seq.*

624 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008, page 215 *et seq.*

625 *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

626 *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

627 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

628 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position.

629 The Commission analysing the 9/11 attacks calculated that the costs for the attack could have been between USD 400 000 and 500 000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved, the cost per person was relatively small. Regarding the related challenges, see also: *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

630 See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

631 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.

632 See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4.

633 Regarding virtual currencies, see: *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

634 *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

635 *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats, Center for Strategic and International Studies, December 2002.

636 *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

637 *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 *et seq.*

638 *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.

639 CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

640 Law Enforcement Tools and Technologies for Investigating Cyberattacks, DAP Analysis Report 2004, available at: www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.

641 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

642 United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17, 1996. Vol. 61, No. 138.

643 Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: www.gao.gov/new.items/d07706r.pdf.

644 Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

645 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

646 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

647 Cybersecurity Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

648 *Falliere/Murchu/Chien*, W32.Stuxnet Dossier, Symantec, November 2010, page 1; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

649 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

650 Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

651 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1; Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

652 See for example: *Leyden*, Lame Stuxnet Worm: "Full of Errors" says Security Consultant, The Register, 19.02.2011.

653 *Albright/Brannan/Walrond*, Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 22.12.2010; *Broad/Markoff/Sanger*, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times, 15.01.2011; *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 2; *Timmerman*, Computer Worm Shuts Down Iranian Centrifuge Plant, Newsmax, 29.11.2010.

654 *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: www.pp.bme.hu/tr/2003_1/pdf/tr2003_1_03.pdf; *Merten/Teufel*, Technological Innovations in the Passenger Process of the Airline Industry: A Hypotheses Generating Explorative Study in O'Conner/Hoepken/Gretzel, Information and Communication Technologies in Tourism 2008.

655 Sasser B Worm, Symantec Quick reference guide, 2004, available at: http://eval.symantec.com/mktginfo/enterprise/other_resources/sasser_quick_reference_guide_05-2004.en-us.pdf.

656 *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; The Sasser Event: History and Implications, Trend Micro, June 2004, available at: http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp02sasserevent040812us.pdf.

657 *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP, 1997; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

658 *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence? available at: www.projects.ncassr.org/hackback/ethics00.pdf.

659 *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html.

660 *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

661 Improving our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center, Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary United States Senate One Hundred Seventh Congress First Session, July 2001, Serial No. J–107–22, available at: http://cipp.gmu.edu/archive/215_S107FightCyberCrimeNICPhearings.pdf.

662 Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: www.cio.com/article/print/30933.

663 Regarding the Stuxnet software, see: *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1.000 Centrifuges at the Nataz Enrichment Plant? Preliminary Assessment, Institute for Science and International Security, 2010.

[664] *Wilson*, Information Operations and Cyberwar, Capabilities and related Policy Issues, CRS Report for Congress, RL21787, 2006; *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

[665] *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

[666] *Schwartau*, Information Warfare: Chaos on the Electronic Superhighway, 1994, page 13.

[667] *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

[668] Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

[669] *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

[670] *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

[671] *Libicki*, Sub Rosa Cyberwar, COEP, 2010.

[672] *Myers*, Estonia removes Soviet-era war memorial after a night of violence, The New York Times, 27.04.2007; Estonia removes Soviet memorial, BBC News, 27.04.2007; *Tanner*, Violence continues over Estonia's removal of Soviet war statue, The Boston Globe, 28.04.2007.

[673] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

[674] *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

[675] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[676] Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf

[677] See: *Waterman*: Analysis: Who cybersmacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

[678] See for example: *Landler/Markoff*, Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007.

[679] *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27, page 193.

[680] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18-20.

[681] Estonia hit by Moscow cyberwar, BBC News, 17.05.2007; *Traynor*; Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17.05.2007.

[682] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

[683] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

[684] *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

[685] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[686] Regarding the background to the conflict, see: Council of Europe Parliamentary Assembly Resolution 1633 (2008), The consequences of the war between Georgia and Russia.

[687] *Tikk/Kaska/Rünnimeri/Kert/Talihärm/Vihul*, Cyberaattacks Against Georgia: Legal Lessons Identified, 2008, page 4; *Hart*, Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar, Washington Post, 14.08.2008; Cybersecurity and Politically, Socially and Religiously Motivated Cyberattacks, European Union, Policy Department External Policies, 2009, page 15; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

[688] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

[689] See for example: *Partitt,* Georgian blogger Cyxymu blames Russia for cyberattack, The Guardian, 07.08.2009.

[690] *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 75; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

[691] See *Walker*, Information Warfare and Neutrality, *Vanderbilt Journal of Trans-national Law* 33, 2000; *Banks*, Information War Crimes: Mitnick meets Milosevic, 2001, AU/ACSC/019/2001-04.

692 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyberforce, Alb. Law Journal of Science and Technology, Vol. 18, page 315.

693 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 61.

694 *Rushton*, Liberty Reserve shut down in $6bn money laundering case, The Telegraph, 28.05.2013.

695 Santora/Rashbaum/Perlroth, Online Currency Exchange Accused of Laundering $ 6 Billion, NYT.

696 Notice of Finding, Departement of the Treasury, 2013, available at: www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf.

697 One of the most important obligations is the requirement to keep records and to report suspicious transactions.

698 Offenders may tend to make use of the existing instruments, e.g. the services of financial organizations to transfer cash, without the need to open an account or transfer money to a certain account.

699 For case studies, see: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000-2001", 2001, page 8.

700 See: *Woda*, Money Laundering Techniques With Electronic Payment Systems, Information & Security, Vol. 18, 2006, page 40.

701 Regarding the related challenges, see below: § 3.2.l.

702 Regarding the fundermental concept see: Nakamoto (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

703 Regarding the attacks see: Cohen, Speed Bumps on the Road to Virtual Cash, NYT, 3.7.2011, available at: www.nytimes.com/2011/07/04/business/media/04link.html.

704 Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

705 Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at:....???...

706 The costs of setting up an online casino are not significantly larger than other e-commerce businesses.

707 Regarding approaches to the criminalization of illegal gambling, see below: § 6.2.12.

708 See: Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000-2001, 2001, page 2.

709 Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

710 Regarding the phenomenon of phishing, see: *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

711 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, "The Phishing Guide Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

712 The following section describes e-mail-based phishing attacks, compared to other phishing scams, which may, for example, be based on voice communications. See: *Gonsalves*, Phishers Snare Victims with VoIP, 2006, available at: www.techweb.com/wire/security/186701001.

713 "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organized crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see above: § 2.6.7.

714 Regarding related trademark violations, see above: § 2.7.2.

715 For an overview of what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

716 In some phishing attacks, as many as 5 per cent of victims provided sensitive information on fake websites. See *Dhamija/Tygar/Hearst*, Why Phishing Works, available at:

http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, page 1, that refers to *Loftesness*, Responding to "Phishing" Attacks, Glenbrook Partners (2004).

[717] Anti-Phishing Working Group. For more details, see: www.antiphishing.org.

[718] Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[719] Phishing Activitiy Trends Report, 1st Quarter 2014, WPWG, 2014.

[720] See above: § 2.8.3.

3. Les enjeux de la lutte contre la cybercriminalité

Bibliography (selected): *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV; *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142; *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 291 *et seq.*; *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2; *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19; *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*; *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001; *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58*; Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf*; Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001*; Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf*; Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004*; Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003; *Wallsten*, Regulation and Internet Use in Developing Countries, 2002.

Si l'évolution récente des technologies de l'information et de la communication a ouvert la voie à de nouveaux cyberdélits et à de nouvelles méthodes criminelles, elle a aussi permis de mettre au point de nouvelles méthodes d'investigation. Les progrès réalisés dans le domaine des TIC ont ainsi considérablement élargi les capacités des agences de répression. Inversement, les cyberdélinquants créent de nouveaux outils afin d'empêcher leur identification et de gêner les enquêtes. Le présent chapitre se propose d'étudier les enjeux de la lutte contre la cybercriminalité.

3.1 Opportunités

Si le développement de certains services TIC, comme les serveurs de communication anonymes ou les outils anti-criminalistiques, peut représenter une sérieuse entrave aux enquêtes, les avancées techniques ont également permis de mener des enquêtes plus poussées.

3.1.1 Automatisation générale des enquêtes

Par le passé, la recherche de preuves pertinentes sur l'ordinateur d'un suspect était principalement effectuée de manière manuelle. Avec le développement d'outils de criminalistique évolués, la situation a

changé du tout au tout. Pour accélérer les enquêtes et automatiser les procédures de recherche, les agences de répression peuvent aujourd'hui exploiter la puissance, toujours plus grande, des systèmes informatiques et profiter des logiciels sophistiqués utilisés en criminalistique.[721] Toutes les méthodes d'enquête ne peuvent cependant pas être automatisées. S'il est facile d'effectuer une recherche de contenus illicites à partir de mots-clés, la recherche d'images illicites se révèle, quant à elle, plus problématique. Les approches fondées sur la valeur de hachage ne portent leurs fruits que si l'image à analyser a préalablement été évaluée, la valeur de hachage stockée dans une base de données et l'image non modifiée.[722]

Les logiciels utilisés en criminalistique sont capables de rechercher automatiquement des images pornographiques mettant en scène des enfants en comparant les fichiers se trouvant sur des disques durs appartenant à des suspects avec des données concernant des images connues. Fin 2007, les autorités ont trouvé plusieurs images d'abus sexuels sur des enfants, dans lesquelles, pour empêcher son identification, l'auteur avait numériquement modifié son visage avant diffusion sur Internet. Les experts informatiques spécialisés en criminalistique sont parvenus à défaire les modifications apportées à l'image et à reconstruire le visage du suspect.[723] Si cette enquête réussie met clairement en évidence le potentiel des spécialistes en informatique criminalistique, elle ne témoigne aucunement d'une avancée majeure dans l'investigation des affaires de pédopornographie. Si le criminel s'était contenté de masquer son visage d'une tache blanche, l'identification aurait été impossible.

3.1.2 Création de données dans le cadre des services en ligne

Comme indiqué précédemment, les services liés aux TIC sont très populaires. Facebook, YouTube, Instagram et Twitter ne sont que quelques-uns des services qui comptent des centaines de millions d'utilisateurs.[724] La plupart des fournisseurs de ces services effectuent un suivi des activités des utilisateurs[725], ce qui fait partie de leur modèle économique. Ces données peuvent présenter un grand intérêt pour les enquêteurs. En effet, si de telles informations peuvent être légalement demandées et utilisées, les enquêteurs peuvent mener des enquêtes très sophistiquées et vérifier par exemple avec qui le suspect a été en contact avant de commettre une infraction qu'il serait difficile de commettre seul. Les géoinformations créées par les opérateurs de téléphonie mobile peuvent être tout aussi utiles, dans la mesure où ces données peuvent permettre de savoir si le téléphone mobile du suspect se trouvait près de la scène du crime au moment où ce dernier a été commis.[726]

3.1.3 Création de données par la numérisation des processus du monde réel

A l'heure actuelle, les TIC sont largement utilisées dans les processus quotidiens, ce qui intensifie la création de données qui peuvent être utilisées par les organismes chargés de l'application de la loi lorsque ces derniers sont autorisés à y accéder et à les utiliser dans le cadre d'enquêtes judiciaires. Si les nouveaux services purement numériques tels que les réseaux sociaux attirent l'attention des utilisateurs et mènent au stockage de données, même les services traditionnels sont progressivement numérisés. Ainsi, les TIC sont de plus en plus utilisés pour les services postaux.[727] Des scanners à haut débit sont utilisés pour scanner les adresses et les transformer en données électroniques.[728] Cette technologie a été introduite aux Etats-Unis dès les années 1980.[729]

En 2013, la presse a indiqué que le service postal des Etats-Unis répertoriait tous les courriers pour les enquêtes des organismes chargés de l'application de la loi. Grâce au programme MICT (Mail Isolation Control and Tracking) créé en 2011 suite aux attaques à l'anthrax perpétrées aux États-Unis, on conserve une photo de chaque lettre et de chaque colis postés aux Etats-Unis.[730] Ces informations ont été utilisées dans le cadre d'enquêtes judiciaires.[731]

3.2 Enjeux généraux

3.2.1 Dépendance à l'égard des TIC

De nombreuses communications de la vie quotidienne s'appuient aujourd'hui sur les TIC et les services Internet. Ainsi les appels vocaux sur IP et les communications par courriel.[732] Les TIC prennent désormais en charge les fonctions de commande et de gestion dans les bâtiments,[733] les voitures et les services aériens.[734] Il en va de même pour l'approvisionnement en énergie et en eau ainsi que les services de communication. Et il y a toutes les chances pour que ces nouvelles technologies continuent de s'installer dans notre vie.[735] Cette dépendance croissante à l'égard des TIC augmente la vulnérabilité des systèmes et des services liés aux infrastructures essentielles.[736] Des interruptions de service, même de courte durée, peuvent entraîner de lourdes pertes financières pour les entreprises de cybercommerce.[737] Les communications civiles ne sont pas les seules concernées, la dépendance à l'égard des TIC met aussi gravement en danger les communications militaires.[738]

Les infrastructures techniques existantes présentent un certain nombre de faiblesses, parmi lesquelles la monoculture ou homogénéité des systèmes d'exploitation. Bien des particuliers et PME utilisent en effet le système d'exploitation de Microsoft,[739] cible dès lors privilégiée des cyberdélinquants.[740]

La dépendance de la société vis-à-vis des TIC n'est pas un phénomène propre aux pays occidentaux.[741] Les pays en développement aussi sont confrontés aux problèmes de prévention des attaques visant leurs infrastructures et leurs utilisateurs.[742] Grâce au développement de technologies moins onéreuses en termes d'infrastructures, telles que WiMAX,[743] les pays en développement peuvent aujourd'hui proposer des services Internet à un plus grand nombre d'utilisateurs. Ces pays peuvent éviter les erreurs de certains pays occidentaux, qui ont axé leur développement sur la maximisation de l'accessibilité sans investir notablement dans la protection. Selon certains experts américains, les attaques contre le site officiel des organisations gouvernementales d'Estonie[744] n'ont pu porter leurs fruits qu'en raison de l'insuffisance des mesures de protection.[745] Les pays en développement ont une occasion exceptionnelle d'intégrer des mesures de sécurité dès les premières phases de mise en œuvre. Cela suppose, certes, des investissements initiaux plus importants, mais l'intégration de mesures de sécurité à un stade ultérieur pourrait se révéler plus coûteuse sur le long terme.[746]

Il importe donc de développer des stratégies de prévention et de concevoir des contre-mesures, notamment de mettre au point et de promouvoir des moyens techniques de protection, mais aussi une législation adaptée et suffisante, qui permette aux services de répression de lutter efficacement contre la cybercriminalité.[747]

3.2.2 Nombre d'utilisateurs

La popularité d'Internet et de ses services augmente rapidement et l'on comptait plus de 2 milliards d'internautes dans le monde en 2010.[748] Les sociétés informatiques et les FAI s'intéressent tout particulièrement aux pays en développement dont le potentiel de croissance est le plus élevé.[749] En 2005, le nombre d'internautes dans ces pays a dépassé celui des pays industrialisés,[750] et il devrait encore augmenter sous l'effet de la baisse du prix du matériel et du développement des accès sans fil.[751]

Le nombre de cibles potentielles et de cyberdélinquants augmente avec le nombre d'internautes.[752] Il est difficile d'estimer le nombre de personnes utilisant Internet dans le but de mener des activités illicites, mais, quand bien même ils ne représenteraient que 0,1 % des internautes, le nombre de cyberdélinquants dépasserait un million. Bien que les taux d'utilisation d'Internet y soient inférieurs, il n'est pas plus facile de promouvoir la cybersécurité dans les pays en développement, car les cyberdélinquants peuvent agir de n'importe quel point du globe.[753]

Étant donné qu'il est relativement difficile d'automatiser les processus d'enquête, l'augmentation du nombre d'internautes est source de difficultés supplémentaires pour les services de répression. S'il est relativement facile d'effectuer une recherche de contenus illicites à partir de mots-clés, la recherche d'images illégales est plus problématique. Les approches fondées sur la valeur de hachage par exemple ne

portent leurs fruits que si l'image à analyser a préalablement été évaluée, la valeur de hachage stockée dans une base de données et l'image non modifiée.[754]

3.2.3 Disponibilité des équipements et de l'accès

Pour commettre des cyberdélits, il suffit de disposer d'un équipement élémentaire. Matériel, logiciel et accès Internet suffisent pour commettre un délit.

S'agissant du matériel, il importe de souligner que la puissance des ordinateurs est en constante augmentation.[755] Il existe un certain nombre d'initiatives visant à promouvoir l'utilisation des TIC dans les pays en développement.[756] Il est possible de commettre de graves délits informatiques avec du matériel bon marché ou d'occasion et, dans ce domaine, les connaissances comptent beaucoup plus que l'équipement. Aussi la vétusté d'un matériel a-t-elle peu de rapports avec son utilisation pour commettre des cyberdélits.

Commettre un cyberdélit peut être facilité par des outils logiciels spécialisés. Les cyberdélinquants peuvent télécharger des logiciels[757] conçus pour détecter des ports ouverts ou contourner des protections par mot de passe.[758] Face aux sites « miroirs » et aux échanges *peer-to-peer*, il est difficile de limiter l'expansion de ces dispositifs.[759]

Dernière condition nécessaire à la commission d'un cyberdélit: disposer d'un accès à Internet. Bien que le coût des accès [760] soit plus élevé dans la plupart des pays en développement que dans les pays industrialisés, le nombre d'internautes dans ces pays est en croissance rapide.[761] Pour limiter le risque d'identification, la plupart des cyberdélinquants ne souscrivent pas d'abonnement à Internet, mais préfèrent utiliser des accès libres (sans inscription avec procédure de vérification). Le *wardriving*, ou « piratage Wi-Fi », est une méthode classique pour obtenir un accès au réseau. Elle consiste à balayer des réseaux sans fil en utilisant son automobile à la recherche d'un accès.[762] Les moyens d'accès aux réseaux les plus fréquemment utilisés par les cyberdélinquants pour accéder au réseau relativement anonymement sont les terminaux publics d'accès à Internet, les réseaux (hertziens) libres [763], les réseaux piratés et les services prépayés sans inscription.

Les agences de répression prennent des mesures pour restreindre les accès non contrôlés aux services Internet, et ce, afin d'en prévenir l'utilisation illicite. En Italie et en Chine par exemple, les utilisateurs de terminaux publics d'accès à Internet doivent obligatoirement s'identifier.[764] L'identification systématique a cependant ses détracteurs.[765] Bien que la limitation des accès soit susceptible de prévenir les délits et de faciliter le travail d'enquête, elle pourrait aussi freiner le développement du commerce électronique et de la société de l'information.[766] Certains ont également fait valoir qu'une telle limitation pourrait constituer une violation des droits de l'homme.[767] La Cour européenne a par exemple décidé, dans plusieurs affaires de radiodiffusion, que le droit à la liberté d'expression s'applique non seulement au contenu de l'information, mais aussi aux moyens utilisés pour émettre ou recevoir cette information. Dans l'affaire *Autronic c. Suisse*,[768] la Cour a par exemple soutenu qu'il convenait de faire une interprétation large de la loi, étant donné que toute restriction sur les moyens interfère nécessairement avec le droit de recevoir et de transmettre de l'information. Par conséquent, si ces principes sont appliqués, on peut craindre que les approches législatives consistant à limiter les accès à Internet ne soient interprétées comme une violation des droits de l'homme.

3.2.4 Disponibilité de l'information

On trouve sur Internet des millions de pages [769] d'information régulièrement mises à jour. Quiconque souhaite participer peut mettre en ligne et actualiser des informations. Wikipédia,[770] encyclopédie en ligne dans laquelle tout internaute peut publier ses articles, est un exemple du succès des plates-formes de contenu généré par l'utilisateur.[771]

Le succès d'Internet tient également à l'existence de moteurs puissants, qui permettent aux utilisateurs de faire des recherches dans des millions de pages en quelques secondes. Si cette technologie peut servir des intérêts légitimes, elle est aussi à la portée d'utilisateurs moins honnêtes. On utilise à cet égard les termes *Googlehacking* (piratage par Google) et *Googledorks* (pirates utilisant Google) pour faire référence à l'utilisation de requêtes complexes sur des moteurs de recherche dans le but de filtrer de grandes quantités

de résultats à la recherche d'informations mettant en évidence des problèmes de sécurité. Certains cyberdélinquants recherchent, par ce biais, des systèmes sont la protection par mot de passe est insuffisante.[772] Certains rapports soulignent d'ailleurs les risques liés à l'utilisation des moteurs de recherche à des fins illicites.[773] Pour préparer un attentat, un criminel peut trouver sur Internet des informations détaillées sur la fabrication d'une bombe à partir de produits chimiques, tous en vente dans des supermarchés non spécialisés.[774] Avant le développement d'Internet, ces informations étaient certes disponibles, mais d'accès plus difficile; aujourd'hui, tout internaute peut y avoir accès.

Les cyberdélinquants peuvent également utiliser les moteurs de recherche pour analyser leurs cibles.[775] On a ainsi trouvé, au cours d'enquêtes concernant les membres d'un groupe terroriste, un manuel de formation qui soulignait combien il est facile de collecter sur Internet des renseignements sur des cibles potentielles.[776] Les criminels peuvent, à l'aide de moteurs de recherche, réunir des informations en libre accès, qui les aident à préparer leurs infractions (plans de construction d'un bâtiment public par exemple). Il a ainsi été rapporté que les insurgés qui ont attaqué les troupes britanniques en Afghanistan avaient utilisé des images satellitaires provenant de Google Earth.[777]

3.2.5 Insuffisance des mécanismes de contrôle

Tous les réseaux de communication de masse – des réseaux téléphoniques pour la communication vocale aux réseaux Internet – nécessitent une gestion centrale et des normes techniques qui garantissent une bonne opérabilité. Les études en cours concernant la gouvernance d'Internet tendent à indiquer que ce réseau n'est pas différent des autres infrastructures de communication nationales, voire transnationales.[778] Internet aussi doit être régi par des lois. Les législateurs et les agences de répression ont d'ailleurs commencé à élaborer des normes juridiques, qu'il conviendra, dans une certaine mesure, de contrôler à un niveau central.

À l'origine, Internet a été conçu comme un réseau militaire [779] reposant sur une architecture décentralisée afin de préserver la fonctionnalité principale intacte et opérationnelle, même en cas d'attaque de certains éléments du réseau. Par son infrastructure, Internet résiste donc aux tentatives externes de prise de contrôle. Il n'était pas prévu, dans le cahier des charges initial, de faciliter les enquêtes pour infraction ni de prévenir les attaques provenant de l'intérieur du réseau.

Internet est aujourd'hui de plus en plus utilisé dans le civil. Cette évolution du secteur militaire vers le secteur civil s'accompagne d'une évolution de la demande en termes d'instruments de contrôle. Le réseau reposant sur des protocoles conçus à des fins militaires, il n'existe pas de tels instruments à un niveau central et il est difficile de les mettre en place *a posteriori* sans repenser profondément la conception globale. L'absence de ces instruments complique considérablement les enquêtes sur les cyberdélits.[780]

À titre d'exemple de problème posé par l'absence d'instrument de contrôle, les internautes peuvent contourner les techniques de filtrage[781] en utilisant des services chiffrés de communication anonyme.[782] Il est normalement impossible de se connecter aux sites Internet proposant des contenus illicites (pédopornographie par exemple) si les FAI en ont bloqué l'accès. Pourtant, en passant par un serveur de communication anonyme qui chiffre les transferts entre les internautes et le serveur central, il est possible de passer outre le blocage des contenus. En effet, les requêtes étant envoyées sous forme chiffrée, les FAI ne sont pas en mesure de les lire ni, par conséquent, de les bloquer.

3.2.6 Dimensions internationales

De nombreux processus de transfert de données mettent en jeu plusieurs pays.[783] Les protocoles utilisés sur Internet sont conçus pour optimiser le routage en cas d'indisponibilité temporaire des liens de communication directs.[784] Même lorsqu'un pays limite les transferts sur son propre territoire, les données peuvent quitter le pays, transiter par des routeurs situés à l'étranger et être redirigées vers le pays pour atteindre leur destination finale.[785] Par ailleurs, de nombreux services Internet reposent sur d'autres services situés à l'étranger.[786] On peut notamment citer le cas où un hébergeur loue un espace Web dans un pays donné, alors que l'espace en question se trouve en réalité sur du matériel dans un autre pays.[787]

Si les cyberdélinquants et les victimes sont situés dans des pays différents, il est nécessaire, pour mener à bien les enquêtes, que les services de répression de tous les pays concernés coopèrent.[788] Or, en vertu du

principe de souveraineté nationale, il n'est pas permis de diligenter une enquête sur le territoire d'un pays sans l'autorisation des autorités locales.[789] Il est donc essentiel d'obtenir le soutien et la participation des autorités de tous les pays impliqués.

La coopération en matière de cybercriminalité peut difficilement reposer sur les principes de l'entraide judiciaire traditionnelle. Le formalisme et le temps nécessaire à la collaboration avec les agences de répression étrangères freinent souvent les enquêtes.[790] Les enquêtes se déroulent souvent sur des périodes très courtes.[791] Les données cruciales qui permettent de retrouver l'origine d'une infraction sont souvent effacées après un laps de temps très court. Ces délais très courts sont problématiques, car il faut souvent du temps pour organiser une opération d'entraide judiciaire.[792] Autre difficulté, le principe de la double incrimination [793] en vertu duquel l'infraction en cause doit être incriminée de manière comparable dans la législation de tous les pays concernés.[794] Ainsi, pour compliquer l'enquête, les cyberdélinquants intègrent parfois délibérément un pays tiers dans leur attaque.[795]

Il arrive que les cyberdélinquants choisissent à dessein des cibles situées à l'extérieur de leur propre pays et qu'ils agissent à partir de pays où la législation anticybercriminalité est insuffisante.[796] L'harmonisation des législations relatives à la cybercriminalité d'une part et de la coopération internationale d'autre part devrait donc être bénéfique. Deux initiatives visent à accélérer la coopération internationale dans les enquêtes sur les cyberdélits: le réseau 24/7 [797] du G8 et les dispositions relatives à la coopération internationale énoncées dans la Convention sur la cybercriminalité du Conseil de l'Europe.[798]

3.2.7 Indépendance de l'emplacement et présence sur le site du délit

Comme il n'est pas nécessaire que les cyberdélinquants se trouvent au même endroit que leurs victimes, de nombreux cyberdélits sont commis d'un pays à un autre. Commettre ces infractions de niveau international demande beaucoup d'efforts et de temps. Les cyberdélinquants cherchent donc à éviter les pays dotés d'une législation forte en matière de cybercriminalité.[799]

L'un des enjeux majeurs du combat contre la cybercriminalité est de lutter contre les « refuges ».[800] Tant qu'il existera de tels lieux, les cyberdélinquants chercheront à les utiliser pour freiner les enquêtes. Les pays en développement non encore dotés d'une législation contre la cybercriminalité pourraient devenir des points vulnérables, les cyberdélinquants choisissant de s'y installer pour échapper aux poursuites. Si la législation est insuffisante dans les pays à partir desquels les cyberdélinquants opèrent, il est difficile de mettre fin aux attaques graves qui frappent l'ensemble de la planète. Ce problème pourrait conduire à accentuer la pression sur certains pays afin qu'ils adoptent les lois nécessaires. « Love Bug », ver informatique développé par un pirate aux Philippines en 2000,[801] et responsable de l'infection de millions d'ordinateurs dans le monde, est tout à fait représentatif de cette problématique.[802] Le travail d'enquête au niveau local avait été freiné du fait que, à l'époque, le développement et la diffusion de logiciels malveillants n'étaient pas suffisamment sanctionnés dans ce pays.[803] On peut également citer le cas du Nigéria, instamment prié de prendre des mesures pour lutter contre les escroqueries financières diffusées par courriel.

3.2.8 Automatisation

Les TIC présentent un avantage considérable: celui de rendre automatisables certains processus. L'automatisation a plusieurs conséquences importantes: elle augmente la vitesse des processus ainsi que leur ampleur et leur impact et, enfin, elle permet de limiter l'intervention humaine.

L'automatisation entraîne une réduction de la main-d'œuvre coûteuse, et donc une baisse des prix des services proposés par les fournisseurs.[804] Grâce à l'automatisation, les cyberdélinquants peuvent intensifier leurs activités et, par exemple, envoyer automatiquement plusieurs millions de courriels de spam [805] en masse.[806] Les tentatives de piratage aussi sont souvent automatisées, [807] on en compte pas moins de 80 millions chaque jour [808] commises à l'aide d'outils logiciels [809] capables d'attaquer des milliers de systèmes informatiques en quelques heures.[810] Grâce à l'automatisation, les cyberdélinquants peuvent concevoir des escroqueries reposant sur un très grand nombre d'infractions, chacune n'entraînant pour la victime que des pertes relativement faibles, et ainsi réaliser des profits très importants.[811] Or, plus la perte unitaire est faible, moins il y a de risques que la victime signale l'infraction.

L'automatisation des attaques touche tout particulièrement les pays en développement, qui, du fait de leurs ressources limitées, sont plus durement touchés que les pays industrialisés, notamment par le spam.[812] L'augmentation du nombre des cyberdélits du fait de l'automatisation est problématique, car les services de répression du monde entier doivent se préparer à gérer dans leur juridiction un nombre de victimes beaucoup plus important.

3.2.9 Ressources

Les ordinateurs modernes disponibles aujourd'hui sur le marché sont très puissants et constituent, de ce fait, de bons outils pour élargir le champ des activités criminelles. Pour les enquêteurs, ce n'est pas tant la puissance croissante[813] des ordinateurs pris isolément qui fait problème, mais les capacités réseau, toujours plus importantes, de ces machines.

On peut citer, à ce titre, les attaques récentes essuyées par des sites Internet de l'administration publique en Estonie.[814] Selon certaines analyses, les attaques ont été commises par des milliers d'ordinateurs appartenant à un « botnet »,[815] c'est-à-dire un groupe d'ordinateurs infectés sur lesquels s'exécutent des programmes commandés à distance.[816] La plupart du temps, les ordinateurs sont infectés par des logiciels malveillants, chargés d'installer des outils permettant à l'auteur de l'infraction de prendre le contrôle à distance. Les botnets sont utilisés pour collecter des informations sur les cibles ou pour lancer des attaques massives.[817]

Ces dernières années, les botnets sont devenus de graves menaces pour la cybersécurité.[818] Leur taille est variable: certains ne comptent que quelques ordinateurs, d'autres plus d'un million.[819] Selon certaines analyses en cours, jusqu'à un quart de l'ensemble des ordinateurs connectés à Internet pourraient être infectés par des logiciels dont le but est de les inclure dans un botnet.[820] Les botnets peuvent être utilisés pour commettre divers cyberdélits, notamment les attaques par refus de service,[821] le spam,[822] le piratage et l'échange de fichiers protégés par le droit d'auteur.

Les botnets offrent aux cyberdélinquants plusieurs avantages. D'une part, ils augmentent les capacités informatiques et de réseau des cyberdélinquants. En effet, ceux-ci peuvent, en utilisant des milliers d'ordinateurs, attaquer des systèmes informatiques qu'il serait impossible d'atteindre avec quelques ordinateurs seulement.[823] D'autre part, les botnets compliquent la recherche des personnes qui sont à l'origine des attaques, car l'analyse des traces initiales ne mène qu'aux membres des botnets. Étant donné que les cyberdélinquants commandent des systèmes informatiques et des réseaux plus puissants que ceux des autorités chargées d'enquêter, leurs moyens sont plus importants et l'écart se creuse.

3.2.10 Vitesse des processus d'échange de données

Le transfert d'un courriel entre deux pays ne prend que quelques secondes. Si Internet a permis d'éliminer le temps de transport des messages – et c'est assurément l'une des raisons de son succès, les agences de répression disposent désormais de très peu de temps pour mener leurs enquêtes ou collecter des données, temps insuffisamment long pour des enquêtes classiques.[824]

On peut citer, à cet égard, l'échange de contenu pornographique mettant en scène des enfants. Les vidéos pornographiques étaient autrefois apportées ou livrées aux acheteurs, ce qui donnait aux services de répression l'occasion d'enquêter. Dans ce domaine, ce qui fait la différence entre l'avant et l'après-Internet, c'est justement le transport: sur Internet, les films peuvent être échangés en quelques secondes.

L'exemple du courriel met également en évidence l'intérêt de disposer d'outils ultrarapides permettant d'intervenir immédiatement. En effet, pour remonter jusqu'aux suspects et les identifier, les enquêteurs ont souvent besoin d'accéder à des données qui sont effacées peu de temps après le transfert.[825] Il est donc essentiel qu'ils puissent réagir très rapidement. Il paraît difficile de lutter efficacement contre la cybercriminalité sans une législation et des instruments adéquats permettant aux enquêteurs d'agir immédiatement et d'empêcher que des données ne soient effacées.[826]

Les « procédures de gel rapide »[827] et les points de contact du réseau 24/7[828] sont deux exemples d'outil permettant d'accélérer les enquêtes. La législation de conservation des données vise, de son côté, à augmenter le temps dont disposent les services de répression pour enquêter. En effet, si les données

nécessaires pour retrouver les cyberdélinquants sont conservées suffisamment longtemps, les enquêteurs ont plus de chances de parvenir à identifier les suspects.

3.2.11 Rapidité des évolutions

Internet est en perpétuelle évolution. C'est la création d'une interface utilisateur graphique (WWW[829]), venue remplacer l'interface en ligne de commande moins conviviale, qui a marqué le début de son expansion phénoménale. La création du www a ouvert la voie à de nouvelles applications, mais aussi à de nouvelles infractions[830]. Les services de répression essaient de ne pas se laisser distancer et ne ménagent pas leurs efforts. Sans cesse, de nouvelles applications voient le jour, notamment avec les jeux en ligne et les communications vocales sur IP (VoIP).

Les jeux en ligne sont plus populaires que jamais et il est difficile de savoir si les services de répression peuvent efficacement enquêter sur les infractions commises dans le monde virtuel et poursuivre en justice leurs auteurs.[831]

Avec la transition de la téléphonie traditionnelle vers la téléphonie sur Internet, les services de répression sont aussi confrontés à de nouveaux problèmes. En effet, les techniques et les procédures d'interception des appels classiques via les opérateurs de téléphonie ne s'appliquent généralement pas aux communications sur IP. S'ils appliquaient le principe de la téléphonie classique à la voix sur IP, les services de répression devraient s'adresser aux FAI et aux fournisseurs de services VoIP. Or, si l'appel téléphonique repose sur une technologie de type *peer-to-peer*, les fournisseurs de services ne sont généralement pas en mesure d'intercepter les communications, car la transmission des données s'effectue directement entre les interlocuteurs.[832] D'où la nécessité de nouvelles techniques d'interception.[833]

Par ailleurs, de nouveaux appareils mettant en jeu des technologies réseau voient régulièrement le jour et sont rapidement adoptés. Les dernières consoles de jeux transforment les télévisions en des points d'accès à Internet, alors que les téléphones portables les plus récents sont capables de stocker des données et de se connecter à Internet via des réseaux hertziens.[834] Des montres, des stylos et des couteaux de poche intègrent aujourd'hui des mémoires à connexion USB (*Universal Serial Bus*) de plus de 1 GO. Pour pouvoir tenir compte de ces technologies en pleine évolution, les agents chargés des enquêtes dans les affaires de cybercriminalité doivent impérativement être formés, et ce, de façon continue, seule façon pour eux de connaître les nouveautés et de savoir, lors d'une enquête, quel matériel ou dispositif il convient de saisir.

Autre évolution, l'utilisation des points d'accès hertzien, qui, s'ils constituent pour les pays en développement une opportunité, sont aussi pour les services de répression source de difficultés.[835] En effet, certains points d'accès hertzien ne requièrent pas d'identification. Dès lors, les recherches s'arrêtent au niveau du point d'accès et il est plus difficile de retrouver les cyberdélinquants qui se sont connectés.

3.2.12 Communications anonymes

Déterminer l'origine d'une communication est très souvent la clé des enquêtes de cybercriminalité. Toutefois, la nature distribuée du réseau[836], ainsi que la disponibilité de certains services Internet, qui crée de l'incertitude sur l'origine, est un obstacle à l'identification des cyberdélinquants.[837] L'anonymat des communications peut être une simple caractéristique d'un service ou offerte dans le but de protéger l'utilisateur. Il est crucial d'appréhender cette incertitude sur l'origine pour éviter toute conclusion infondée.[838] Parmi les services concernés, on peut citer — éventuellement en combinaison:

- les terminaux publics d'accès à Internet (dans les aéroports, les cybercafés, etc.);[839]
- les dispositifs de traduction d'adresse réseau (NAT) et les réseaux privés virtuels (VPN);[840]
- les réseaux hertziens;[841]
- les services mobiles prépayés sans identification;
- les offres de stockage de pages Internet sans identification;
- les serveurs de communication anonyme;[842]

- les services de courriel anonyme.[843]

L'utilisation de fausses adresses de courriel est l'une des possibilités qui s'offrent aux cyberdélinquants pour cacher leur identité[844]. De nombreux prestataires proposent l'ouverture gratuite de comptes de courriel. Or les renseignements personnels – lorsqu'ils sont demandés – ne sont pas toujours vérifiés. Il est donc possible de créer des adresses de courriel sans révéler son identité. L'adresse anonyme présente un intérêt: elle permet par exemple à un internaute de se joindre à un groupe de discussions politiques de façon anonyme. D'un côté, les communications anonymes peuvent favoriser les comportements antisociaux; de l'autre, elles donnent aux internautes une plus grande liberté[845].

Il apparaît clairement nécessaire, au vu de toutes les traces laissées par les utilisateurs sur Internet, d'empêcher, par des instruments législatifs, le profilage des activités sur le réseau [846]. Plusieurs États et organisations soutiennent ainsi le principe de l'utilisation anonyme des services de courriel, principe énoncé notamment dans la Directive « vie privée et communications électroniques » de l'Union européenne[847]. L'article 37 du règlement de l'Union européenne relatif à la protection des données fournit un exemple d'approche juridique permettant de protéger la vie privée des utilisateurs[848]. Cela étant, certains États cherchent à résoudre les problèmes que posent les communications anonymes en mettant en place des limitations juridiques [849], notamment l'Italie, qui impose aux fournisseurs d'accès public à Internet d'identifier les utilisateurs dès le début d'une session[850].

Ces mesures ont pour objectif d'aider les services de répression à identifier les suspects. Il est toutefois facile de passer outre, en se connectant à des réseaux hertziens privés non protégés ou en utilisant des cartes SIM émises par des pays dans lesquels l'identification n'est pas exigée. Quant à savoir si la limitation des communications et des accès anonymes devrait tenir une place plus importante dans les stratégies de cybersécurité, la question reste posée[851].

3.2.13 Échec des moyens d'enquête traditionnels

Les enquêtes et des poursuites en matière de cybercriminalité supposent de disposer d'outils et d'instruments propres à Internet permettant aux autorités compétentes de mener leurs investigations.[852] Dans ce contexte, il est essentiel de disposer d'instruments permettant d'identifier les délinquants et de réunir les preuves nécessaires aux poursuites pénales.[853] Ces instruments peuvent être les mêmes que ceux utilisés dans les enquêtes de terrorisme traditionnel non lié à la technologie informatique. Cependant, dans un nombre croissant de cas liés à l'Internet, les moyens d'enquête traditionnels ne suffisent pas à identifier un délinquant. L'interception de communication utilisant la voix sur IP (VoIP) en est un exemple.[854] Au cours des dernières décennies, les états ont conçu des instruments d'enquête, comme les écoutes téléphoniques, qui leur permet d'intercepter les communications téléphoniques fixes et mobiles.[855] L'interception des appels vocaux traditionnels est habituellement exécutée par l'intermédiaire des opérateurs téléphoniques.[856] Pour appliquer le même principe à la VoIP, les agences de répression doivent s'adresser aux fournisseurs d'accès Internet (FAI) et aux fournisseurs de services de VoIP. Toutefois, si le service est basé sur une technologie peer-to-peer, le fournisseur de services est généralement incapable d'intercepter les communications, car les données concernées sont transférées directement entre les deux protagonistes de la communication.[857] Par conséquent, il est nécessaire de se doter de nouvelles solutions techniques assorties d'outils juridiques adaptés.

3.2.14 Technologies de chiffrement

Autre facteur susceptible de compliquer les enquêtes sur les cyberdélits: les technologies de chiffrement[858]. Ces technologies sont destinées à protéger l'accès aux données par des personnes non autorisées. Elles constituent aussi une solution technique majeure de la lutte contre la cybercriminalité[859]. Le chiffrement est une technique qui consiste à convertir un texte clair dans un format indéchiffrable en utilisant un algorithme[860]. De même que l'anonymat, le chiffrement est un domaine scientifique ancien[861], qui a évolué grâce à la technologie informatique. Pendant longtemps, ce domaine a été soumis au secret, mais dans un environnement connecté il est difficile de le maintenir[862].

Il est aujourd'hui possible de chiffrer des données informatiques grâce à la disponibilité généralisée d'outils logiciels simples et à l'intégration des technologies de chiffrement aux systèmes d'exploitation[863], ce qui

complique la tâche des agences de répression qui sont confrontées à des données chiffrées.[864] Divers logiciels sont disponibles et permettent aux utilisateurs de protéger leurs fichiers contre toute intrusion non autorisée[865], mais on ne sait pas avec certitude dans quelle mesure les cyberdélinquants utilisent les technologies de chiffrement pour dissimuler leurs activités[866]. Une étude sur la pédopornographie avance que seulement 6 % des personnes arrêtées pour possession de matériel pornographique mettant en scène des enfants utilisent des technologies de chiffrement[867], mais les experts craignent toutefois une augmentation de l'utilisation de ces technologies dans les cyberdélits[868].

Différentes stratégies techniques existent pour forcer les données chiffrées et plusieurs logiciels permettant d'automatiser ces processus sont disponibles[869]. Ces stratégies vont de l'analyse[870] des faiblesses des logiciels de chiffrement utilisés,[871] la recherche des phrases de chiffrement [872] et les essais de mots de passe usuels, aux attaques de type « force brute » longues et complexes. Le terme « attaque par force brute » est utilisé pour décrire le processus d'identification d'un code en testant toutes les combinaisons possibles[873]. En fonction de la technique de chiffrement et de la taille de la clé, ce processus peut prendre des décennies[874]. Avec un logiciel de chiffrement d'une longueur de clé de 20 bits, l'espace de la clé est d'environ un million. Un ordinateur récent effectuant un million d'opérations par seconde permettrait de briser le code en moins d'une seconde. Pour un chiffrement avec une longueur de clé de 40 bits, le temps nécessaire pourrait atteindre deux semaines[875]. En 2002, le Wall Street Journal a pu déchiffrer des fichiers trouvés sur un ordinateur de l'organisation terroriste Al Qaeda qui étaient chiffrés avec une longueur de clé de 40 bits[876]. En utilisant un chiffrement en 56 bits, il faudrait jusqu'à 2 285 ans à un seul ordinateur pour briser le chiffrement, et si un cyberdélinquant utilise une clé de chiffrement en 128 bits, un milliard de systèmes d'exploitation dédiés uniquement au chiffrement ne pourraient le briser qu'après des milliers de milliards d'années[877]. Or la dernière version du célèbre logiciel de chiffrement PGP permet de chiffrer des données avec une clé de 1 024 bits.

Les capacités des logiciels actuels dépassent largement le simple chiffrement de fichiers unitaires. La dernière version du système d'exploitation de Microsoft par exemple permet de chiffrer la totalité d'un disque dur[878]. Par ailleurs, l'installation d'un logiciel de chiffrement est aisée. Si certains experts informatiques spécialisés en criminalistique ne s'en effraient pas[879], il n'en reste pas moins qu'en généralisant l'accès à cette technologie, on risque d'encourager son utilisation. Certains outils permettent aussi de chiffrer les communications, notamment le courriel et les appels téléphoniques[880] – qui peuvent être passés en utilisant un service VoIP[881]. Les cyberdélinquants y ont recours pour protéger leurs conversations des écoutes[882].

Il est également possible de combiner les techniques. Certains logiciels permettent par exemple de chiffrer des messages et de les échanger sous forme d'images ou de photographies. Cette technique porte le nom de stéganographie[883]. Faire la distinction entre une photo de vacances et une photo dans laquelle des messages chiffrés ont été cachés n'est pas chose aisée pour les agences de répression.[884]

Pour les services de répression, l'accès aux techniques de chiffrement et leur utilisation par des délinquants sont problématiques. Plusieurs approches juridiques sont actuellement examinées[885]: possibilité d'obliger les développeurs de logiciels à installer une porte dérobée (*back-door*) à l'usage des services de répression, restrictions sur la puissance de chiffrement, obligation pour les personnes faisant l'objet d'une instruction pénale de révéler leurs clés[886]. Il importe toutefois de rappeler que les techniques de chiffrement ne relèvent pas exclusivement de l'infraction, mais qu'elles sont utilisées, de diverses manières, à des fins tout à fait licites pour protéger des données sensibles, ce qui requiert un accès suffisant aux techniques de chiffrement. Étant donné le nombre croissant d'attaques informatiques[887], l'autoprotection est un élément essentiel de la cybersécurité.

3.2.15 Résumé

Les enquêtes sur les cyberdélits et la poursuite en justice de leurs auteurs présentent pour les services de répression plusieurs types de difficulté. Il est donc essentiel non seulement de former les membres des services de répression, mais également d'élaborer une législation suffisante et efficace en la matière. Cette section a permis de faire le point sur les enjeux clés en matière de promotion de la cybersécurité et de mettre en avant les secteurs pour lesquels les instruments en vigueur peuvent se révéler insuffisants ou qui requièrent éventuellement la mise en œuvre d'instruments spécifiques.

3.3 Difficultés juridiques

3.3.1 Difficultés liées à l'élaboration de la législation pénale au niveau national

L'existence d'une législation satisfaisante est la clé de voûte des enquêtes sur la cybercriminalité et de la poursuite en justice des auteurs de cyberdélits. Mais la tâche du législateur est doublement difficile: il doit, d'une part, tenir compte en permanence des évolutions d'Internet et, d'autre part, contrôler l'efficacité des dispositions législatives en vigueur, mission d'autant plus importante que les technologies réseau évoluent rapidement.

Peu après l'apparition des nouvelles technologies, les services informatiques et les technologies fondées sur Internet ont donné lieu à de nouvelles formes de criminalité. Ainsi, le premier accès non autorisé à des réseaux informatiques date des années 70, soit peu de temps après leur invention[888]. De même, les premières infractions (des copies illégales de produits logiciels) ont suivi de peu la commercialisation des premiers ordinateurs personnels dans les années 80.

Or, adapter la législation pénale d'un pays dans le but de sanctionner de nouvelles formes de cyberdélits prend du temps. Certains pays n'ont d'ailleurs pas encore terminé ce processus d'ajustement. Il est nécessaire de passer en revue et de mettre à jour les différentes infractions sanctionnées par la législation pénale au niveau national et, notamment, d'accorder aux données numériques la même importance qu'aux signatures et aux documents imprimés traditionnels[889]. Pour que les infractions en matière de cybercriminalité puissent faire l'objet de poursuites, il faut qu'elles soient légalement reconnues.

La principale difficulté tient au fait qu'il existe un délai entre la prise de conscience d'une utilisation abusive potentielle des nouvelles technologies et l'adoption des modifications nécessaires de la législation nationale en matière pénale. Face à l'accélération des innovations dans le monde des réseaux, cette difficulté est plus réelle et plus actuelle que jamais. Bien des pays s'emploient d'ailleurs activement à rattraper leur retard sur le plan législatif[890]. Le processus d'ajustement législatif s'effectue en général en trois étapes: l'ajustement de la législation nationale, l'identification des vides juridiques dans le Code pénal et l'élaboration d'une nouvelle législation.

L'ajustement de la législation nationale doit commencer par la reconnaissance d'une utilisation abusive des nouvelles technologies

Les agences de répression nationales doivent disposer de départements spécialisés dans l'étude des nouveaux cyberdélits potentiels. La mise en place d'équipes d'intervention rapide en cas d'urgence informatique (CERT)[891], d'équipes d'intervention en cas d'incident informatique (CIRT) et d'équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) et autres structures de recherche peut améliorer la situation;

Le recensement des vides juridiques dans le Code pénal.

Pour établir une base législative efficace, il est nécessaire de confronter les dispositions pénales énoncées dans le droit national avec les obligations découlant des nouvelles infractions relevées. Dans de nombreux cas, on a affaire à de nouvelles variantes d'infractions existantes, qui peuvent entrer dans le champ de dispositions déjà en vigueur (par exemple, telles dispositions concernant la falsification seront facilement applicables aux documents électroniques). Des aménagements législatifs ne s'imposent donc que pour les infractions qui ne figurent pas ou sont insuffisamment prises en compte dans la législation nationale;

L'élaboration d'une nouvelle législation

L'expérience nous apprend que les autorités nationales ont parfois des difficultés à procéder à l'élaboration des lois sur la cybercriminalité sans l'aide internationale, du fait de l'évolution rapide des technologies réseau et de leurs structures complexes[892]. Un pays peut en effet difficilement engager seul un tel processus sans risquer de faire double emploi et de gaspiller les ressources. Il doit également suivre l'évolution des normes et des stratégies internationales. Sans une harmonisation internationale, la lutte contre la cybercriminalité transnationale se heurtera au manque de cohérence et à l'incompatibilité des législations nationales et donc à de graves difficultés. Les initiatives internationales visant à harmoniser les dispositions pénales adoptées au niveau de chaque pays sont par conséquent plus essentielles que jamais[893]. Les

législations nationales peuvent tirer un bénéfice considérable de l'expérience des autres pays et de l'expertise juridique internationale.

3.3.2 Nouvelles infractions

La plupart des délits commis à l'aide des TIC ne sont pas, à proprement parler, de nouveaux délits, mais des escroqueries qui ont été adaptées à Internet. C'est le cas par exemple de la fraude: il y a peu de différence entre l'envoi d'une lettre dans le but de tromper son destinataire et l'envoi d'un courriel avec la même intention[894]. Si la fraude est déjà considérée comme une infraction pénale, il n'est peut-être pas nécessaire de modifier la législation afin de sanctionner pénalement les actes de fraude informatique.

La situation est différente si les actes commis ne sont pas connus de la législation en vigueur. Certains pays, qui disposaient d'une législation suffisante pour lutter contre la fraude ordinaire, mais pas contre les infractions dont la victime est un système informatique et non un être humain, ont dû adopter de nouvelles lois pour sanctionner pénalement la fraude informatique. On pourrait citer de nombreux exemples qui montrent que la large interprétation de dispositions existantes ne peut se substituer à l'adoption de nouvelles lois.

Si les dispositions concernant les escroqueries bien connues doivent faire l'objet d'ajustements, le législateur doit aussi analyser en permanence les nouveaux types de cyberdélit pour veiller à ce qu'ils soient sanctionnés de façon efficace. Le vol et la fraude dans les jeux informatiques et dans les jeux en ligne sont des exemples de cyberdélits non encore pénalisés dans tous les pays[895]. Pendant longtemps, les études sur les jeux en ligne ont porté prioritairement sur des questions de protection de la jeunesse (obligation de vérification de l'âge par exemple) et sur les contenus illicites (pédopornographie dans le jeu en ligne *Second life*, etc.)[896]. Or de nouvelles infractions sont découvertes tous les jours, tel le « vol » de monnaies virtuelles dans des jeux en ligne et leur revente sur des plates-formes d'enchères[897]. Certaines monnaies virtuelles ont en effet une valeur monétaire réelle (sur la base d'un taux de change), ce qui donne à l'infraction une dimension « réelle »[898]. De tels délits n'étant pas nécessairement sanctionnés dans tous les pays, il est essentiel de suivre les évolutions au niveau mondial afin d'empêcher l'apparition de refuges pour cyberdélinquants.

3.3.3 Utilisation croissante des TIC et besoin de nouvelles méthodes d'investigation

Pour préparer et commettre leurs infractions, les cyberdélinquants utilisent les TIC de manières diverses et variées[899]. Les services de répression doivent donc disposer d'outils appropriés pour enquêter sur les délits en préparation. Or certains mécanismes (conservation des données[900]) peuvent porter atteinte aux droits des internautes innocents[901]. Si la gravité de l'infraction est sans commune mesure avec l'importance du préjudice, le recours à ces mécanismes peut être injustifié, voire illégal, ce qui explique pourquoi plusieurs pays n'ont pas encore mis en place certains mécanismes susceptibles de faciliter les enquêtes.

La mise en place d'une nouvelle méthode d'investigation est toujours le résultat d'un compromis entre les avantages qu'elle procure aux services de répression et l'atteinte qu'elle porte aux droits des internautes innocents. À cet égard, il est essentiel de suivre en permanence les activités criminelles afin d'estimer si le niveau de la menace évolue. Si la mise en place de nouvelles méthodes a souvent été justifiée par la nécessité de « combattre le terrorisme », il s'agit plus d'une motivation poussée à l'extrême que d'une justification *per se*.

3.3.4 Elaboration de procédures visant à collecter des données numériques

Du fait notamment de leur faible coût[902] de stockage en comparaison des documents sur papier, le nombre de documents numériques croît constamment[903]. La numérisation et l'utilisation émergente des TIC ont des effets considérables sur les procédures relatives à la collecte d'éléments de preuve et sur l'utilisation de ces éléments au cours des procès[904]. En réponse à ces évolutions, les contenus numériques ont été acceptés comme nouvelles sources de preuve[905]. Ils désignent toutes les données stockées ou transmises à l'aide de la technologie informatique venant étayer les hypothèses relatives aux modalités de la commission d'une infraction[906]. La prise en compte des données numériques en tant qu'éléments de preuve s'accompagne de difficultés bien spécifiques et requiert des procédures spéciales[907]. L'un des problèmes les plus délicats est

de maintenir l'intégrité des données numériques[908], elles sont très fragiles et peuvent être facilement effacées[909] ou modifiées. Cela vaut tout particulièrement pour les données stockées en mémoire RAM, automatiquement effacées à l'arrêt des systèmes[910], qui, pour être conservées, nécessitent des techniques spéciales[911]. Par ailleurs, ce domaine connaît des évolutions permanentes, dont l'impact sur la gestion des éléments de preuve au format numérique peut être considérable. Pour preuve, le *Cloud computing* ou « informatique en nuage ». Les enquêteurs pouvaient autrefois concentrer leurs recherches sur les données informatiques trouvées sur les lieux. Ils doivent aujourd'hui tenir compte du fait que les données numériques peuvent être stockées à l'étranger et que le suspect y accède à distance uniquement lorsque cela est nécessaire.[912]

Les éléments de preuve numériques jouent un rôle essentiel dans plusieurs phases du travail d'enquête sur les cyberdélits. On peut en général distinguer quatre phases[913]. La première phase est l'identification des éléments de preuve pertinents[914], elle est suivie de la phase de collecte et archivage des éléments de preuve[915]. La troisième phase englobe l'analyse de la technologie informatique et des éléments de preuve numériques, puis, enfin, la dernière phase est la présentation des éléments de preuve au tribunal.

Outre les procédures relatives à la présentation des éléments de preuve numériques au tribunal, les modalités de collecte de ces éléments demandent une attention particulière. Cette collecte relève en fait de la « criminalistique informatique », terme qui désigne l'analyse systématique des équipements informatiques et de télécommunication dans le but de trouver des éléments de preuve numériques[916]. Étant donné que la quantité d'information stockée au format numérique augmente constamment, les enquêteurs sont confrontés à des problèmes de logistique[917]. Il est donc important qu'ils appliquent des procédures automatisées, notamment des recherches fondées sur les valeurs de hachage pour trouver des images pornographiques connues mettant en scène des enfants[918] ou des recherches par mots-clés[919], outre les méthodes de recherche manuelles[920].

Selon les besoins de chaque enquête, les experts en criminalistique informatique peuvent par exemple analyser les matériels et les logiciels utilisés par le suspect[921], aider les enquêteurs à identifier les éléments de preuve pertinents[922], récupérer des fichiers effacés[923], décrypter des fichiers[924] et identifier des internautes en analysant des données relatives au trafic[925].

[721] See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf ; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[722] Regarding hash-value based searches for illegal content, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

[723] For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp

[724] In 2014 Facebook alone reported 829 million daily active users and 1.32 billion monthly active user. Source: http://newsroom.fb.com/company-info/.

[725] See for example: *Chaabane/Kaafar/Boreli*, Big Friend is Watching You: Analyzing Online Social networks Tracking Capabilities, Proceedings of the 2012 ACM workshop on online social networks, page 7 et seq.

[726] See in this regard: *Daniel*, Cellular Location Evidence for Legal Professionals, 2014.

[727] Regarding the development see: The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

[728] Regarding the process see: *Rlamondon/Srihari*, On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey, ICC Transactions on pattern Analysis and machine Intelligence, Vol. 22, No.1, 2000, page 63 et seq.

[729] The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

[730] *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

[731] *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

[732] It was reported that the United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[733] Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

[734] See *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[735] *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[736] Regarding the impact of attacks, see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[737] A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[738] *Shimeall/Williams/Dunlevy*, Countering cyber war, NATO review, Winter 2001/2002, page 16, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

[739] One analysis by "Red Sheriff" in 2002 stated that more than 90 per cent of users worldwide use Microsoft`s operating systems (source: www.tecchannel.de – 20.09.2002).

[740] Regarding the discussion on the effect of the monoculture of operating systems on cybersecurity, see *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf;

Warning: Microsoft 'Monoculture', Associated Press, 15.02.2004, available at www.wired.com/news/privacy/0,1848,62307,00.html; *Geer and others*, CyberInsecurity: The Cost of Monopoly, available at: http://cryptome.org/cyberinsecurity.htm

741 With regard to the effect of spam on developing countries, see: Spam issues in developing countries, 2005, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

742 Regarding the integration of developing countries in the protection of network infrastructure, see: Chairman's Report on ITU Workshop On creating trust in Critical Network Infrastructures, available at: www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

743 WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services over long distances. For more information, see: The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX Technology for Broadband Wireless Access.

744 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf

745 See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

746 Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

747 See below: § 4.

748 According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

749 See *Wallsten*, Regulation and Internet Use in Developing Countries, 2002, page 2.

750 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

751 An example for new technology in this area is WiMAX (Worldwide Interoperability for Microwave Access), a standards-based wireless technology that provides broadband connections over long distances. Each WiMAX node could enable high-speed Internet connectivity in a radius of up to 50 km. For more information, see: The WiMAX Forum at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

752 Regarding the necessary steps to improve cybersecurity, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

753 The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: § 2.9.4.

754 Regarding hash-value based searches, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

755 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law). For more information, see *Moore*, Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law, available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.

756 "World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr/

757 "Websense Security Trends Report 2004", page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

758 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

759 In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime. See below: § 6.2.15.

760 Regarding the costs, see: The World Information Society Report, 2007, available at: www.itu.int/wisr/

761 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

762 For more information, see: *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

763 With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

764 One example of an approach to restrict the use of public terminals for criminal offences is Art. 7 of the Italian Decree-Law No. 144. Decree-Law 27 July 2005, No. 144 – "Urgent measures for combating international terrorism". For more information about the Decree-Law, see for example the article "Privacy and data retention policies in selected countries", available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

765 See below: § 6.5.13.

766 Regarding the impact of censorship and control, see: *Burnheim*, The right to communicate, The Internet in Africa, 1999, available at: www.article19.org/pdfs/publications/africa-internet.pdf

767 Regarding the question whether access to the Internet is a human right, see: *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; Regarding the declaration of Internet Access as a human right in Estonia, see: Information and Communications Technology, in UNDP Annual Report 2001, page 12, available at: www.undp.org/dpa/annualreport2001/arinfocom.pdf; Background Paper on Freedom of Expression and Internet Regulation, 2001, available at: www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

768 Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument.

769 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 a total of nearly 130 million websites at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

770 http://www.wikipedia.org

771 In the future development of the Internet, information provided by users will become even more important. "User generated content" is a key trend among the latest developments shaping the Internet. For more information, see*: O'Reilly*, What Is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software, 2005, available at: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

772 For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

773 See *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

774 One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

775 See *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003, page 112 *et seq.*, available at: www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf; *Brown/Carlyle/Salmerón/Wood*, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530, available at: www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

776 "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 per cent of all information required about the enemy". Reports vary as to the source of the quotation: The British High Commissioner Paul Boateng mentioned in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: *Boateng*, The role of the media in multicultural and multifaith societies, 2007, available at: www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624. The United States Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see:

www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites, see: *Knezo*, "Sensitive but Unclassified" Information and Other Controls: Policy & Options for Scientific and Technical Information, 2006, page 24, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

777 See Telegraph.co.uk, news from 13 January 2007..

778 See for example, *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004, available at: www.internetpolicy.net/governance/20040315paper.pdf;

779 For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff*, A Brief History of the Internet, available at: www.isoc.org/internet/history/brief.shtml.

780 *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

781 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/ *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et. seq*., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

782 For more information regarding anonymous communications, see below: § 3.2.l2..

783 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

784 The first and still most important communication protocols are: Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

785 See *Kahn/Lukasik*, Fighting Cyber Crime and Terrorism: The Role of Technology, presentation at the Stanford Conference, December 1999, page 6 *et seq.*; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

786 One example of the international cooperation of companies and delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system of the mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, page 429 *et seq.* (with notes *Sieber*).

787 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

788 Regarding the need for international cooperation in the fight against Cybercrime, see: *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

789 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

790 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in

Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

791 See below: § 3.2.10.

792 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142.

793 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

794 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, page 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

795 See: *Lewis*, Computer Espionage, Titan Rain and China, page 1, available at: www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

796 Regarding the extend of cross-border cases related to computer fraud, see: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 9, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

797 See below: § 6.6.12.

798 See below: § 6.6.

799 One example is phishing. Although most sites are still stored in the United States (32%), which has strong legislation in place, countries such as China (13%), Russia (7%) and the Republic of Korea (6%), which may have less effective instruments in the field of international cooperation in place, are playing a more important role. Apart from the United States, none of them has yet signed and ratified cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

800 This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: § 5.1.

801 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU. Regarding the effect of the worm on critical information infrastructure protection, see: *Brock*, ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: www.gao.gov/archive/2000/ai00181t.pdf.

802 BBC News, Police close in on Love Bug culprit, 06.05.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. Regarding the technology used, see: http://radsoft.net/news/roundups/luv/20000504,00.html.

803 See for example: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf..

804 One example of low-cost services that are automated is e-mail. The automation of registration allows providers to offer e-mail addresses free of charge. For more information on the difficulties of prosecuting cybercrime involving e-mail addresses, see: § 3.2.l2.

805 The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

806 For more details on the automation of spam mails and the challenges for law-enforcement agencies, see: *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

807 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

[808] The Online-Community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). Source: www.hackerwatch.org.

[809] Regarding the distribution of hacking tools, see: CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

[810] See CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

[811] Nearly 50 per cent of all fraud complains reported to the United States Federal Trade Commission are related to an amount paid between USD 0 and 25. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[812] See Spam Issue in Developing Countries, Page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[813] Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

[814] Regarding the attacks, see: Lewis, Cyber Attacks Explained, 2007, available at: www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; A cyber-riot, The Economist, 10.05.2007, available at: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007, available at: www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

[815] See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[816] See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf.

[817] See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, available at: www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, An Inside Look at Botnets, available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, BotNets: Detection and Mitigation.

[818] See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf.

[819] *Keizer*, Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, 21.10.2005, available at: www.techweb.com/wire/172303160

[820] See *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

[821] E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[822] "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: www.ic3.gov/media/initiatives/BotRoast.pdf.

[823] *Staniford/Paxson/Weaver*, How to Own the Internet in Your Space Time, 2002, available at: www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

[824] *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International, 2006, page 142.

[825] *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[826] Regarding the necessary instruments, see below: § 6.5. One solution that is currently being discussed is data retention. Regarding the possibilities and risks of data retention, see: *Allitsch*, Data Retention on the Internet – A measure with one foot offside?, Computer Law Review International 2002, page 161 *et seq.*

[827] The term "quick freeze" is used to describe the immediate preservation of data on request of law-enforcement agencies. For more information, see below: § 6.5.4.

[828] The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country. For more information, see below: § 6.6.8.

[829] The graphical user interface called World Wide Web (WWW) was created in 1989.

[830] The development of the graphical user interface supported content-related offences in particular. For more information, see above: § 2.6.

[831] For more information see above: § 2.6.5.

[832] Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at

www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

833 With regard to the interception of peer-to-peer based VoIP communications, law-enforcement agencies need to concentrate on carrying out the interception by involving the access provider.

834 Regarding the implications of the use of cell phones as storage media for computer forensics, see: *Al-Zarouni*, Mobile Handset Forensic Evidence: a challenge for Law Enforcement, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Al-Zarouni%20-%20Mobile%20Handset%20Forensic%20Evidence%20-%20a%20challenge%20for%20Law%20Enforcement.pdf.

835 On the advantages of wireless networks for the development of an IT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries", 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

836 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

837 Regarding the challenges related to anonymous communication, see: *Sobel*, The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity, Virginia Journal of Law and Technology, Symposium, Vol. 5, 2000, available at: www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

838 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

839 Regarding legislative approaches requiring identification prior to the use of public terminals, see Art. 7 of the Italian Decree-Law No. 144. For more information, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.* and below: § 6.5.14.

840 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

841 Regarding the difficulties that are caused if offenders use open wireless networks, see above: § 3.2.3.

842 Regarding technical approaches in tracing back users of anonymous communication servers based on the TOR structure, see: *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

843 See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

844 Regarding the possibilities of tracing offenders using e-mail headers, see: *Al-Zarouni*, Tracing Email Headers, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

845 *Donath*, Sociable Media, 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

846 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Regarding the benefits of anonymous communication see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

847 "(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services [...]". Source: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

848 Article 37 – Traffic and billing data "1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection". – Regulation (EC) no 45/2001 of

the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

849 See below: § 6.5.13.

850 Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

851 Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

852 This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

853 Regarding user-based approaches in the fight against cybercrime, see: *Goerling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

854 The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols. For more information, see: *Swale*, Voice Over IP: Systems and Solutions, 2001; *Black*, Voice Over IP, 2001.

855 Regarding the importance of interception and the technical solutions, see: *Karpagavinayagam/State/Festor*, Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection – ICIMP 2007. Regarding the challenges related to interception of data communication, see*: Swale/Chochliouros/Spiliopoulou/Chochliouros*, Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response, in *Janczewski/Colarik*, Cyber Warfare and Cyber Terrorism, 2007, page 424.

856 Regarding the differences between PSTN and VoIP communication, see: *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq.*

857 Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq*.

858 Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the mathematical background, see: *Menezes*, Handbook of Applied Cryptography, 1996, page 49 *et seq.*

859 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: 2006 E-Crime Watch Survey, page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

860 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

861 *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

862 *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58, page 143.

863 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

864 Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are

beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital
Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

865 Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see www.truecrypt.org).

866 Regarding the use of cryptography by terrorists, see: *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

867 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf..

868 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

869 Regarding the most popular tools, see: *Frichot*, An Analysis and Comparison of Clustered Password Crackers, 2004, page 3, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf. Regarding practical approaches in responding to the challenge of encryption see: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

870 See: Data Encryption, Parliament Office for Science and Technology No. 270, UK, 2006, page 3, available at: www.parliament.uk/documents/upload/postpn270.pdf.

871 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

872 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

873 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

874 *Schneier*, Applied Cryptography, page 185; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005, page 36, available at: www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

875 1 099 512 seconds.

876 *Usborne*, Has an old computer revealed that Reid toured world searching out new targets for al-Qaida?, The Independent, 18.01.2002, available at: http://www.independent.co.uk/news/world/americas/has-an-old-computer-revealed-that-reid-toured-world-searching-out-new-targets-for-alqaida-663609.html; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf. With further reference to the case: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

877 Equivalent to 10790283070806000000 years.

878 This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.

879 See *Leyden*, Vista encryption 'no threat' to computer forensics, The Register, 02.02.2007, available at: www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

880 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, Skype Security Evaluation, 2005, available at: www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

881 Phil Zimmermann, the developer of the encryption software PGP, developed a plug-in for VoIP software that can be used to install added encryption, in addition to the encryption provided by the operator of the communication services. The difficulty arising from the use of additional encryption methods is the fact that, even if the law-enforcement agencies intercept the communications between two suspects, the additional encryption will hinder the analysis. For more information on the software, see: *Markoff*, "Voice Encryption may draw US Scrutiny", New York Times, 22.05.2006, available at: www.nytimes.com/2006/05/22/technology/22privacy.html?ex=1305950400&en=ee5ceb136748c9a1&ei=5088. Regarding the related challenges for law-enforcement agencies, see: *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

882 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

883 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; *Labs*, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

884 For practical detection approaches, see: *Jackson/Grunsch/Claypoole/Lamont*, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, page 1 *et seq.*; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001.

885 See below: § 6.5.11.

886 See below: § 6.5.11.

887 See above: § 3.2.8.

888 See BBC News, Hacking: A history, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

889 An example of the integration of digital sources is Section 11, Subsection 3 of the German Penal Code: "Audio & visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection."

890 Within this process, the case-law based Anglo-American law system has advantages in terms of reaction time.

891 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 per cent of Internet systems to a halt in November 1988. For more information on the history of the CERT CC, see: www.cert.org/meet_cert/; *Goodman*, Why the Police don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.

892 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and UN Resolution 55/63.

893 See below: § 5.

894 See above: § 2.8.1.

895 Regarding the offences recognized in relation to online games, see above: § 2.6.5.

896 Regarding the trade of child pornography in Second Life, see for example BBC, Second Life "child abuse" claim, 09.05.2007, at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: http://secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy/.

897 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 *et seq.*

898 *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

899 Regarding the use of ICTs by terrorist groups, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16; *Hutchinson*, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf; *Gercke*, Cyberterrorism, Computer Law Review International 2007, page 64.

900 Data retention describes the collection of certain data (such as traffic data) through obliged institutions, e.g. access providers. For more details, see below: § 6.5.5.

901 Relating to these concerns, see: Advocate General Opinion, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

902 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

903 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

904 *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

905 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historic development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

906 *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

907 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq*.

908 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1.

909 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

910 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

911 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

912 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

913 Regarding the different models of cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also: *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

914 This includes the development of investigation strategies.

915 The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

916 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

917 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

918 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

919 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[920] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[921] This includes for example the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[922] This includes for example the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[923] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[924] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[925] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

4. Renforcement des capacités

Bibliography (selected): *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141*; Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf*; Henten/Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1; *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003*; Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf; *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et seq.*; *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

Du fait du nombre croissant des cyberdélits reconnus et de leurs victimes, même dans les pays en développement moins connectés, la cybersécurité et la cybercriminalité figurent désormais en bonne place parmi les priorités tant du secteur privé que des pouvoirs publics. Le développement des TIC est tellement rapide, tout particulièrement dans les pays en développement, qu'il est aujourd'hui essentiel d'élaborer et de mettre en œuvre des mesures anticybercriminalité efficaces. Le chapitre ci-après présente un aperçu des problèmes que rencontrent fréquemment les pays lorsqu'ils élaborent de telles mesures.

4.1 Cybersécurité et cybercriminalité

L'une des premières questions que se posent fréquemment les pays lorsqu'ils commencent à se préoccuper de la cybercriminalité est la suivante : cette démarche doit-elle s'inscrire dans le cadre de l'application de la loi ou de la cybersécurité ? La distinction entre ces deux domaines est difficile à opérer[926], dans la mesure où ils sont clairement connexes. Preuve en est que la Résolution sur la cybersécurité[927] adoptée en 2010 par l'Assemblée générale des Nations Unies traite de la cybercriminalité comme représentant un problème majeur. La cybercriminalité peut par conséquent être considérée comme faisant partie intégrante[928] de toute approche destinée à améliorer la cybersécurité, mais elle n'en reste pas moins une des composantes seulement d'une stratégie de cybersécurité. On perçoit ainsi la nature interdisciplinaire de ces deux sujets, et le fait qu'il est nécessaire que soient impliquées dans le processus différentes parties prenantes des pouvoirs publics. L'élaboration d'une réponse nationale à la cybercriminalité implique souvent la participation de différents ministères (Ministère de la justice, Ministère des communications, Ministère de l'éducation, etc.).

4.2 Méthode de renforcement des capacités

Une analyse des différentes approches en matière de renforcement des capacités nationales nécessaires pour lutter contre la cybercriminalité dans chaque pays permet d'identifier certains éléments essentiels qui peuvent être considérés comme des éléments de base d'une approche en matière de bonnes pratiques.

4.2.1 Organisation

Il convient avant tout de tenir une discussion ciblée dans le pays (et avec les organisations internationales qui apportent leur soutien) pour comprendre pleinement les attentes et être en mesure d'élaborer un plan ou une proposition de projet correspondant. Cette discussion doit porter sur divers points, notamment les suivants : le projet doit-il présenter une stratégie, une politique ou une législation, ou seulement de éléments de ces dernières ? Existe-t-il déjà des structures sur lesquelles le projet devrait reposer ? Quelles normes nationales, régionales ou internationales devraient être utilisées comme références pour une analyse comparative ? Quels sont les sujets à traiter (par exemple, la protection en ligne des enfants, la protection des données, la cybercriminalité ou la protection des données et les transactions électroniques) ? Le projet devrait-il également prévoir une formation des experts et/ou l'élaboration de matériel didactique ? Le pays bénéficie-t-il actuellement d'un quelconque autre soutien ? Il est extrêmement important de savoir où en sont les différentes activités pour coordonner les diverses activités d'appui.

4.2.2 Elaboration d'un plan de projet

A partir des résultats des discussions initiales, il est possible d'élaborer un plan de projet présentant plus en détail les activités, les experts concernés, les résultats attendus et un calendrier.

4.2.3 Une évaluation comme point de départ

Il est essentiel, pour mener un projet avec succès, de commencer par réaliser une évaluation adéquate. L'appui fourni ne peut être adapté aux besoins que si les responsables et les experts concernés connaissent la situation en ce qui concerne les composantes existantes (comme les politiques ou la législation), ainsi que les détails tels que les spécificités nationales en matière d'élaboration des lois. Cette évaluation doit notamment porter sur les capacités institutionnelles et l'identification des principales parties prenantes (par exemple les experts gouvernementaux, les associations professionnelles et les groupes d'intérêt comme les groupes de défense des libertés civiles).

4.2.4 Analyse comparative

Les résultats de l'évaluation donnent un aperçu de la situation actuelle, mais ne permettent pas de voir où se positionne un pays en fonction de certains points de référence. L'analyse comparative s'appuie sur les résultats de l'évaluation, mais comprend également un volet analytique. La comparaison repose sur la détermination de points de référence utilisés pour identifier les possibles lacunes et mettre en lumière les bonnes pratiques. Si le pays bénéficiaire est un petit pays insulaire du Pacifique et fait partie du Commonwealth, la législation nationale existante ou en projet pourra être comparée à la loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique, ainsi qu'à l'ossature de modèle régional du projet ICB4PAC destiné aux pays du Pacifique. D'autres normes pourraient être ajoutées à cette liste, comme la Directive de l'Union européenne relative aux attaques contre les systèmes d'information ou la Convention du Conseil de l'Europe sur la cybercriminalité. L'analyse débouchera sur un rapport complexe dans le cadre duquel les éléments nationaux identifiés et les éléments comparables des points de référence seront comparés ou répertoriés, les différences et les similarités seront mises en évidence et des recommandations seront faites.

4.2.5 Consultation des parties prenantes

Une autre bonne pratique en matière de renforcement des capacités consiste à organiser des consultations avec les parties prenantes. Les nombreuses années d'expérience dans le domaine du renforcement des capacités pour ce qui est de la stratégie, des politiques et de la législation montrent que les consultations avec les parties prenantes peuvent grandement renforcer le processus d'élaboration. Il est incontestablement plus laborieux d'examiner les éléments d'une politique nationale et d'un projet de législation avec des parties prenantes très diverses. Toutefois, la facilité avec laquelle le processus législatif a été mené, suite à des consultations avec les parties prenantes, dans les pays qui ont déjà effectué le

processus de transition montre qu'il est avantageux que des discussions intensives aient lieu lors du processus d'élaboration, afin qu'il soit tenu compte des différentes préoccupations.

Au cours de ces consultations organisées dans le pays, diverses parties prenantes nationales (par exemple le grand public, des politiciens, des fonctionnaires, des entrepreneurs et des professionnels, des fournisseurs de services Internet et des groupes de défense des libertés civiles) seront invitées à participer à des réunions de consultation au cours desquelles seront examinés les résultats des analyses et la marche à suivre proposée. Il sera pris note de l'avis des parties prenantes, dont on tiendra compte lors de l'élaboration des politiques et de la législation.

4.2.6 Processus d'élaboration

À partir de l'analyse comparative et des consultations avec les parties prenantes, les stratégies, les politiques et la législation pertinentes peuvent être élaborées ou modifiées. Dans le cadre de ce processus, on élabore généralement aussi des notes explicatives et d'autres documents (comme des notes d'information à l'intention du gouvernement).

4.2.7 Formation, enseignement et activités de suivi

Les stratégies, politiques et législations, aussi bonnes soient-elles, ne suffiront pas à lutter efficacement la cybercriminalité. D'autres mesures sont tout aussi importantes, comme la formation des professionnels et la sensibilisation du public. Les activités de formation sont par exemple des formations dans les écoles, adaptées à l'âge, sur la prévention de la criminalité, ou encore des simulations de cyberincidents en temps réel destinées à aider les hauts fonctionnaires à empêcher les attaques. Les activités de suivi comprennent souvent aussi une évaluation du projet.

4.3 La stratégie comme point de départ

Comme cela a été mentionné précédemment, la cybersécurité [929] joue un rôle essentiel dans le développement des technologies de l'information et des services Internet[930]. Le renforcement de la sécurité d'Internet (et de la protection des internautes) fait aujourd'hui partie intégrante du développement des nouveaux services, mais aussi des politiques gouvernementales[931]. Les stratégies de cybersécurité – par exemple, le développement de systèmes techniques de protection ou la prévention, par la formation, des victimes de la cybercriminalité – peuvent contribuer à la réduction des risques d'infraction dans le cyberespace[932].

Toute stratégie anticybercriminalité doit être intégrée à une stratégie de cybersécurité. Le Programme mondial cybersécurité de l'UIT [933], en tant que cadre mondial pour le dialogue et la coopération internationale, a pour but de coordonner la réponse internationale à donner aux enjeux de plus en plus pressants de la cybersécurité et d'améliorer la confiance et la sécurité dans la société de l'information. Il se situe dans le prolongement de travaux, d'initiatives et de partenariat existants, l'objectif étant de proposer des stratégies de niveau international pour faire face aux enjeux actuels. Toutes les mesures requises par les cinq grands axes du Programme mondial cybersécurité s'appliquent aux stratégies de cybersécurité, quelles qu'elles soient. En outre, lutter efficacement contre la cybercriminalité suppose de mettre en œuvre des mesures dans chacun des domaines représentés par les cinq grands axes[934].

4.3.1 Mise en œuvre de stratégies existantes

On pourrait envisager d'appliquer dans les pays en développement des stratégies de lutte contre la cybercriminalité élaborées dans les pays industrialisés, ce qui présenterait l'avantage de réduire les coûts et les temps de développement. Les pays en développement pourraient en outre bénéficier des connaissances et des expériences apportées par les pays industrialisés.

Cette démarche présente cependant plusieurs difficultés. Si les pays développés et les pays en développement rencontrent des problèmes similaires, il n'en reste pas moins que la solution optimale dépend des ressources et des capacités de chaque pays. Les pays industrialisés sont en mesure de

promouvoir la cybersécurité de multiples façons et avec plus de souplesse, par exemple en concentrant leur action sur des mesures de protection techniques plus coûteuses.

Les pays en développement qui souhaitent adopter des stratégies anticybercriminalité déjà en vigueur doivent s'interroger notamment sur la compatibilité des différents systèmes juridiques, la place à donner aux programmes de soutien (formation de la population, etc.), la portée des mesures d'autoprotection en place et enfin le degré de soutien du secteur privé (via des partenariats public-privé).

4.3.2 Différences régionales

Étant donné le caractère international de la cybercriminalité, l'harmonisation des législations et des techniques entre les pays est un élément essentiel de la lutte contre ce fléau. Il importe toutefois de prendre aussi en compte la demande au niveau régional ainsi que les moyens qui existent à ce niveau, et ce d'autant plus que les nombreuses normes juridiques et techniques adoptées d'un commun accord par les pays industrialisés n'intègrent pas nécessairement diverses caractéristiques importantes des pays en développement[935]. Il faut donc réussir à intégrer les facteurs régionaux et les différentes régionales d'une autre façon.

4.3.3 Importance des questions de cybercriminalité dans le cadre des grands axes sur la cybersécurité

Le Programme mondial cybersécurité comporte sept buts stratégiques principaux, qui s'articulent autour de cinq domaines de travail: 1) Cadre juridique, 2) Mesures techniques et de procédure, 3) Structures organisationnelles, 4) Renforcement des capacités, 5) Coopération internationale. Comme cela a été mentionné ci-dessus, les questions de cybercriminalité ont un rôle important à jouer dans chacun des cinq grands axes du Programme mondial cybersécurité. Le domaine de travail « Cadre juridique » se concentre sur la façon de répondre, de façon compatible à l'échelle internationale, aux problèmes juridiques que posent les activités criminelles commises sur des réseaux TIC.

4.3.4 Stratégies: au-delà de l'élaboration de plans futurs

Ces dernières années, certains pays ont élaboré des stratégies en matière de cybersécurité et de cybercriminalité [936], tout comme l'ont fait certaines organisations internationales et institutions intergouvernementales.[937] En comparant leurs différentes approches, on observe des similarités de taille.

La plupart des stratégies de cybersécurité et de cybercriminalité prennent la forme de documents assez courts (10 à 20 pages) qui ne présentent pas beaucoup de détails. Elles s'attachent à souligner la pertinence du sujet, à réaffirmer la volonté d'agir et à présenter des décisions générales sur ce qu'il conviendrait de faire pour améliorer la cybersécurité. La plupart des stratégies ne fournissent aucune solution ou mesure concrète. Le principe d'une stratégie est qu'elle propose une solution à une difficulté ou un problème donné ; elle n'a donc pas besoin d'être adaptée à chaque cas de figure, mais doit proposer des lignes directrices à suivre en cas de problème.[938] Par exemple, la stratégie de cybersécurité de l'Allemagne[939] dispose que le gouvernement allemand a prévu un plan d'action pour mettre en place des initiatives et se pencher sur les responsabilités des fournisseurs. Elle n'indique toutefois pas qui sera chargé de l'appliquer, ni de quelle manière les objectifs devraient être atteints.

Une stratégie très basique présente l'avantage de pouvoir être élaborée rapidement. En raison du caractère très général des principes définis, les mises à jour doivent être effectuées beaucoup moins fréquemment [940]. Une stratégie générale peut rester en place pendant des années avant qu'il soit nécessaire de la mettre à jour. Cette approche présente cependant aussi certaines difficultés. S'il est certain que le développement d'une approche globale ne nécessite pas que les mesures et les activités soient regroupées dans un même document, le fait d'avoir plusieurs documents peut mener à une incompatibilité des différentes mesures. L'expérience montre qu'en raison de la complexité des menaces, la moindre contradiction ou incohérence entre les différentes mesures peut fortement réduire l'efficacité tant de la prévention que de l'intervention en cas d'incident. Une stratégie ne sera pleinement efficace que si tous ses composants sont totalement cohérents et interdépendants.

On peut arriver à un compromis en définissant une stratégie très générale accompagnée de plans d'action concrets (et par là même plus détaillés). Cette approche offre la possibilité de montrer au grand public les efforts déployés en publiant une stratégie de cybercriminalité et de cybersécurité, tout en gardant confidentielles les mesures concrètes. Il peut être demandé instamment aux gouvernements de fournir un aperçu des activités menées dans le domaine de la cybercriminalité et de la cybersécurité, comme il peut être nécessaire pour les pays de disposer d'une stratégie nationale de cybersécurité pour attirer les investisseurs. Il n'est toutefois pas forcément acceptable de divulguer les détails relatifs aux mesures mises en place pour améliorer la cybersécurité et identifier les délinquants, étant donné que de telles informations pourraient être utilisées par les pirates pour identifier les faiblesses de ces mesures.

4.4 Pertinence d'une politique

Élaborer une législation pour pénaliser certains comportements ou introduire de nouveaux outils d'investigation est un processus plutôt inhabituel pour la plupart des pays. En premier lieu, la procédure normale est de définir une politique.[941] Une politique est comparable à une stratégie qui définit les différents instruments utilisés pour traiter un problème. Contrairement à une stratégie plus générale en matière de cybercriminalité qui peut concerner différentes parties prenantes, le rôle d'une politique est de définir la réponse apportée par le gouvernement à un problème spécifique.[942] Cette réponse n'est pas nécessairement limitée à un acte législatif, car les gouvernements ont à leur disposition une panoplie d'instruments susceptibles d'être utilisés pour atteindre les objectifs d'une politique. Et même lorsqu'il a été décidé de mettre en œuvre une législation, elle ne doit pas nécessairement cibler le droit pénal, mais peut également inclure des mesures plus ciblées sur la prévention de la délinquance. À cet égard, élaborer une politique permet à un gouvernement de définir de façon exhaustive la réponse gouvernementale à un problème donné. Comme la lutte contre la cybercriminalité ne peut se limiter à la seule mise en œuvre de dispositifs juridiques, mais englobe diverses stratégies et différentes mesures, la politique peut garantir que ces différentes mesures ne soient pas contradictoires.

Dans les différentes approches visant à harmoniser la législation en matière de cybercriminalité, trop peu de priorité a été accordée non seulement à l'intégration de la législation au cadre juridique national, mais également à son insertion dans une politique existante, ou à développer une nouvelle politique en la matière. Par conséquent, certains pays qui ont simplement adopté une législation en matière de cybercriminalité sans avoir élaboré de stratégie anti cybercriminalité ni de politique au niveau gouvernemental ont rencontré des difficultés majeures. Elles étaient essentiellement le résultat d'un manque de mesures de prévention de la criminalité et d'un chevauchement entre différentes mesures.

4.4.1 Responsabilités au sein du gouvernement

La politique permet l'ajustement des compétences pour un domaine au sein du gouvernement. Les redondances entre les différents ministères ne sont pas inhabituelles – en matière de cybercriminalité cela se produit fréquemment, car c'est un sujet interdisciplinaire.[943] Les différents aspects ayant trait à la lutte contre la cybercriminalité peuvent être du ressort du ministère de la Justice, du ministère de la Communication ou du ministère de la Sécurité nationale, pour n'en citer que trois. Dans le processus d'élaboration d'une politique, le rôle des différentes institutions gouvernementales impliquées peut être défini.

Cela est exprimé, par exemple, dans le projet de modèle de politique de l'ICB4PAC[944] sur la cybercriminalité:

> *Il est crucial à cet égard que les responsabilités des différentes parties prenantes soient clairement définies. Ce point est particulièrement pertinent, car la cybercriminalité est un thème intersectoriel qui peut être du ressort de différentes institutions telles que les procureurs généraux, le ministère de la Communication et autres.*

4.4.2 Définition des différentes composantes

Comme indiqué précédemment, la politique peut être utilisée pour définir les différentes composantes d'une approche. Cela peut aller du renforcement des pouvoirs institutionnels (par exemple la police et la magistrature) à des amendements concrets de la législation (comme l'adoption d'une législation plus avancée).

C'est une autre question soulevée dans le projet de modèle de politique de l'ICB4PAC [945] sur la cybercriminalité:

> *Relever les défis multidimensionnels de la lutte contre la cybercriminalité suppose une approche exhaustive qui doit englober des politiques globales, la législation, l'éducation et la sensibilisation, le renforcement des capacités, la recherche ainsi que les approches techniques.*

Idéalement, la politique devrait être utilisée pour coordonner les différentes activités — même si elles sont mises en œuvre par différents ministères et organes gouvernementaux. Par conséquent, le fait que les politiques requièrent généralement une approbation par un cabinet permet non seulement l'identification des différents organes gouvernementaux et ministères impliqués eu égard au domaine concerné, mais également l'harmonisation de leurs activités.[946]

4.4.3 Définition des parties prenantes

La politique peut non seulement identifier les institutions gouvernementales impliquées, mais également des parties prenantes qui devraient être concernées. Il peut s'avérer nécessaire, par exemple, d'élaborer des lignes directrices eu égard à l'implication du secteur privé.

Par exemple, la question des parties prenantes qui devraient être impliquées et concernées est abordée dans le projet de modèle de politique de l'ICB4PAC[947] sur la cybercriminalité:

> *Par ailleurs, une telle approche doit impliquer divers acteurs tels que le gouvernement, les ministères et les agences gouvernementales, le secteur privé, les établissements scolaires et universités, les chefs coutumiers, la communauté, les institutions internationales et régionales, les services de répression, les juges, les douanes, les magistrats, les avocats, la société civile et les O.N.G.*

4.4.4 Identification des référentiels

Comme souligné ci-après, l'importance de l'harmonisation des législations est une priorité clé identifiée par différentes organisations régionales.[948] Mais le besoin d'harmonisation ne se limite pas à la législation – il englobe des sujets tels que la stratégie et la formation des experts.[949] La politique peut être utilisée pour identifier les domaines où une harmonisation est nécessaire et pour définir les normes régionales ou internationales à mettre en œuvre.

Par exemple, l'importance de l'harmonisation est traitée par le projet de modèle de politique de l'ICB4PAC[950] sur la cybercriminalité.

> *Eu égard à la dimension mondiale de la cybercriminalité et à la nécessité de protéger les utilisateurs d'Internet dans la région afin qu'ils ne soient pas victimes de la cyberdélinquance, les mesures visant à renforcer les capacités pour lutter contre la cybercriminalité doivent bénéficier d'une priorité élevée. Les stratégies, et en particulier la législation élaborée pour relever les défis de la cybercriminalité, devraient d'une part être alignées sur les normes internationales et d'autre part prendre en compte les spécificités régionales.*

Un autre exemple avec le modèle de politique de l'HIPCAR sur la cybercriminalité[951].

> *Des dispositions couvriront les formes de cybercriminalité les plus courantes et les plus largement reconnues à l'échelle internationale, ainsi que les infractions d'intérêt spécifique pour la région (par exemple, le spam). Afin de garantir la capacité à coopérer avec les services de répression dans les pays de la région et en dehors de la région, la législation sera compatible avec les normes et les meilleures pratiques internationales, ainsi qu'avec les normes et meilleures pratiques régionales existantes (dans la mesure du possible).*

4.4.5 Définition des questions clés pour la législation

La politique peut être utilisée pour définir les domaines clés qui doivent être traités par la législation. Cela peut inclure, par exemple, une liste des délits qui doivent être couverts. Le niveau de détail peut aller jusqu'au détail des dispositions qui devraient être intégrées à une loi sur la cybercriminalité.

Un exemple avec le modèle de politique de l'HIPCAR sur la cybercriminalité[952]:

> *Une disposition criminalisera la production, la vente et d'autres actes similaires liés à la pornographie infantile. À cet égard en particulier, il conviendra de prendre en compte les normes internationales. La législation devra par ailleurs prévoir la criminalisation de la possession de matériels pédopornographiques et de l'accès aux sites Internet de pornographie enfantine. Il conviendra d'accorder une exception aux services de répression afin qu'ils puissent mener leurs enquêtes.*

4.4.6 Définition des cadres juridiques qui nécessitent des amendements, des mises à jour ou des changements

Élaborer une législation sur la cybercriminalité n'est pas une tâche aisée, car différents domaines doivent être réglementés. Outre le droit pénal matériel et le droit procédural, la législation sur la cybercriminalité doit englober les questions ayant trait à la coopération internationale, à la preuve électronique et à la fiabilité du fournisseur d'accès Internet (FAI). Dans la plupart des pays, certains éléments d'une telle législation existent déjà — souvent dans des cadres juridiques différents. Des dispositions relatives à la cybercriminalité ne doivent pas nécessairement être mises en œuvre dans un seul instrument juridique. Eu égard aux structures existantes, il peut s'avérer nécessaire d'actualiser différents textes législatifs (par exemple amender une Loi sur la preuve pour garantir son applicabilité eu égard à l'admissibilité de la preuve électronique dans les procédures pénales) ou de supprimer certaines dispositions d'une ancienne loi (par exemple dans une loi sur les télécommunications) au cours du processus d'élaboration d'une nouvelle législation.

Cette approche consistant à mettre en œuvre une législation sur la cybercriminalité par un processus respectant les structures existantes est certainement plus complexe que de simplement mettre en œuvre une norme régionale ou une bonne pratique internationale mot à mot dans un texte législatif autonome. Mais, considérant que ce processus d'adaptation permet de ménager les traditions juridiques nationales, de nombreux pays favorisent cette approche.

La politique peut être utilisée pour définir les différents éléments qui devraient être intégrés et identifier les lois existantes qui nécessitent une actualisation.

4.4.7 Pertinence de la prévention de la criminalité

Malgré le fait que les menaces de sanctions peuvent prévenir la criminalité, la législation en matière de criminalité n'est pas axée sur la prévention, mais plutôt sur la sanction. Cependant, la prévention du crime est un élément-clé clairement identifié de toute lutte efficace contre la cybercriminalité.[953] Les mesures de prévention peuvent aller des solutions techniques (comme les pare-feux qui empêchent l'accès illicite à un système informatique et les logiciels antivirus qui peuvent empêcher l'installation de logiciels malveillants) au blocage d'accès à du contenu illégal.[954]

Importance de la prévention du crime et notamment soulignée par le projet de modèle de politique de l'ICB4PAC[955] sur la cybercriminalité:

Outre la criminalisation de la cybercriminalité et le renforcement des services de répression pour combattre la cyberdélinquance, des mesures de prévention doivent être développées. Au cours du processus de développement de ces mesures, qui peuvent aller des solutions techniques à la sensibilisation de l'utilisateur, il est important d'identifier les groupes méritant une attention particulière comme les jeunes, les populations accusant un retard technologique (comme les personnes vivant dans les villages isolés n'ayant aucune compétence technologique) et les femmes. Toutefois, les mesures de prévention de la délinquance doivent également s'adresser à des utilisateurs plus avancés et à des acteurs au fait de la technologie comme les fournisseurs d'infrastructures critiques (par exemple le secteur du tourisme ou le secteur financier). Le débat sur les mesures nécessaires doit englober l'éventail complet des instruments tels que le renforcement de la sensibilisation, la mise à disposition et la promotion gratuite de technologie de protection (comme les logiciels antivirus) et la mise en œuvre de solutions permettant aux parents de limiter l'accès à certains contenus. Idéalement, ces mesures doivent être disponibles lors du lancement d'un service ou d'une technologie et maintenues tout au long de son exploitation. Pour assurer une portée plus large à ces mesures, il y a lieu d'impliquer un panel exhaustif de parties prenantes allant des fournisseurs d'accès Internet aux gouvernements et institutions régionales, et d'explorer diverses sources possibles de financement.

4.5 Le rôle des régulateurs dans la lutte contre la cybercriminalité

Dans les décennies passées, les solutions envisagées pour traiter de la cybercriminalité étaient centrées sur la législation. Toutefois, comme cela a déjà été souligné dans le chapitre traitant de la stratégie anticybercriminalité, les composantes nécessaires d'une approche exhaustive pour lutter contre la cybercriminalité sont plus complexes. Récemment, l'attention s'est portée sur le rôle des régulateurs dans la lutte contre la cybercriminalité.

4.5.1 D'une réglementation des télécommunications à une réglementation des TIC.

Dans le contexte des télécommunications, le rôle de régulateur est largement reconnu.[956] Internet a érodé les vieux modèles de la division des responsabilités entre le gouvernement et le secteur privé, et l'on peut observer une transformation du rôle traditionnel des régulateurs dans le domaine des TIC et une évolution dans le ciblage de la réglementation des TIC.[957] Déjà aujourd'hui les autorités de réglementation des TIC se trouvent impliquées dans un éventail d'activités liées à la cybercriminalité. Cela est particulièrement vrai pour des domaines comme la réglementation de contenu, la sécurité des réseaux et la protection du consommateur, car les utilisateurs sont devenus vulnérables.[958] Par conséquent, l'implication des régulateurs est liée au fait que la cybercriminalité sape le développement de l'industrie et des produits et services de TIC.

Les nouveaux devoirs et les nouvelles responsabilités des régulateurs de TIC dans la lutte contre la cybercriminalité s'inscrivent dans une tendance plus générale vers la conversion de modèles de réglementation centralisée de la cybercriminalité en des structures flexibles. Dans certains pays, les régulateurs des TIC ont déjà exploré la possibilité de transférer le cadre des devoirs réglementaires ayant trait aux questions de concurrence et d'autorisation au sein du secteur des télécommunications vers la protection du consommateur au sens large, le développement sectoriel, la cyber sécurité, la participation à l'élaboration et à la mise en œuvre de politiques en matière de cybercriminalité qui inclut plus généralement l'utilisation des TIC et, par conséquent, les questions ayant trait à la cybercriminalité. Bien que de nouvelles autorités réglementaires avec des mandats et des responsabilités incluant la cybercriminalité aient été créées,[959] des régulateurs des TIC établis antérieurement ont élargi leurs missions existantes pour intégrer diverses activités visant à s'attaquer aux cybermenaces.[960] Toutefois, l'étendue et les limites de cet engagement font toujours débat.

4.5.2 Modèle pour l'élargissement des responsabilités du régulateur

Il existe deux modèles différents pour définir le mandat des régulateurs dans la lutte contre la cybercriminalité, notamment: l'interprétation large du mandat existant ou la création de nouveaux mandats.

La protection du consommateur et la sécurité des réseaux sont les deux domaines incombant traditionnellement au régulateur. Avec la mutation des services de télécommunications vers des services sur Internet, les objectifs de la protection du consommateur ont évolué. Outre les menaces traditionnelles, l'impact du spam, des logiciels malveillants et des botnets (réseaux d'ordinateurs zombies) doit être pris en compte. Un exemple d'élargissement de mandat vient de l'autorité indépendante des postes et télécommunications allemandes, l'OPTA. Le mandat[961] du régulateur inclut l'interdiction du spam[962] et la lutte contre la dissémination de logiciels malveillants.[963] Pendant le débat sur le mandat de l'OPTA, l'organisation a exprimé la nécessité d'établir un pont entre la cybersécurité en tant que domaine d'activité traditionnel et la cybercriminalité afin de traiter efficacement ces deux questions.[964] Si la cybercriminalité est considérée comme un échec de la cybersécurité, alors le mandat du régulateur se trouve automatiquement élargi.

La possibilité d'élargir le mandat du régulateur pour prendre en compte les questions liées à la cybercriminalité dépend également de sa structure institutionnelle, et de sa vocation multisectorielle (comme les commissions de services publics), ou de régulateur spécifique du secteur des télécommunications, ou de régulateur convergent. Bien que, du point de vue de la régulation du secteur des TIC, chaque modèle de structure institutionnelle a ses avantages et ses inconvénients[965], le type de structure institutionnelle doit être pris en compte au moment d'évaluer comment et dans quel domaine le régulateur des TIC doit être impliqué. Les régulateurs convergents, à la fois responsables des médias, du contenu et des services de TIC, sont généralement confrontés à la complexité des charges de travail. Cependant, leur mandat exhaustif peut-être un avantage s'agissant de traiter de problèmes de contenu, comme la pédopornographie ou d'autres contenus illicites ou nuisibles.[966] Dans un environnement convergent, là où les régulateurs de télécommunications traditionnels peuvent rencontrer des difficultés pour résoudre certains problèmes comme le rapprochement entre le contenu médiatique et les fournisseurs de services de télécommunications, le régulateur convergent semble être plus à même de traiter des problèmes de contenu en réseaux. Par ailleurs, le régulateur convergent peut éviter les incohérences et les incertitudes de régulation et une intervention réglementaire inégale à l'égard de différents contenus diffusés sur des plates-formes diverses.[967] Néanmoins, le débat sur les avantages du régulateur convergent ne doit pas minimiser l'importance des activités des régulateurs n'agissant que sur un seul secteur. Alors que, par exemple, à la fin de l'année 2009, l'Union européenne ne comptait que quatre régulateurs des TIC convergents,[968] un nombre bien plus important de régulateurs étaient concernés par la lutte contre la cybercriminalité.

Au moment d'envisager une interprétation large des mandats existants, la capacité du régulateur et la nécessité d'éviter les chevauchements avec les mandats d'autres organisations doivent être prises en compte. De tels conflits éventuels peuvent être résolus plus facilement si de nouveaux mandats sont clairement définis.

La seconde approche est la création de nouveaux mandats. Considérant l'éventualité de conflits de juridiction, des pays comme la Malaisie ont décidé de redéfinir les mandats afin d'éviter toute confusion et tout chevauchement. La Commission malaisienne des communications et du multimédia (MCMC), en tant que régulateur convergent, a créé un département spécial[969] chargé de la sécurité de l'information et de la fiabilité du réseau, de l'intégrité des communications et de l'infrastructure de communication critique.[970] Une approche similaire a été adoptée en Corée du Sud où, en 2008, la Commission coréenne des communications (KCC) a été créée par la fusion de l'ancien ministère de l'Information et de la Communication et de la Commission coréenne de la radiodiffusion. Entre autres missions, la KCC est chargée de la protection des utilisateurs d'Internet contre le contenu illégal ou nuisible.[971]

4.5.3 Exemples d'implication des régulateurs dans la lutte contre la cybercriminalité

Le champ d'action des régulateurs des TIC dans ce domaine, tout comme le modèle de définition du mandat des régulateurs, n'est pas encore clairement défini. Seuls quelques organes de réglementation des TIC disposent des pouvoirs effectifs pour aller au-delà de la réglementation des télécommunications et traiter des problèmes du secteur des TIC au sens large. Parce qu'ils opèrent dans un secteur en mutation et en développement rapide, les régulateurs des TIC sont exposés à de nouveaux domaines traditionnellement du ressort d'autres services et agences gouvernementales, voire du ressort d'aucune entité.[972] Même si le

régulateur possède *de facto* les compétences et l'expertise sectorielle nécessaires pour être impliqué dans la résolution de problèmes liés à la cybercriminalité, un mandat clair précisant leurs domaines d'influence est essentiel pour l'efficacité des régulateurs. Les domaines potentiels d'influence des régulateurs sont exposés ci-après:

Stratégies de politique globale

Le principe de la division des pouvoirs au sein de l'État[973] sépare l'élaboration de politique et la mise en œuvre.[974] Malgré l'importance de ce concept, la complexité de cette question peut imposer au régulateur d'apporter son conseil dans l'élaboration de la politique.[975] Forts de leur expertise sectorielle et de leurs réseaux de communication existants avec d'autres parties prenantes, les régulateurs de TIC jouent dans de nombreux pays un rôle important dans l'élaboration des politiques et stratégies pour le développement de l'industrie des TIC.[976] Dans certains pays, le rôle de conseil dans le cadre de l'élaboration des politiques est considéré comme l'une des tâches principales du régulateur des TIC.[977] Bien que cette pratique courante s'attache au conseil sur des questions ayant trait aux télécommunications, le mandat pourrait être élargi à la cybercriminalité. En Finlande, le gouvernement a mis sur pied un comité consultatif sur la sécurité de l'information (ACIS) sous l'égide de l'autorité finlandaise de régulation des communications (FICORA) aux fins de développer sa stratégie nationale d'information. [978] La proposition présentée par l'ACIS en 2002 identifie des objectifs et des mesures pour promouvoir une stratégie de sécurité de l'information. Plusieurs de ces mesures peuvent être considérées comme traitant de la cybercriminalité, et soulignent l'importance d'élaborer et d'améliorer une législation adaptée, une coopération internationale, une meilleure information-sensibilisation à la sécurité auprès des utilisateurs finaux.[979]

Implication dans l'élaboration d'une législation sur la cybercriminalité

L'organe compétent pour adopter une législation et le législateur, et non pas une autorité de réglementation. Toutefois, le régulateur des TIC peut jouer un rôle important dans le processus d'élaboration d'une législation sur la cybercriminalité. Eu égard à l'expérience des régulateurs dans les domaines de la protection des données, de la confidentialité des transmissions de données, de la prévention contre la diffusion de logiciels malveillants, d'autres aspects de la protection du consommateur et la responsabilité des FAI, leur implication est particulièrement souhaitable dans ces domaines.[980] Par ailleurs, le droit pénal n'est pas un domaine inconnu des régulateurs, puisque dans de nombreux pays les violations graves des obligations dans le domaine traditionnel couvert par le régulateur peuvent faire l'objet de sanctions pénales. Outre le rôle de conseil ayant trait aux stratégies globales exposé ci-dessus**,** les régulateurs peuvent être impliqués dans le processus de rédaction de législation. La Commission ougandaise des communications, par exemple, a été impliquée en tant que conseiller dans le processus de rédaction d'une législation sur la cybercriminalité. [981] De plus, la Commission ougandaise des communications, au travers du groupe de travail national ougandais sur la législation en matière de cybercriminalité, est désormais intégrée à une initiative régionale baptisée le Groupe de travail des états d'Afrique de l'Est sur la cyberlégislation, qui est chargé du processus en cours pour le développement et l'harmonisation de lois sur la cybercriminalité dans la région d'Afrique de l'Est.[982] En Zambie, l'autorité des communications [983] a participé à la rédaction d'une nouvelle législation sur la cybercriminalité, [984] notamment la loi Electronic Communications and Transactions Act de 2009.[985] Autre exemple avec la Belgique, où, en 2006, le régulateur belge des TIC (BIPT) a également pris part au processus de rédaction de la législation sur la cybercriminalité. Le projet a été élaboré en coopération avec le service public fédéral de la justice et l'unité fédérale de lutte contre la délinquance informatique.[986]

Détection et enquête de cybercriminalité

Les équipes d'intervention en cas d'incident informatique (CIRT - Computer Incident Response Team) jouent un rôle primordial en surveillant, détectant, analysant et enquêtant sur les cybermenaces et les cyberincidents.[987] À cause de la nature multisectorielle de la cybercriminalité, différentes CIRT ont été créées par un éventail de parties prenantes, notamment les gouvernements, les entreprises, les opérateurs de télécommunication et les universités, pour remplir des missions diverses.[988] Dans certains pays, la création et le fonctionnement des CIRT sont confiés aux régulateurs des TIC. Ces CIRT sont habituellement considérés non seulement comme des entités incontournables chargées de détecter les actes de cybercriminalité et d'enquêter au plan national, mais également comme des acteurs clés dans les actions visant à améliorer les coopérations internationales en matière de cybercriminalité. L'une des premières CIRT, créée à l'initiative du régulateur des TIC, est la CIRT Finlandaise, créée en janvier 2002 au sein de l'autorité finlandaise de régulation des communications (la FICORA).[989] On peut citer d'autres exemples en Suède,[990] aux Émirats Arabes Unis[991] et au Qatar.[992]

Faciliter l'application de la loi

Un régulateur des TIC ne peut que diligenter des enquêtes et, à cet égard, agir comme organe chargé d'appliquer la loi sur la base d'un mandat explicite qui lui est confié pour exercer et faire appliquer certaines dispositions légales. Dans certains pays, les régulateurs de TIC sont autorisés à agir en tant qu'organisme d'application de la loi dans des domaines ayant trait à la cybercriminalité comme la lutte antispam, la règlementation du contenu ou la mise en œuvre de mesures de coréglementation. Concernant le spam, certains régulateurs de TIC européens ont déjà adhéré à un réseau de contacts d'autorités de répression antispam créé par la Commission européenne en 2004 pour lutter contre le spam au niveau paneuropéen.[993] Le Groupe de réflexion de l'OCDE sur le spam établit également une liste des régulateurs de TIC agissant comme point de contact pour les agences d'application de la loi.[994] Des accords de coopération entre les régulateurs de TIC et les unités de lutte contre la cybercriminalité au niveau de la police existent également aux Pays-Bas et en Roumanie.[995]

4.5.4 Cadre juridique

Des cinq grands axes, le cadre juridique est probablement le plus pertinent en matière de stratégie de lutte contre la cybercriminalité.

Droit pénal matériel

Cela suppose tout d'abord de disposer des instruments juridiques de droit pénal nécessaires pour criminaliser des actes tels que la fraude informatique, l'accès illégal, l'atteinte à l'intégrité des données, les violations du droit d'auteur et la pédopornographie.[996] L'existence de telles dispositions dans le Code pénal applicables à des actes semblables commis hors du réseau ne signifie pas qu'elles puissent s'appliquer également aux actes commis sur Internet.[997] Par conséquent, il est indispensable de procéder à une analyse approfondie des lois nationales en vigueur pour identifier tout vide juridique possible.[998]

Droit pénal procédural

Hormis un dispositif de droit pénal,[999] les agences de répression ont besoin des outils et instruments nécessaires pour mener leurs enquêtes dans le domaine de la cybercriminalité.[1000] Ces enquêtes elles-mêmes présentent un certain nombre de difficultés.[1001] Les auteurs d'infraction peuvent agir depuis n'importe quel endroit du monde et prendre des mesures pour masquer leur identité.[1002] Les outils et instruments nécessaires aux enquêtes de cybercriminalité peuvent être très différents de ceux utilisés pour enquêter sur des délits conventionnels.[1003] À cause de la dimension internationale[1004] de la cybercriminalité, il est en outre nécessaire d'élaborer un cadre juridique national pour permettre la coopération avec d'autres agences de répression à l'étranger.[1005]

Preuve électronique

S'agissant de cybercriminalité, les autorités compétentes chargées d'enquêter, ainsi que les tribunaux, ont à faire avec la preuve électronique. Traiter ce genre de preuve présente un certain nombre de difficultés,[1006] mais offre également de nouvelles possibilités pour l'enquête et pour le travail des experts judiciaires.[1007] Dans les cas où aucune autre source de preuve n'est disponible, la capacité à identifier et à poursuivre un délinquant peut dépendre de la collecte et de l'évaluation d'une preuve électronique.[1008] Cela influence la manière dont les agences de répression et les tribunaux traitent de ces preuves.[1009] Là où les documents traditionnels sont versés en présentant l'original au tribunal, la preuve électronique suppose dans certains cas de disposer de procédures spécifiques qui ne permettent pas de la convertir en preuve traditionnelle, par exemple en présentant une version imprimée de fichiers ou d'autres données découvertes.[1010] Dans le contexte de la lutte contre la cybercriminalité, il est donc essentiel de disposer d'une législation permettant de traiter la question de l'admissibilité de la preuve.

Coopération internationale

À cause de la dimension transnationale d'Internet et de la mondialisation des services, un nombre croissant de cyberdélits revêtent une dimension internationale.[1011] Les pays souhaitant coopérer avec d'autres pays dans les enquêtes sur des délits transfrontaliers devront recourir à des instruments de coopération internationale.[1012] Pour se rendre compte de la nécessité d'une collaboration des autorités de répression et judiciaires et du défi à relever, il suffit de prendre en compte la mobilité des délinquants, l'inutilité de leur présence physique et l'impact du délit.[1013] En raison des différences entre le droit national et des instruments disponibles limités, la coopération internationale est considérée comme l'un des défis majeurs posés par la mondialisation de la criminalité. [1014] Dans le cadre d'une approche exhaustive de la cybercriminalité, les États doivent songer à renforcer leur capacité à coopérer avec d'autres États et l'efficacité de leurs procédures.

Responsabilité du fournisseur de service

La cybercriminalité peut difficilement se passer de l'utilisation des services d'un fournisseur d'accès Internet. Les courriels renfermant du contenu menaçant sont expédiés en utilisant les services d'un fournisseur de messagerie électronique, et le contenu illégal téléchargé depuis un site Web implique, entre autres, l'intervention d'un fournisseur d'hébergement et d'un fournisseur d'accès. Par conséquent, les FAI sont souvent au cœur des enquêtes impliquant des délinquants utilisant leurs services pour commettre une infraction.[1015] Considérant, d'une part, que la cybercriminalité ne peut avoir lieu sans l'entremise des FAI, et, d'autre part, que les fournisseurs d'accès n'ont souvent pas la possibilité d'empêcher ces délits, la question de savoir si la responsabilité des fournisseurs d'accès Internet doit être limitée se pose.[1016] Cette question peut être réglée dans le cadre d'une approche juridique exhaustive de la cybercriminalité.

4.5.5 Mesures techniques et de procédures

Les enquêtes sur les cyberdélits ont très souvent une forte composante technique[1017]. De plus, la nécessité de maintenir l'intégrité des éléments de preuve découverts pendant l'enquête requiert la mise en œuvre de procédures précises. Il est donc essentiel, pour lutter contre la cybercriminalité, de se donner les moyens et d'élaborer les procédures qui s'imposent.

Par ailleurs, étant donné qu'il est plus difficile d'attaquer des ordinateurs bien protégés, il importe de développer des systèmes de protection technique. Il s'agit, dans un premier temps, de se conformer à des normes de sécurité adéquates. Les modifications apportées aux systèmes bancaires en ligne (passage du TAN[1018] à l'ITAN[1019]) ont ainsi permis d'éliminer une grande partie des risques liés aux attaques actuelles par « hameçonnage », exemple qui illustre bien l'importance fondamentale des solutions techniques[1020]. Ces mesures doivent s'appliquer à tous les éléments de l'infrastructure technique, de l'infrastructure de base du réseau à tous les ordinateurs connectés dans le monde entier. Pour protéger les internautes et les entreprises, deux groupes cibles potentiels se dégagent: les utilisateurs et les entreprises en bout de chaîne (approche directe), et les fournisseurs d'accès et les éditeurs de logiciels.

D'un point de vue logistique, il peut être plus facile de privilégier la protection de l'infrastructure de base (réseau dorsal, routeurs, services essentiels, etc.) que d'inclure des millions d'utilisateurs dans une stratégie de lutte contre la cybercriminalité. On peut en effet estimer que la protection des internautes peut découler indirectement de la sécurisation des services qu'ils utilisent, par exemple les services bancaires. Cette approche indirecte permet de réduire le nombre de personnes et d'organisations nécessaires à la promotion des mesures de protection techniques.

Cela étant, si la limitation du nombre d'intervenants peut sembler souhaitable, il ne faut pas perdre de vue que les utilisateurs de l'informatique et d'Internet constituent souvent le maillon faible et la cible principale des infractions. Pour collecter des données sensibles, il est en effet souvent plus facile de viser des ordinateurs privés que les systèmes informatiques bien protégés des établissements financiers. Au-delà des problèmes logistiques, il est donc essentiel de protéger aussi l'infrastructure en bout de chaîne afin d'assurer la protection technique de l'ensemble du réseau.

Par ailleurs, les fournisseurs d'accès à Internet et les fabricants (éditeurs de logiciels, etc.) jouent un rôle essentiel dans les stratégies de lutte contre la cybercriminalité. Acteurs en contact direct avec les clients, ils sont garants des activités de sécurité (diffusion d'outils de protection et d'information concernant les escroqueries les plus récentes, etc.)[1021].

Structures organisationnelles

Pour lutter efficacement contre la cybercriminalité, il est nécessaire de disposer de structures organisationnelles très solides. En effet, c'est seulement en mettant en place de bonnes structures, qui ne se recoupent pas et reposent sur des compétences précises, qu'il est possible de mener des enquêtes complexes, qui exigent l'assistance de différents experts juridiques et techniques.

Renforcement des capacités et formation des utilisateurs

La cybercriminalité est un phénomène mondial. Pour être en mesure d'enquêter efficacement sur les infractions, il est nécessaire d'harmoniser les législations et de se donner les moyens de coopérer au niveau international. C'est en renforçant les capacités dans les pays développés, mais aussi dans les pays en développement, que l'on pourra garantir le respect des normes internationales[1022].

Il importe également de former les utilisateurs[1023]. En effet, certains cyberdélits – notamment ceux qui s'apparentent à la fraude, tels que l'hameçonnage (*phishing*) et l'espionnage (*spoofing*) – ne sont pas liés généralement à une absence de protection technique, mais plutôt à un manque de sensibilisation des victimes[1024]. On trouve certes sur le marché divers produits logiciels capables d'identifier automatiquement certains sites Internet malveillants[1025], mais aucun ne peut les identifier tous. Une stratégie de protection des utilisateurs exclusivement fondée sur les logiciels n'est donc pas totalement fiable[1026]. Aussi, malgré l'évolution permanente des mesures de protection technique et la mise à jour régulière des logiciels de protection, ces derniers ne peuvent encore se substituer à d'autres approches.

Parmi elles, la formation des utilisateurs, qui est l'une des composantes les plus importantes de la prévention de la cybercriminalité[1027]. Par exemple, des utilisateurs sensibilisés au fait que leur banque a pour principe de ne jamais les contacter par courriel pour leur demander leur mot de passe ou leurs coordonnées bancaires ne peuvent être victimes d'attaques par hameçonnage ou d'usurpation d'identité. La formation des internautes permet donc de réduire le nombre de cibles potentielles. Pour atteindre cet objectif, plusieurs moyens: les campagnes d'information publique, les cours dans les écoles, les bibliothèques, les centres de formation informatique et les universités, et enfin les partenariats public-privé (PPP).

Pour qu'une stratégie de formation et d'information soit efficace, il importe de faire connaître ouvertement les dernières cybermenaces en date. Or, certains États et/ou entreprises privées refusent de mettre en avant le fait que leurs clients et le grand public sont victimes de cyberdélits afin que ceux-ci ne perdent pas confiance dans les services de communication en ligne. Le Bureau fédéral d'enquête des États-Unis (FBI) a d'ailleurs explicitement demandé aux entreprises de surmonter leur réticence extrême à communiquer des informations négatives et de signaler les cas de cybercriminalité[1028]. Pour pouvoir correctement déterminer

le niveau des menaces et informer les utilisateurs, il est essentiel d'améliorer la collecte et la publication d'informations pertinentes[1029].

Coopération internationale

Les processus de transfert de données sur Internet font très souvent intervenir plusieurs pays[1030]. Ceci tient à la conception du réseau, mais aussi au fait que les protocoles chargés d'assurer la bonne transmission des données peuvent s'exécuter même en cas de blocage temporaire des lignes directes [1031]. De plus, un grand nombre de services Internet (services d'hébergement par exemple) sont proposés par des sociétés situées à l'étranger[1032].

Lorsque l'auteur de l'infraction ne se trouve pas dans le même pays que la victime, l'enquête nécessite la coopération des services de répression de tous les pays concernés [1033]. Or, en vertu du principe de souveraineté nationale, il est difficile de mener des enquêtes au niveau international ou transnational sans le consentement des autorités compétentes de l'ensemble des pays. Selon ce principe, un pays ne peut généralement pas mener d'enquêtes sur le territoire d'un autre pays sans la permission des autorités locales[1034]. Les enquêteurs doivent donc obtenir le soutien des autorités de tous les pays concernés. Étant donné que, dans la plupart des cas, le délai pendant lequel une enquête peut aboutir est très court, l'application, dans le cadre des enquêtes de cybercriminalité, des accords classiques d'entraide judiciaire pose de grandes difficultés. En effet, en règle générale, l'entraide judiciaire est tributaire de procédures formelles qui prennent beaucoup de temps. Il est donc absolument essentiel, dans l'élaboration et la mise en œuvre des stratégies de cybersécurité et de lutte contre la cybercriminalité, d'améliorer et de renforcer la coopération internationale.

4.6 Expériences du Groupe des États d'Afrique, des Caraïbes et du Pacifique (ACP) en matière de renforcement des capacités

Entre 2008 et 2013, l'UIT et l'UE ont cofinancé un projet[1035] visant à soutenir l'élaboration de politiques et législations dans les pays ACP, dans le cadre du programme "ACP-Technologies de l'information et de la communication" et du neuvième Fonds européen de développement. Les pays d'Afrique subsaharienne ont bénéficié du projet sur l'harmonisation des politiques relatives aux TIC en Afrique subsaharienne (projet HIPSSA), tandis que le projet visant à renforcer la compétitivité des pays des Caraïbes grâce à l'harmonisation des politiques, de la législation et des procédures réglementaires dans le domaine des TIC (projet HIPCAR) a été mis en oeuvre pour les pays des Caraïbes.[1036] Les pays du Pacifique ont également reçu un soutien, avec le projet sur le renforcement des capacités politiques, réglementaires et législatives dans le domaine des TIC des Etats insulaires de la région Pacifique (projet ICB4PAC). Au cours de ces six années, l'UIT a développé une méthodologie spécifique et a réalisé d'importants progrès en matière de renforcement des capacités.

4.6.1 Méthodologie

L'un des principaux résultats des projets est l'élaboration d'une méthodologie globale de renforcement des capacités dans le domaine de la stratégie/des politiques/de la législation, en vue de laquelle des exemples de bonnes pratiques en matière de méthodologie existante d'harmonisation régionale des politiques et de la législation ont été examinés. Toutefois, du fait du caractère unique du projet du point de vue du nombre de pays concernés (plus de 70 pays de trois régions), des domaines de travail (jusqu'à neuf) et du calendrier (six ans), il a été nécessaire de développer de nouvelles approches.

Pendant la première des deux phases des projets, des politiques et législations types au niveau régional ont été élaborées. Cette phase a débuté avec l'évaluation des politiques et législations existantes dans les pays bénéficiaires. Pour faire en sorte que toutes les lois applicables soient identifiées, cette évaluation a été menée par des experts internationaux et régionaux, avec le soutien d'interlocuteurs spécialisés dans chaque pays. Dans le rapport récapitulant les résultats, les normes existantes identifiées ont été comparées aux bonnes pratiques régionales et internationales, la priorité étant donnée à celles qui étaient directement applicables dans au moins certains des pays bénéficiaires (législation type du Commonwealth par exemple). Les bonnes pratiques d'autres régions, notamment de l'UE, ont toutefois également été prises en compte.

Les rapports d'évaluation[1037] ont présenté un aperçu de la législation existante, ainsi qu'une analyse comparative des législations existantes par rapport aux bonnes pratiques régionales et internationales. En vue de l'élaboration d'une analyse d'écart, le rapport d'évaluation a également identifié les besoins spécifiques régionaux qui n'étaient pas nécessairement pris en compte par les bonnes pratiques internationales. Il a ensuite fait l'objet d'une discussion avec les principales parties prenantes de tous les pays bénéficiaires, consultations suite auxquelles des politiques et législations types, ainsi que des notes explicatives, ont été élaborées pour tous les domaines de travail pertinents. Ce processus a été dirigé par des experts régionaux (de tous les pays bénéficiaires), afin de faire en sorte que les résultats ne soient pas seulement conformes aux bonnes pratiques régionales et internationales, mais qu'ils puissent aussi être facilement mis en œuvre.

La deuxième phase était consacrée à la transposition nationale, pour laquelle il a également été nécessaire d'élaborer une méthodologie individuelle. Compte tenu des délais serrés et du nombre de domaines de travail, il fallait que la méthodologie permette un soutien très efficace dans les pays. Une fois identifiés les différents modules de travail nécessaires, chaque pays a reçu un plan de projet pour un soutien personnalisé et individuel. Pour assurer le meilleur appui possible de la part des parties prenantes du pays, de vastes consultations ont été menées avec ces dernières dans le cadre de la transposition des politiques et législations types. Au cours de ces consultations, diverses parties prenantes nationales (par exemple le grand public, des politiciens, des fonctionnaires, des entrepreneurs et des professionnels, des fournisseurs de services Internet et des groupes de défense des libertés civiles) ont été invitées à participer à des réunions de consultation au cours desquelles elles ont pu débattre ouvertement du processus de transposition et de la politique et de la législation types. Lors du processus d'élaboration, mené conjointement par des experts locaux et régionaux/internationaux, il a été tenu compte de l'avis des parties prenantes. Par ailleurs, des ateliers de renforcement des capacités ont été organisés pour les différents groupes d'intérêts (par exemple, des formations spéciales pour la police, des sessions distinctes pour les juges, les magistrats et les procureurs, des conférences dans les écoles et les universités, des ateliers pour le grand public et des campagnes menées en coopération avec la presse locale).

4.6.2 Enseignements tirés

Le travail intensif réalisé avec plus de 70 pays a permis de dégager différentes bonnes pratiques qui pourraient s'avérer utiles pour les futurs projets de renforcement des capacités.

Un politique est nécessaire en sus de la législation

L'élaboration d'une législation est essentielle à la création d'un environnement fiable dans lequel utiliser les TIC.[1038] Il est toutefois inhabituel d'introduire une législation avant de mettre en place une stratégie et une politique, et la plupart des pays commencent par introduire une politique. Une politique a pour objectif de déterminer la réponse des pouvoirs publics face à un problème donné[1039]. Elle permet aux pouvoirs publics de déterminer une réponse globale à une difficulté donnée, ce qui peut comprendre, en plus de la législation, d'autres éléments de réponse qui peuvent être utilisés pour atteindre les objectifs de ladite politique. Contrairement à d'autres approches régionales axées sur l'harmonisation de la législation –telles que la Convention du Conseil de l'Europe sur la cybercriminalité[1040] - les projets HIPSSA, HIPCAR et ICB4PAC ont prévu l'élaboration de telles politiques, ce qui a permis de faciliter la coopération des différentes parties prenantes (en particulier entre ministères) dont les compétences dans le domaine des TIC se recoupent. Le fait de coupler une politique à une législation a certainement aussi permis de réduire le temps nécessaire à l'introduction de la législation au niveau national.

Des différences limitées entre législations types

Si l'on compare les différentes approches régionales (comme la Convention du Conseil de l'Europe sur la cybercriminalité[1041], la Décision-cadre de l'UE relative aux attaques visant les systèmes d'information[1042], le projet de Convention de l'Union africaine sur la cybersécurité[1043] et les projets HIPSSA, HIPCAR et ICB4PAC) utilisées pour faire face à des infractions concrètes (accès illégal par exemple), on constate que les approches et les méthodologies recommandées sont très cohérentes. Elles suivent toutes les bonnes

pratiques internationales et il a donc été possible d'utiliser la législation type élaborée par les experts des Caraïbes pour développer la structure type des projets HIPSSA et ICB4PAC.

Des normes élevées dans les pays en développement

Le projet fait apparaître que les normes élaborées par les petits pays et les pays en développement ne sont pas nécessairement inférieures aux normes de l'Europe. Plusieurs aspects des cadres juridiques vont même au-delà des normes européennes. La pornographie enfantine en est un exemple : l'article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité ne fait référence qu'à la "matière pornographique représentant de manière visuelle" un enfant et ne couvre par conséquent pas les données audio, alors que l'on sait parfaitement bien que les criminels échangent aussi des fichiers audio de pornographie enfantine.[1044] L'approche adoptée dans le cadre des projets HIPCAR, HIPSSA et ICB4PAC est différente, puisqu'on évite d'employer le terme "visuel" et que les fichiers audio sont par conséquent aussi visés.

Avantage d'une forte implication des experts et de la tenue de consultations avec les parties prenantes

Deux aspects se sont révélés fort utiles au cours de la phase de transition : l'implication d'experts de presque tous les pays bénéficiaires dans l'élaboration d'une politique et d'une législation types, et la forte implication des parties prenantes nationales dans le processus de transition.

Il ressort de l'évaluation qu'une forte implication d'experts de tous les pays bénéficiaires dans l'élaboration d'une norme régionale est très fructueuse. La Convention du Conseil de l'Europe sur la cybercriminalité a par exemple été élaborée par des experts de seulement 14[1045] des 47 États Membres et quatre experts d'Etats non Membres.[1046] À l'inverse, les politiques et législations types des projets HIPSSA, HIPCAR et ICB4PAC ont été élaborées par des experts de presque tous les pays bénéficiaires.

Une autre expérience positive a trait à la tenue de consultations avec les parties prenantes. Toutes les parties concernées sont convenues qu'il est bien plus difficile d'examiner les éléments d'une politique nationale et d'un projet de législation avec des parties prenantes très diverses, que de tenir des discussions en interne. Toutefois, la facilité avec laquelle le processus législatif a été mené suite à la participation des parties prenantes montre qu'il est avantageux que des discussions intensives aient lieu au cours du processus d'élaboration, pour faire en sorte de répondre aux différentes préoccupations.

926 Regarding a clear distinction see for example: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1, page 3.

927 NGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

928 See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cybersecurity, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

929 The term "cybersecurity" is used to summarize various activities ITU-T Recommendation X.1205 "Overview of Cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: *ITU*, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

930 With regard to developments related to developing countries, see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

931 See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008) on Cybersecurity available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; EU Communication towards a general policy on the fight against cyber crime, 2007 available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

932 For more information, see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

933 For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

934 See below: § 4.4.

935 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arab regions.

936 See for example: Austria: National ICT Security Strategy Austria, available at: www.ccdcoe.org/strategies/Austrian_Cyber_Security_Strategy.pdf; Estonia: Cyber Security Strategy, available at: www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf; Germany: Cybersecurity Strategy for Germany, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile; United Kingdom: UK Cyber Security Strategy, available at.: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf; New Zealand: www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf; For more examples see: National Cyber Security Framework Manual, NATO CCD, 2012, page 53 et seq.

937 See for example the EU Cybersecurity Strategy: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1. Regarding the activities of the UN in relation to Cybersecurity see: *Maurer*, Cyber Norm Emergence at the United Nations, An Analysis of the Activities at the UN regarding Cyber-Security, 2011.

938 See: National Cyber Security Framework Manual, NATO CCD, 2012, page 46.

939 Cybersecurity Strategy for Germany, 2011, page 7, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

940 With regard to the need of updates see below III.5.c..

941 This issue was for example taken into consideration within the EU/ITU co-funded projects HIPCAR and ICB4PAC. The model policy, as well as the model legislation, are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

942 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

943 Regarding the need for an interdisciplinary approach see: *Schjolberg/Ghernaouti-Helie*, A Global Treaty on Cybersecurity and Cybercrime, Second Edition, 2011, page 17, available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

944 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

945 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

946 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

947 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

948 See below: § 5.

949 The harmonization of training is one of the main objectives for the EU Cybercrime Centers of Excellence Network (2Centre). Information is available at: www.2centre.eu. Other examples are the European Cybercrime Training & Education Group (ECTEG) as well as the Europol Working Group on the Harmonization of Cybercrime Training (EWGHCT).

950 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

951 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

952 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

953 See for example: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, 2007, page 5, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf; *Pladna*, The Lack of Attention in the Prevention of Cyber Crime and How to improve it, University of East Carolina, ICTN6883, available at: www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf.

954 Regarding blocking of websites with illegal content see: *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008.

955 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

956 Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary, page 7, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf; see also ITU, World Summit on Information Society, The Report of the Task Force on Financial Mechanisms for ICT for Development, December, 2004, available at: www.itu.int/wsis/tffm/final-report.pdf; ITU/infoDEV ICT Regulation Toolkit, Chapter 4.1. What is the Role of Regulators?, available at: www.ictregulationtoolkit.org/en/Section.3109.html

957 See GSR09 – Best Practice Guidelines on innovative regulatory approaches in a converged world to strengthen the foundation of a global information society, available at www.itu.int; *Macmillian*. Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009 // available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf

[958] *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf; *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

[959] E.g. Korea Communications Commission, established in February 2008 (formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission), announced among other core regulatory duties protection of Internet users from harmful or illegal content. Korea Communications Commission: http://eng.kcc.go.kr.

[960] E.g. Swedish ICT Regulator PTS addresses cyberthreats and cybercrime under user protection mandate and network security mandate. See: *PTS*. Secure communications, available at www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

[961] *OPTA*. Regulatory areas, available at: www.opta.nl/en/about-opta/regulatory-areas/.

[962] The Dutch regulator is granted the mandate to monitor any contravention of the prohibition of unsolicited communication under its duties to provide Internet safety for consumers.

[963] OPTA has the power to take action against anyone contravening the prohibition of spam and unsolicited software by imposing fines.

[964] OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

[965] *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Henten/ Samarajiva/ Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; infoDev/ITU ICT regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

[966] See the discussions on regulation, illegal content and converged regulators: *Van Oranje et al,* Responding to Convergence: Different approaches for Telecommunication regulators TR-700-OPTA, 30 September 2008, available at: www.opta.nl/download/convergence/convergence-rand.pdf; *Millwood Hargrave, et al,* Issues facing broadcast content regulation, Broadcasting Standards Authority, New Zealand, 2006, available at: www.bsa.govt.nz/publications/IssuesBroadcastContent-2.pdf. See also: *ITU*, Case Study: Broadband, the Case of Malaysia, Document 6, April 2001, available at: www.itu.int/osg/spu/ni/broadband/workshop/malaysiafinal.pdf.

[967] See*: infoDev/ITU* ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html. See also: *Henten/ Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; *Singh/Raja*, Convergence in ICT services: Emerging regulatory responses to multiple play, June 2008, available at: http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/Convergence_in_ICT_services_Emerging_regulatory_responses_to_multiple_play.pdf; *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1.

[968] The four states which have regulators that can be regarded as converged regulatory authorities are: Finland, Italy, Slovenia and the United Kingdom. See: infoDev/ITU ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html.

[969] Information and network security (INS).

[970] See: *MCMC*, What do we Do. Information Network Security, available at: www.skmm.gov.my/what_we_do/ins/feb_06.asp.

[971] Korea Communications Commission: Important Issues, available at: http://eng.kcc.go.kr.

[972] Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary. 2009, P. 11, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

[973] See: *Haggard/McCubbins*, Presidents, Parliaments, and Policy. University of California, San Diego, July 1999, available at: http://mmccubbins.ucsd.edu/ppp.pdf. For the discussion with regard to regulatory agencies, see: *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making: a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf.

[974] The rationale for separating the ICT regulator from the policy-making body is to have an independent regulator that maintains a distance from the ministry or other government bodies which could remain as the major shareholder of the incumbent. An independent regulator can avoid conflict of interest that can happen if the regulator is also responsible

for industry promotion. See: *OECD*, Telecommunications Regulatory Structures and Responsibilities, DSTI/ICCP/TISP(2005)6/FINAL, January, 2006, available at: www.oecd.org/dataoecd/56/11/35954786.pdf.

975 InfoDev ITU ICT Regulation toolkit. Section 6.3. Separation of Power and Relationship of Regulator with Other Entities, available at: www.ictregulationtoolkit.org/en/Section.1269.html.

976 Public Consultation Processes. InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; *Labelle*, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

977 One example is the Botswana Telecommunications Authority, which is required to provide the input to government policy-making efforts. See: Case Study Single Sector Regulator: Botswana Telecommunications Authority (BTA). InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/PracticeNote.2031.html.

978 International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich, 2009, available at www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663, P. 133.

979 National Information Security Strategy Proposal, November, 2002 // available at: www.mintc.fi/fileserver/national_information_security_strategy_proposal.pdf.

980 *Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

981 See: *Uganda Communications Commission*, Recommendations on Proposed Review of the Telecommunications Sector Policy, 2005, available at: www.ucc.co.ug/UgTelecomsSectorPolicyReview_31_Jan_2005.pdf; *Blythe*, The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control in Repositioning African Business and Development for the 21st Century, Simon Sigué (Ed.), 2009, available at: www.iaabd.org/2009_iaabd_proceedings/track16b.pdf; Uganda Computer Misuse Bill 2004, available at: www.sipilawuganda.com/files/computer%20misuse%20bill.pdf.

982 See, for example: Report of the Second EAC Regional Taskforce Meeting on Cyber Laws. June 2008, Kampala, Uganda, available at: http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf.

983 Now: Zambia Information and Communications Technology Authority.

984 *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis, Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf; *Hatyoka*, ZICTA Corner – Defining ZICTA's new mandate. Times of Zambia, 2009 // available at: www.times.co.zm/news/viewnews.cgi?category=12&id=1262768483.

985 Zambia Electronic Communications and Transactions Act 2009, available at: www.caz.zm/index.php?option=com_docman&Itemid=75. See also ZICTA. Cybercrime Penalties (Part 1), available at: www.caz.zm/index.php?option=com_content&view=article&id=76:cyber-crime-penalties-part-1&catid=34:column&Itemid=38.

986 Annual report 2008 Belgian Institute for postal service and telecommunication, BIPT, 2009, available at: http://bipt.be/GetDocument.aspx?forObjectID=3091&lang=en.

987 See: *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003, available at: www.cert.org/archive/pdf/03hb001.pdf.

988 *Scarfone/Grance/Masone,* Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61, 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf, pp. 2-2.

989 www.ficora.fi/.

990 Sweden's IT Incident Centre (Sitic) is located in the ICT regulator PTS.See: PTS. Secure communications, available at: www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

991 aeCERT created as an initiative of the UAE Telecommunications Regulatory Authority to detect, prevent and respond to current and future cybersecurity incidents in the UAE*: Bazargan*, A National Cybersecurity Strategy aeCERT Roadmap. Presentation at Regional Workshop on Frameworks for Cybersecurity and CIIP 18 – 21 Feb 2008 Doha, Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

992 The national CERT (qCERT) was established by the Qatari ICT regulator (ictQatar) and acts on behalf of ictQatar; *Lewis*, Q-CERT. National Cybersecurity Strategy Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incid ent-management-brisbane-july-08.pdf.

993 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at:

http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf.

994 E.g. ICT regulators are involved in law-enforcement efforts with regard to combating spam in the following countries: Australia, Finland, Greece, Hungary, Japan, Malaysia, Mexico, Netherlands, Portugal, Turkey. See: *OECD* Task Force on Spam. Enforcement authorities contact list, available at: www.oecd-antispam.org/countrycontacts.php3.

995 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

996 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

997 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et. seq*.

998 For an overview of cybercrime-related legislation and its compliance with the standards defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

999 See below: § 6.2.

1000 See below: § 6.2.

1001 For an overview of the most relevant challenges in the fight against cybercrime, see above: § 3.1.

1002 One possibility to mask identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems, see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

1003 Regarding legal responses to the challenges of anonymous communication, see below: §§ 6.5.10 and 6.3.11.

1004 See above: § 3.2.6.

1005 See in this context below: § 6.6.

1006 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

1007 *Vaciago*, Digital Evidence, 2012.

1008 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

1009 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

1010 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

1011 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1012 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United

Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[1013] See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[1014] *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[1015] See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

[1016] For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[1017] *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

[1018] Transaction authentication number – for more information, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[1019] The ITAN system improves the TAN system. The financial institutions provide the customer with a number of TAN-indexed identity numbers. With regard to each relevant transaction, the online banking system requires a specific ITAN number selected at random from the list of supplied TAN. For more information, see: *Bishop*, Phishing & Pharming: An investigation into online identity theft, 2005, available at: http://richardbishop.net/Final_Handin.pdf.

[1020] Regarding various authentication approaches in Internet banking, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[1021] Regarding approaches to coordinate the cooperation of law-enforcement agencies and Internet service providers in the fight against cybercrime, see the results of the working group established by Council of Europe in 2007. For more information, see: www.coe.int/cybercrime/.

[1022] Capacity building is in general defined as the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation (of women in particular), human resources development and strengthening of managerial systems. In addition, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations, user groups, professional associations, academics and others).

[1023] At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect". Regarding user-education approaches in the fight against phishing, see: Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, Technical Trends in Phishing Attacks, available at: www.cert.org/archive/pdf/Phishing_trends.pdf. Regarding sceptical views on user education, see: *Görling*, The Myth Of User Education, 2006, available at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[1024] Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: www.cert.org/archive/pdf/Phishing_trends.pdf.

[1025] *Shaw*, Details of anti-phishing detection technology revealed in Microsoft Patent application, 2007, available at: http://blogs.zdnet.com/ip-telephony/?p=2199; Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers – Cyota Inc., Internet Identity and MarkMonitor to provide phishing Web site data for Microsoft Phishing Filter and SmartScreen Technology services, 2005, available at: www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

[1026] For a different opinion, see: *Görling*, The Myth Of User Education, 2006, at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[1027] At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[1028] "The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack, explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, available at: www.heise-security.co.uk/news/80152.

[1029] Examples of the publication of cybercrime-related data include: Symantec Government Internet Security Threat Report Trends for July–December 06, 2007, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf; Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[1030] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1031] The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1032] See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network-storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

[1033] Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1034] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[1035] Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/

[1036] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

[1037] The assessment reports are available on the HIPCAR website and will be on the HIPSSA and ICB4PAC website shortly.

[1038] With regard to the relevance of legislation related to the specific topic cybercrime see: *Gercke*, CRi 2012, 81.

[1039] See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

[1040] Council of Europe Convention on Cybercrime (CETS No. 185); *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225,; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, CRi 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, page 7 *et seq.*; *Gercke*, 10 years Convention on Cybercrime, Cri 2011, 142 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[1041] Art. 2: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

[1042] Art. 2 (1) :Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

[1043] Art. III-2: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system.

[1044] Regarding the relevance of audio files see: *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1045] Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Netherlands, Portugal, Sweden and "The Former Yugoslav Republic of Macedonia".

[1046] The decision to establish the working group was made during the 583rd Meeting of the Minister's, Decision No. CM/Del/Dec(97)583.

5. Présentation générale des activités des organisations régionales et internationales

Bibliography (selected): *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009; Committee II Report, 11th UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007; *Nilsson* in *Sieber*, Information Technology Crime, page 576; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001; Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, 2001; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07.

Le présent chapitre se propose de fournir une vue d'ensemble des approches législatives internationales[1047] et d'étudier comment elles se situent par rapport aux approches nationales.

5.1 Approches internationales

Plusieurs organisations internationales qui analysent en continu l'évolution de la cybercriminalité ont mis en place des groupes de travail chargés d'élaborer des stratégies de lutte contre les cyberdélits.

5.1.1 G7 (anciennement G8)[1048]

En 1997, le Groupe des huit (G8) a créé un « sous-groupe sur la criminalité liée à la haute technologie » (*Subcommittee*[1049] *on High-tech Crimes*), chargé des questions de lutte contre la cybercriminalité[1050]. À leur réunion de Washington D.C., États-Unis, les ministres de la Justice de l'Intérieur du G8 ont adopté dix principes et un plan d'action en dix points pour lutter contre la criminalité liée à la haute technologie[1051]. Les chefs du G8 ont ensuite avalisé ces principes, qui stipulent notamment que:

- Il ne doit pas exister de refuges pour ceux qui exploitent les technologies de l'information à des fins criminelles.
- Les enquêtes sur les délits de niveau international liés à la haute technologie et la poursuite en justice leurs auteurs doivent être coordonnées par tous les États concernés, indépendamment du lieu du préjudice.
- Le personnel des services de répression doit être formé et équipé pour faire face aux cyberdélits.

En 1999, lors d'une conférence ministérielle sur la lutte contre le crime transnational organisé, tenue à Moscou, Fédération de Russie, les chefs du G8 ont précisé leurs plans concernant la lutte contre les cyberdélits[1052]. Ils ont exprimé leur inquiétude au sujet des crimes (notamment la pédopornographie) et de la traçabilité des transactions et des accès transfrontaliers aux données. Leur communiqué contient des principes concernant la lutte contre la cybercriminalité, qui sont aujourd'hui repris dans plusieurs stratégies internationales.[1053]

Sur le plan pratique, les travaux des groupes d'experts ont notamment donné lieu à la mise en place d'un réseau international de contacts 24/7. Les pays participant à ce réseau s'engagent à mettre à disposition pour les enquêtes transnationales des points de contact accessibles 24 heures sur 24 et 7 jours sur 7[1054].

En 2000, lors de sa conférence tenue à Paris, France, le G8 s'est penché sur le problème de la cybercriminalité et a appelé de ses vœux la prévention des zones numériques de non-droit. À l'époque déjà, dans sa recherche de solutions internationales, le G8 évoquait la Convention du Conseil de l'Europe sur la cybercriminalité[1055]. En 2001, lors d'un atelier organisé à Tokyo[1056], le G8 a examiné des instruments de procédure visant à lutter contre la cybercriminalité, la question étant de savoir s'il fallait imposer des obligations de conservation des données ou si l'archivage des données était une autre solution envisageable[1057].

En 2004, les ministres de la Justice et de l'Intérieur du G8 ont publié un communiqué faisant part de la nécessité de développer des moyens, à l'échelle mondiale, pour lutter contre l'exploitation d'Internet à des fins criminelles [1058]. Le G8 prenait encore note de la Convention du Conseil de l'Europe sur la cybercriminalité[1059].

À la réunion de Moscou de 2006, les ministres de la Justice et de l'Intérieur du G8 ont examiné plusieurs points se rapportant à la lutte contre la cybercriminalité et au cyberespace, notamment la nécessité d'améliorer les contre-mesures [1060]. La question du cyberterrorisme [1061] a également été abordée au sommet du G8 de Moscou, qui a suivi cette réunion[1062].

En 2007, lors de la réunion des ministres de la Justice de l'Intérieur du G8 à Munich, Allemagne, la question de l'exploitation d'Internet à des fins terroristes a été examinée plus avant. Les participants sont convenus d'ériger en infraction pénale l'exploitation d'Internet par des groupes terroristes[1063]. Cet accord ne contient pas d'actes précis devant être pénalement sanctionnés.

En 2009, lors de la réunion des ministres de la Justice de l'Intérieur du G8 à Rome, Italie, plusieurs sujets ayant trait à la cybercriminalité ont été débattus. Dans leur déclaration finale, en vue du G8, les ministres ont recommandé le blocage des sites Internet diffusant de la pédopornographie sur la base de listes noires actualisées et diffusées par des organisations internationales [1064]. S'agissant de la cybercriminalité en général, cette déclaration finale souligne la menace croissante et interpelle sur la nécessité d'une coopération renforcée entre les fournisseurs de service et les services de répression et d'un renforcement des formes de coopération existantes, telles que les Points de contact 24/7 du G8 pour la cybercriminalité[1065].

Lors du sommet du G8 de Muskoka, Canada, la cybercriminalité n'a été abordée que brièvement. La déclaration de Musoka stipule seulement, dans le contexte des activités terroristes, que le G8 est préoccupé à propos de la menace croissance de la cybercriminalité et travaillera intensivement à affaiblir les réseaux terroristes et criminels.[1066]

Les questions de la cybercriminalité et de la cybersécurité ont été toutes deux abordées dans le cadre du forum e-G8, où des délégations ont débattu de sujets ayant trait à Internet avec des dirigeants d'entreprises, [1067] ainsi qu'au sommet du G8 de Deauville, France. Mais, bien que le sujet de la

cybercriminalité ait retenu toute l'attention, la déclaration finale du sommet ne contenait, contrairement aux années précédentes, aucune recommandation spécifique. Le G8 ne s'est prononcé que sur des principes généraux, comme l'importance de la sécurité et de la protection contre le crime qui sous-tendent un Internet puissant et florissant.[1068]

5.1.2 Nations Unies et Office des Nations Unies contre la drogue et le crime [1069]

Les Nations Unies ont adopté plusieurs approches importantes pour relever le défi de la cybercriminalité. Alors que sa réponse était, au début, limitée à des lignes directrices générales, l'organisation a récemment travaillé plus intensément sur cette question et sur la réponse juridique à y apporter.

Convention des Nations Unies relative aux droits de l'enfant

La Convention des Nations Unies relative aux droits de l'enfant, adoptée en 1989,[1070] propose plusieurs instruments juridiques visant à protéger l'enfant. Elle ne définit pas la pédopornographie, et ne contient aucune disposition visant à harmoniser la criminalisation de la diffusion de contenu pornographique à caractère pédophile en ligne. Cependant, son article 34 appelle les États membres à empêcher l'exploitation abusive de l'enfant dans les productions pornographiques.

Résolution 45/121 de l'Assemblée générale de l'ONU

Après le huitième congrès des Nations Unies sur la prévention du crime et le traitement de la délinquance (qui s'est tenu à La Havane, Cuba, du 27 août au 7 septembre 1990), l'Assemblée générale a adopté une résolution traitant de la législation en matière de cybercriminalité.[1071] Sur la base de sa résolution 45/121 (1990), l'ONU a publié, en 1994, un manuel sur la prévention et le contrôle des cyberdélits.[1072]

Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants

Le Protocole optionnel traite non seulement de la question de la pédopornographie en général, mais aborde également explicitement le rôle d'Internet dans la distribution de ces supports.[1073] La pédopornographie se définit comme toute représentation, par quelque moyen que ce soit, d'un enfant engagé dans des activités sexuelles réelles ou simulées explicites ou toute représentation des organes sexuels d'un enfant à des fins essentiellement sexuelles. [1074] L'article 3 invite les parties à la Convention à criminaliser certains comportements — notamment les actes assimilables à la pédopornographie.

> ***Article 3***
> *1. Chaque État Partie à la Convention veille à ce que, au minimum, les actes et activités suivants soient pleinement couverts par son droit pénal, que ces infractions soient commises au plan interne ou transnational, par un individu ou de façon organisée:*
> *[...]*
> *c) Le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de vendre ou de détenir aux fins susmentionnées, des matériels pornographiques mettant en scène des enfants, tels que définis à l'article 2.*
> *[...]*

Dixième congrès des Nations Unies sur la prévention de la criminalité et le traitement des délinquants

Pendant le dixième congrès des Nations Unies sur la prévention de la criminalité et le traitement des délinquants, qui s'est tenu à Vienne en 2000, l'impact de la cybercriminalité a été débattu dans un atelier spécifique. [1075] Le débat était centré en particulier sur les catégories de crimes et les enquêtes transnationales, ainsi que sur la réponse juridique au phénomène. [1076] Les conclusions de cet atelier contiennent des éléments essentiels du débat qui est toujours en cours: la criminalisation est nécessaire, la législation doit inclure des instruments procéduraux, la coopération internationale est cruciale et les partenariats public-privé doivent être renforcés. [1077] Par ailleurs, l'importance du renforcement des capacités a été soulignée — une question qui a été reprise les années suivantes.[1078] La déclaration de Vienne

a appelé la Commission de la prévention du crime et de la justice pénale à entreprendre des travaux à cet égard:

> *18. Nous décidons d'élaborer des recommandations concrètes sur la prévention et la répression des délits liés à l'informatique, et invitons la Commission pour la prévention du crime et la justice pénale à entreprendre des travaux sur la question compte tenu des travaux en cours dans d'autres instances. Nous nous engageons à œuvrer au renforcement des moyens dont nous disposons pour prévenir les délits liés à la technologie et à l'informatique, à enquêter sur ces délits et à en poursuivre les auteurs.*

Résolution 55/63 de l'Assemblée générale de l'ONU

La même année, l'Assemblée générale de l'ONU adoptait une résolution pour lutter contre l'utilisation à des fins criminelles des technologies de l'information, qui présente un certain nombre de similitudes avec le Plan d'action en dix points du G8 de 1997.[1079] Dans sa résolution, l'Assemblée générale identifiait plusieurs mesures pour prévenir l'utilisation abusive des technologies de l'information, notamment:

> *Les Etats devraient faire en sorte que leurs lois et leur pratique ne permettent pas que ceux qui exploitent les technologies de l'information à des fins criminelles puissent compter sur l'impunité;*
> *Tous les Etats concernés devraient coordonner l'action de leurs services de répression en ce qui concerne les enquêtes et poursuites relatives aux affaires d'exploitation des technologies de l'information à des fins criminelles au niveau international;*
> *Le personnel chargé de la répression devrait être formé et équipé pour faire face à l'exploitation des technologies de l'information à des fins criminelles;*

La résolution 55/63 invite les États à prendre les mesures nécessaires pour combattre la cybercriminalité au plan régional et international. Cela inclut l'élaboration d'une législation nationale pour éliminer les refuges dont jouissent les délinquants lorsqu'ils utilisent des technologies à des fins criminelles, renforcer les moyens d'application de la loi pour coopérer dans les enquêtes transfrontalières et poursuivre les auteurs de délits internationaux impliquant une utilisation de technologies de l'information, améliorer l'échange d'informations, renforcer la sécurité des données et des systèmes informatiques, former les agents de répression pour les préparer aux particularités de la cybercriminalité, concevoir des régimes d'assistance mutuelle et sensibiliser le public aux menaces de la cybercriminalité.

Résolution 56/121 de l'Assemblée générale de l'ONU

En 2002, l'Assemblée générale de l'ONU a adopté une autre résolution relative à la lutte contre l'exploitation des technologies de l'information à des fins criminelles.[1080] La résolution se réfère aux approches internationales existantes de la lutte contre la cybercriminalité et souligne différentes solutions.

> *Notant les travaux des organisations internationales et régionales consacrés à la lutte contre la criminalité faisant appel aux technologies de pointe, notamment ceux du Conseil de l'Europe pour élaborer la Convention sur la cybercriminalité ainsi que les travaux de ces organisations destinés à promouvoir un dialogue entre les pouvoirs publics et le secteur privé sur la sécurité et la confiance dans le cyberespace,*
> *1. Invite les Etats Membres, lorsqu'ils élaboreront leurs lois, politiques et pratiques nationales contre l'exploitation des technologies de l'information à des fins criminelles, à tenir compte, comme il convient, des travaux et des réalisations de la Commission pour la prévention du crime et la justice pénale et d'autres organisations internationales et régionales;*
> *2. Prend note de la valeur des mesures énoncées dans sa résolution 55/63 et invite à nouveau les Etats Membres à en tenir compte dans leurs efforts pour lutter contre l'exploitation des technologies de l'information à des fins criminelles;*
> *3. Décide d'ajourner l'examen du sujet en attendant l'achèvement des travaux envisagés dans le plan d'action contre la criminalité faisant appel aux technologies de pointe et à l'informatique que mène la Commission pour la prévention du crime et la justice pénale.*

La résolution 56/121 insiste sur la nécessité d'établir une coopération inter-états dans la lutte contre l'exploitation des technologies de l'information à des fins criminelles. Elle insiste sur le rôle qui peut être joué par les Nations Unies et d'autres organisations internationales et régionales. Cette résolution exhorte par ailleurs les états à prendre en compte les objectifs définis par la Commission de la prévention du crime et de la justice pénale pour l'élaboration des législations nationales.

Résolutions 57/239 et 58/199 de l'Assemblée générale de l'ONU

Les résolutions 57/239 et 58/199 sont les deux principales résolutions de l'Assemblée générale de l'ONU sur la cybersécurité. Sans approfondir la question de la cybercriminalité, elles rappellent les termes des résolutions 55/06 et 56/121. Les deux résolutions insistent par ailleurs sur la nécessité d'établir une coopération internationale en matière de lutte contre la cybercriminalité, en prenant acte que les écarts existant entre les états dans l'accès aux technologies de l'information et leur utilisation peuvent affecter l'efficacité de la coopération internationale dans la lutte contre l'exploitation des technologies de l'information à des fins criminelles.[1081]

11e Congrès des Nations Unies sur la prévention du crime et la justice pénale

La cybercriminalité était à l'ordre du jour du onzième Congrès des Nations Unies sur la prévention du crime et la justice pénale. Tant dans le document de fond qu'au cours des[1082] ateliers, plusieurs défis ayant trait à l'utilisation de l'informatique pour commettre des infractions et la dimension transnationale ont été traités.[1083] Dans le cadre des réunions préparatoires du congrès, certains pays comme l'Égypte ont réclamé une nouvelle convention des Nations Unies contre la cybercriminalité, et la réunion préparatoire des pays d'Asie occidentale a appelé à l'ouverture de négociations pour cette convention.[1084] La possibilité de négocier une telle convention était inscrite dans le guide de discussion préparé pour le onzième Congrès des Nations Unies sur la prévention du crime et la justice pénale.[1085] Cependant, les États membres n'ont pu à cette occasion se mettre d'accord pour lancer une harmonisation de la législation. Toutefois, la déclaration de Bangkok — sans mentionner d'instrument spécifique — fait référence aux approches existantes.

> *Nous notons qu'en cette période de mondialisation, les technologies de l'information et le développement rapide de systèmes de télécommunication et de réseaux informatiques nouveaux s'accompagnent d'un détournement de ces technologies à des fins criminelles. Nous nous félicitons donc des efforts déployés pour renforcer et compléter la coopération visant à prévenir la criminalité liée aux technologies de pointe et à l'informatique et à la combattre en menant des enquêtes et en engageant des poursuites, notamment en développant des partenariats avec le secteur privé. Nous reconnaissons l'importante contribution de l'Organisation des Nations Unies à des instances régionales et d'autres instances internationales dans la lutte contre la cybercriminalité, et invitons la Commission pour la prévention du crime et la justice pénale, compte tenu de cette expérience, à examiner la possibilité de fournir une assistance complémentaire dans ce domaine sous l'égide de l'Organisation des Nations Unies en partenariat avec d'autres organisations ayant des centres d'intérêt analogues.*

Résolution 60/177 de l'Assemblée générale de l'ONU

À l'issue du onzième Congrès des Nations Unies sur la prévention du crime et la justice pénale de Bangkok, Thaïlande, en 2005, une déclaration soulignant la nécessité d'une harmonisation dans la lutte contre la cybercriminalité a été adoptée.[1086] Elle traitait, entre autres, des questions suivantes:

> *Nous réaffirmons qu'il est essentiel d'appliquer les instruments en vigueur et d'étoffer encore les mesures nationales et la coopération internationale dans le domaine pénal, par exemple en envisageant des mesures renforcées et plus étendues, en particulier en matière de lutte contre la cybercriminalité, le blanchiment d'argent et le trafic de biens culturels et dans le domaine de l'extradition, de l'entraide judiciaire, ainsi que de la confiscation, du recouvrement et de la restitution du produit du crime.*

Nous notons qu'en cette période de mondialisation, les technologies de l'information et le développement rapide de systèmes de télécommunication et de réseaux informatiques nouveaux s'accompagnent d'un détournement de ces technologies à des fins criminelles. Nous nous félicitons donc des efforts déployés pour renforcer et compléter la coopération visant à prévenir la criminalité liée aux technologies de pointe et à l'informatique et à la combattre en menant des enquêtes et en engageant des poursuites, notamment en développant des partenariats avec le secteur privé. Nous reconnaissons l'importante contribution de l'Organisation des Nations Unies à des instances régionales et d'autres instances internationales dans la lutte contre la cybercriminalité, et invitons la Commission pour la prévention du crime et la justice pénale, compte tenu de cette expérience, à examiner la possibilité de fournir une assistance complémentaire dans ce domaine sous l'égide de l'Organisation des Nations Unies en partenariat avec d'autres organisations ayant des centres d'intérêt analogues.

La résolution 60/177 de l'Assemblée générale de l'ONU a approuvé la déclaration de Bangkok de 2005, encourageant les efforts de la communauté internationale pour renforcer et compléter la coopération existante pour lutter contre la criminalité utilisant l'informatique, et appelant à apporter une assistance aux États membres dans la lutte contre la criminalité utilisant l'informatique sous l'égide des Nations Unies, et en partenariat avec d'autres organisations poursuivant les mêmes buts.

Douzième Congrès des Nations Unies sur la prévention du crime et la justice pénale

La cybercriminalité était également à l'ordre du jour du douzième Congrès des Nations Unies sur la prévention du crime et la justice pénale qui s'est tenu au Brésil, en 2010.[1087] Au cours des quatre réunions préparatoires régionales pour le congrès, pour l'Amérique latine et les Caraïbes,[1088] l'Asie occidentale,[1089] l'Asie Pacifique[1090] et l'Afrique,[1091] les pays ont appelé à l'élaboration d'une convention internationale sur la cybercriminalité. Des appels semblables ont été lancés dans les milieux universitaires.[1092]

Lors du congrès, les États membres ont franchi une étape majeure vers une implication plus active des Nations Unies dans le débat sur la question de la criminalité utilisant l'informatique et de la cybercriminalité. Le fait que les délégations aient débattu de ces sujets pendant deux jours et que des évènements parallèles aient été organisés souligne l'importance de cette question, débattue plus en détail qu'aux congrès précédents sur la criminalité.[1093] Les délibérations étaient centrées sur deux questions primordiales: comment harmoniser les normes juridiques, et comment aider les pays en développement à lutter contre la cybercriminalité ? Le premier point est particulièrement pertinent si les Nations Unies élaborent des normes juridiques exhaustives ou suggèrent que les États membres mettent en œuvre la Convention du Conseil de l'Europe sur la cybercriminalité. Lors de la préparation du Congrès des Nations Unies sur la prévention du crime et la justice pénale, le Conseil de l'Europe a exprimé des réserves quant à l'approche adoptée par les Nations Unies,[1094] et a lancé un appel à soutenir sa Convention sur la cybercriminalité. Après un débat intense, pendant lequel a été débattue en particulier la question de la portée limitée de la Convention sur la cybercriminalité, les États membres ont décidé de ne pas appeler à la ratification de la Convention, mais plutôt à renforcer le rôle des Nations Unies dans deux domaines importants, qui sont mentionnés dans la déclaration de Salvador:

41. Nous recommandons que l'Office des Nations Unies contre la drogue et le crime fournisse aux États qui en font la demande, en coopération avec les États membres, les organisations internationales compétentes et le secteur privé, une assistance technique et une formation afin d'améliorer la législation nationale et de renforcer la capacité des autorités nationales, pour lutter contre la cybercriminalité, sous toutes les formes, y compris la prévenir, en détecter les manifestations, enquêter sur celles-ci et en poursuivre les auteurs, et renforcer la sécurité des réseaux informatiques.
42. Nous invitons la Commission pour la prévention du crime et la justice pénale à convoquer un groupe intergouvernemental d'experts à composition non limitée en vue de réaliser une étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États membres, la communauté internationale et le secteur privé, y compris en matière d'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin d'examiner les options envisageables pour renforcer les mesures juridiques ou autres prises à l'échelle nationale et internationale face à la cybercriminalité et pour en proposer de nouvelles.

Les États membres recommandaient ainsi de confier un mandat fort à l'Office des Nations Unies contre la drogue et le crime (UNODC) pour fournir, sur demande, un renforcement des capacités. Considérant l'expérience de l'UNODC en matière de renforcement de capacité dans le domaine de la législation criminelle et le fait que, contrairement au Conseil de l'Europe, l'UNODC dispose d'un réseau mondial de bureaux régionaux, il y a fort à penser que les Nations Unies, au travers de l'UNODC, jouent un rôle primordial dans ce domaine à l'avenir.

La seconde recommandation souligne que, à l'heure du congrès des Nations Unies sur la criminalité, les États membres ne sont pas parvenus à statuer sur l'élaboration d'un texte juridique ou non. Cela reflète la controverse qu'a suscitée la discussion pendant le congrès, où les pays européens qui ont déjà ratifié la Convention sur la cybercriminalité, en particulier, ont exprimé leur soutien envers cet instrument, alors qu'un certain nombre de pays en développement ont appelé à l'élaboration d'une convention des Nations Unies en la matière. Toutefois, les États membres ont eu une réponse différente de celle du onzième Congrès sur la criminalité, où ils s'en remettaient aux instruments existants. Cette fois-ci, ils ne s'en remettaient pas à un instrument existant, et, plus important encore, ils ne décidèrent point de recommander d'adopter la Convention sur la cybercriminalité en tant que norme mondiale. Au contraire, les États membres recommandèrent d'inviter la Commission pour la prévention du crime et la justice pénale à mener une étude exhaustive visant, inter alia, à examiner les options possibles pour renforcer les dispositions juridiques nationales et internationales et autres réponses à la cybercriminalité et en proposer de nouvelles.

Résolution 64/211 de l'Assemblée générale de l'ONU

En mars 2010, l'Assemblée générale de l'ONU a voté une nouvelle résolution[1095] dans le cadre de l'initiative « Création d'une culture mondiale de la cybersécurité ». La résolution 64/211 se réfère à deux résolutions majeures sur la cybercriminalité[1096] ainsi qu'à deux résolutions majeures sur la cybersécurité.[1097] L'outil d'autoévaluation volontaire pour les initiatives nationales visant à protéger les infrastructures d'information critiques, fourni en annexe à la résolution, invite les pays à un audit et une rénovation de leurs instances juridiques (y compris celles ayant trait à la cybercriminalité, la confidentialité, la protection des données, le droit commercial, les signatures numériques et le chiffrement) susceptibles d'être désuètes ou obsolètes à la suite de l'adoption rapide des nouvelles technologies d'information et de communication, ou à cause de leur dépendance envers ces technologies. La résolution exhorte également les états à utiliser les conventions, arrangements et précédents internationaux lors de ces audits.

13. Examiner les textes juridiques (notamment ceux qui se rapportent à la cybercriminalité, la confidentialité, la protection des données, le droit commercial, les signatures numériques et le codage) et actualiser ceux qui seraient devenus obsolètes du fait de l'adoption rapide de nouvelles technologies de l'information et
des communications et de la dépendance du pays vis-à-vis de ces technologies, en se fondant sur les conventions, mécanismes et précédents régionaux et internationaux. Déterminer si le pays a légiféré en matière d'enquêtes et de poursuites pour cybercriminalité en ayant à l'esprit les dispositifs existants, tels que les résolutions
55/63 et 56/121 de l'Assemblée générale relatives à la lutte contre l'exploitation des technologies de l'information à des fins criminelles, ainsi que des initiatives régionales telles que la Convention du Conseil de l'Europe sur la cybercriminalité.
14. Déterminer quelle est la situation en ce qui concerne les procédures et mécanismes nationaux de lutte contre la cybercriminalité, y compris les textes juridiques, et les structures nationales, et dans quelle mesure les procureurs, les juges et les législateurs sont sensibilisés aux problèmes de cybercriminalité.
15. Déterminer dans quelle mesure les codes et textes juridiques existants sont adéquats compte tenu des difficultés qui sont et seront à l'avenir associées à la cybercriminalité et, d'une manière plus générale, au cyberespace.
16. Évaluer la participation du pays aux initiatives internationales de lutte contre la cybercriminalité, par exemple au Réseau de contacts contre la cybercriminalité qui fonctionne 24 heures sur 24 et sept jours sur sept.

17. Déterminer ce dont ont besoin les services nationaux de répression pour coopérer avec leurs homologues d'autres pays à des enquêtes sur des affaires de cybercriminalité transnationale dans lesquelles l'infrastructure est située sur le territoire national ou les auteurs des infractions résident sur ce territoire, mais les victimes résident ailleurs.

Le fait que quatre sujets, sur 18, de l'outil d'autoévaluation aient trait à la cybercriminalité souligne l'importance que revêt la capacité des services de répression à lutter contre la cybercriminalité efficacement pour maintenir la cybersécurité.

Etude mondiale sur la cybercriminalité

Suite à un examen approfondi[1098] des thèmes et de la méthodologie[1099] exposés dans une étude exhaustive sur la cybercriminalité réalisée par l'ONUDC, un questionnaire a été envoyé début 2012 aux Etats Membres de l'ONU, tandis qu'un portail en ligne a été développé dans le même temps.[1100] Ce questionnaire complexe contient plusieurs questions portant sur différents domaines de la législation en matière de cybercriminalité, tels que les définitions, l'incrimination et les instruments de procédure. Il a été demandé aux Etats Membres de fournir des informations sur le statut de leur législation, ainsi que sur l'état d'avancement de la mise en œuvre de différentes normes régionales (comme la Convention sur la cybercriminalité). En 2013, les résultats ont été présentés[1101] à la Commission pour la prévention du crime et la justice pénale[1102].

En 2013, l'ONUDC a publié les premiers résultats de l'étude[1103], qui est la plus complexe réalisée à ce jour. Elle prend en compte les résultats donnés par 69 Etats Membres[1104] ayant répondu au questionnaire, mais aussi les résultats de l'examen de 500 documents accessibles au public et d'informations soumises par plus de 40 entreprises et 16 établissements universitaires. Cette étude souligne le caractère limité de la portée des instruments d'harmonisation régionale tels que la Convention du Conseil de l'Europe sur la cybercriminalité. Elle montre par ailleurs que d'autres instruments régionaux sont tout aussi importants.[1105] Le Groupe d'experts s'est réuni en février 2013 et a soumis la question à la Commission pour la prévention du crime et la justice pénale. [1106]

En avril 2013, ladite Commission a examiné les résultats de l'étude pour la première fois.[1107] La Résolution 22/7 examine les travaux réalisés, sans toutefois aller dans le détail.[1108] Au lieu de cela, la Commission invite les Etats Membres à examiner les résultats, demande au Groupe d'experts de poursuivre ses travaux et prie le Secrétariat de traduire l'étude dans les six langues de l'ONU. Au cours de la 23e réunion, plusieurs intervenants ont abordé le thème de la cybercriminalité.[1109] Bien que plusieurs d'entre eux en aient appelé à une harmonisation au niveau mondial, la Commission n'a pris aucune décision à cet égard. Elle se concentre davantage sur le renforcement des capacités en mettant en avant le Programme mondial de renforcement des capacités dirigé par l'ONUDC.[1110]

Groupe d'experts gouvernementaux

En 2013, un Groupe d'experts gouvernementaux composés d'experts de pays européens (Estonie, France, Allemagne et Royaume-Uni) et dont les travaux étaient axés sur la cybersécurité/sécurité de l'information, a présenté un rapport sur "les progrès de la téléinformatique dans le contexte de la sécurité internationale".[1111] Par ailleurs, bien que la question des normes ait été examinée, le Groupe a mis l'accent sur un aspect spécifique de la cybersécurité, à savoir la participation de l'Etat.[1112]

Groupe d'experts intergouvernemental sur la cybercriminalité

À la suite de la décision des États membres de confier à l'UNDOC la constitution d'un groupe de travail intergouvernemental, la première réunion du groupe s'est déroulée à Vienne au mois de janvier 2011.[1113] Le groupe d'experts était composé de représentants des États membres, du secteur privé et du monde universitaire. Pendant la réunion, les membres du groupe d'experts ont travaillé sur un projet de structure pour une analyse exhaustive de la question de la cybercriminalité ainsi que de la réponse à y apporter.[1114] Eu égard à la réponse juridique, plusieurs membres ont souligné l'utilité des instruments juridiques existants, y compris la Convention des Nations Unies contre la criminalité transnationale organisée (UNTOC)

et la Convention sur la cybercriminalité du Conseil de l'Europe, et la pertinence d'élaborer un instrument juridique mondial pour traiter spécialement du problème de la cybercriminalité. Il a été convenu que la décision quant à la pertinence de l'élaboration d'un instrument mondial serait prise après que l'analyse ait été achevée.

Autres résolutions et activités

En outre, un certain nombre de décisions, de résolutions et de recommandations de système des Nations Unis ont trait à des questions liées à la cybercriminalité, dont les plus importantes sont les suivantes: l'Office des Nations Unies contre la drogue et le crime (UNODC) et la Commission pour la prévention du crime et la justice pénale[1115] ont adopté une résolution relative à la prévention efficace de la criminalité et visant à apporter des réponses en matière de justice pénale pour combattre l'exploitation sexuelle des enfants.[1116] En 2004, le Conseil économique et social des Nations Unies[1117] a adopté une résolution sur la coopération internationale en matière de prévention, d'enquête, de poursuite des délinquants et de condamnation des fraudes, pour l'utilisation illégale et la falsification d'identité et autres délits apparentés.[1118] Un groupe de travail a été créé en 2005.[1119] Un panel d'experts en criminalité liée à l'identité a été créé pour mener une étude exhaustive sur cette question. En 2007, l'ECOSOC a adopté une résolution portant sur la coopération internationale en matière de prévention, d'enquête, de poursuite et de condamnation pour les fraudes économiques et les délits liés à l'identité.[1120] Aucune de ces résolutions ne traite explicitement des défis de la criminalité liée à Internet,[1121] mais elles s'appliquent néanmoins à ces délits également. Sur la base des résolutions 2004/26[1122] et 2007/20 de l'ECOSOC,[1123] l'UNODC a réuni en 2007 un panel d'experts qui ont confronté leurs opinions sur la meilleure ligne d'action à adopter.[1124] Le panel a mené plusieurs études qui abordaient différents aspects de la criminalité liée à Internet.[1125] En 2004, l'ECOSOC a voté une résolution sur la vente de drogues licites sur Internet qui prenait en compte explicitement un phénomène apparenté à un délit informatique.[1126]

Protocole d'entente UNODC/UIT

En 2011, l'UNODC et L'Union internationale des télécommunications (UIT) ont signé un protocole d'entente sur la cybercriminalité.[1127] Ce protocole couvre la coopération (en particulier le renforcement de capacités et l'assistance technique pour les pays en développement), la formation et les ateliers pratiques conjoints. Eu égard aux activités de renforcement de capacités, les deux organisations peuvent s'appuyer sur un large réseau de bureaux implantés sur le terrain dans tous les continents. Par ailleurs, les organisations se sont entendues pour diffuser l'information et les connaissances et analyser les données conjointement.

5.1.3 Union internationale des télécommunications [1128]

L'Union internationale des télécommunications (UIT), en tant qu'institution spécialisée des Nations Unies, joue un rôle essentiel dans la normalisation et le développement des télécommunications et dans les questions de cybersécurité.

Sommet mondial sur la société de l'information

Entre autres activités, l'UIT a été le chef de file du Sommet mondial sur la société de l'information (SMSI), qui s'est tenu en deux parties à Genève, Suisse (2003) et à Tunis, Tunisie (2005). Des gouvernements, des décideurs et des experts du monde entier ont mis en commun leurs idées et leurs expériences sur la meilleure façon de faire face aux nouveaux problèmes liés à l'évolution de la société mondiale de l'information, y compris à l'élaboration de normes et de lois compatibles. Les conclusions de ce sommet figurent dans la *Déclaration de principes de Genève*, dans le *Plan d'action de Genève*, dans l'*Engagement de Tunis* et dans l'*Agenda de Tunis pour la société de l'information*.

Le Plan d'action de Genève souligne l'importance des mesures de lutte contre la cybercriminalité:[1129]

> ***C5. Établir la confiance et la sécurité dans l'utilisation des TIC***
> *12. La confiance et la sécurité sont au nombre des principaux piliers de la société de l'information*

[…]

b) En coopération avec le secteur privé, les pouvoirs publics devraient prévenir et détecter la cybercriminalité et l'utilisation abusive des TIC et y remédier: en élaborant des lignes directrices qui tiennent compte des efforts en cours dans ces domaines; en envisageant une législation qui autorise des investigations efficaces et des poursuites en cas d'utilisation illicite; en encourageant les efforts d'assistance mutuelle; en renforçant l'appui institutionnel sur le plan international afin de prévenir et de détecter de tels incidents et d'y remédier; et en encourageant l'éducation et la sensibilisation.

[…]

La seconde partie du SMSI, organisé à Tunis en 2005, a également été l'occasion d'examiner le problème de la cybercriminalité. L'Agenda de Tunis pour la société de l'information [1130] souligne la nécessité d'une coopération internationale dans la lutte contre la cybercriminalité et mentionne les approches législatives existantes, notamment les résolutions prises par l'Assemblée générale des Nations Unies et la Convention du Conseil de l'Europe sur la cybercriminalité:

40. Nous soulignons combien il est important de poursuivre les auteurs de cyberdélits, y compris ceux commis dans un pays, mais dont les conséquences sont ressenties dans un autre pays. Nous insistons en outre sur la nécessité de disposer d'instruments et de mécanismes efficaces, au plan national et international, pour promouvoir la coopération internationale notamment entre les services de police et de justice dans le domaine de la cybercriminalité. Nous exhortons les États à élaborer, en collaboration avec les autres parties prenantes, la législation nécessaire permettant d'enquêter sur la cybercriminalité et de poursuivre en justice les auteurs de cyberdélits, en tenant compte des cadres existants, par exemple les Résolutions 55/63 et 56/121 de l'Assemblée générale des Nations Unies sur la lutte contre l'exploitation des technologies de l'information et de la communication à des fins criminelles, et les initiatives régionales, parmi lesquelles la Convention du Conseil de l'Europe sur la cybercriminalité.

Programme mondial cybersécurité

À l'issue du SMSI, l'UIT a été désignée comme seul coordonnatrice de la grande orientation C5 intitulée « Établir la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication »[1131]. À la deuxième réunion de coordination relevant de la grande orientation C5 du SMSI en 2007, le Secrétaire général de l'UIT a souligné l'importance de la coopération internationale dans la lutte contre la cybercriminalité et a annoncé le lancement du *Programme mondial cybersécurité de l'UIT*.[1132] Le Programme mondial cybersécurité (GCA) comporte sept buts stratégiques[1133], et repose sur cinq grands axes stratégiques[1134], portant notamment sur le développement de stratégies pour l'élaboration d'une législation type en matière de cybercriminalité. Les sept buts sont les suivants:

1 Elaborer des stratégies en vue d'établir une législation type en matière de cybercriminalité qui soit applicable à l'échelle mondiale et compatible avec les dispositions réglementaires en vigueur aux niveaux national et régional.
2 Elaborer des stratégies [...] en vue de créer des structures organisationnelles et des politiques appropriées aux niveaux national et régional dans le domaine de la cybercriminalité.
3 Concevoir une stratégie en vue de mettre en place des critères de sécurité et des mécanismes d'accréditation minimaux et mondialement acceptés pour les applications et les systèmes [...] logiciels.
4 Elaborer des stratégies en vue de créer un cadre mondial de veille, d'alerte et d'intervention en cas d'incident qui garantisse la coordination transfrontière des initiatives existantes et des initiatives nouvelles.
5 Concevoir des stratégies en vue de créer et d'entériner un système générique et universel d'identité numérique ainsi que les structures organisationnelles nécessaires pour faire en sorte que les justificatifs numériques [pour les personnes] soient reconnus au-delà des frontières géographiques.
6 Mettre au point une stratégie mondiale visant à faciliter le renforcement des capacités humaines et institutionnelles pour perfectionner les connaissances et le savoir-faire à tous les niveaux et dans tous les domaines susmentionnés.

7 Présenter des propositions relatives à un cadre pour une stratégie mondiale multi-parties prenantes de coopération, de dialogue et de coordination au niveau international dans tous les domaines susmentionnés.

Afin d'analyser et d'élaborer les mesures et les stratégies ayant trait aux sept objectifs du Programme mondial cybersécurité (GCA), le secrétariat général de l'UIT a créé un groupe d'experts de haut niveau (HLEG) réunissant des représentants des états membres, de l'industrie et du monde scientifique.[1135] En 2008, le groupe d'experts a conclu ses négociations et publié son « Rapport stratégique mondial ».[1136] En matière de cybercriminalité, le volet le plus important du rapport est constitué des mesures juridiques présentées au chapitre 1. Outre un aperçu général des différentes approches régionales et internationales de la lutte contre la cybercriminalité,[1137] ce chapitre fournit un résumé des dispositions de droit pénal,[1138] des instruments de procédure,[1139] les réglementations régissant la responsabilité des fournisseurs d'accès Internet[1140] et des mesures de sauvegarde visant à protéger les droits fondamentaux des utilisateurs d'Internet.[1141]

Renforcement de capacités

Sous l'égide du Programme mondial cybercriminalité de l'UIT, l'UIT-D aide les différents pays dans la mise en œuvre d'activités harmonisées en matière de cybersécurité au niveau national, régional et international. La mission de l'UIT en matière de renforcement de capacités a été réaffirmée par la résolution 130 (Rév. Guadalajara, 2010) de la Conférence plénipotentiaire de l'UIT. En vertu de cette résolution, l'UIT a pour mission d'assister les états membres, en particulier les pays en développement, dans l'élaboration de mesures juridiques adaptées et applicables en matière de protection contre les cybermenaces.

Cela englobe les activités de renforcement de capacités dans l'élaboration des stratégies nationales, de la législation et de l'application des lois, des structures organisationnelles (par exemple de surveillance, d'alerte et de réponse en cas d'incident), entre autres domaines. L'UIT a organisé plusieurs conférences régionales pendant lesquelles a été traitée spécifiquement, *inter alia*, la question de la cybercriminalité.[1142] Avec des partenaires des secteurs publics et privés, l'UIT-D a développé des outils de cybersécurité/CIIP pour aider les états membres à améliorer la sensibilisation au plan national, à mener des autoévaluations de cybersécurité au plan national, à réviser la législation et à renforcer les capacités en matière de surveillance, d'alerte et de réponse en cas d'incident. Parmi ces outils figurent la publication « Comprendre la cybercriminalité : guide pour les pays en développement », l'outil d'autoévaluation nationale cybersécurité/CIIP de l'UIT et le « Botnet Mitigation Toolkit » (outils pour prévenir la menace des Botnets) de l'UIT.

Résolutions

L'UIT a adopté plusieurs résolutions en matière de cybersécurité qui s'appliquent à la cybercriminalité, bien que ne traitant pas directement cette question dans des dispositions pénales spécifiques.

- Résolution 130 de la Conférence de plénipotentiaires de l'UIT (Rév. Guadalajara, 2010), sur le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication;
- Résolution 149 de la Conférence de plénipotentiaires de l'UIT (Antalya, 2006), sur l'étude des définitions et des termes relatifs à l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication;
- Résolution 45 (Doha, 2006) de la Conférence mondiale de développement des télécommunications (CMDT), relative à l'établissement de mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam et le rapport de la *Réunion sur les mécanismes de coopération pour la cybersécurité et la lutte contre le spam* (31 août – 1er septembre 2006);
- Résolution 50 (Rév. Johannesburg, 2008) de l'Assemblée mondiale de normalisation des télécommunications (WTSA), sur la cybersécurité;

- Résolution 52 (Rév. Johannesburg, 2008) de l'Assemblée mondiale de normalisation des télécommunications (WTSA), « lutter contre et combattre le spam »;
- Résolution 58 (Johannesburg, 2008) de l'Assemblée mondiale de normalisation des télécommunications (WTSA), « Encourager la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement ».

Projets cofinancés par l'UIT et l'UE dans les pays ACP

Pour soutenir l'élaboration des politiques et législations dans les pays ACP, l'UIT et l'UE ont décidé de cofinancer un projet [1143] dans le cadre du programme "ACP-Technologies de l'information et de la communication" et du neuvième Fonds européen de développement. Le projet a été subdivisé en trois sous-programmes régionaux, pour tenir compte des différences entre Afrique, Caraïbes et Pacifique en matière de progrès réalisés et de priorités. Les pays d'Afrique subsaharienne ont bénéficié du projet sur l'harmonisation des politiques relatives aux TIC en Afrique subsaharienne (projet HIPSSA), tandis que le projet visant à renforcer la compétitivité des pays des Caraïbes grâce à l'harmonisation des politiques, de la législation et des procédures réglementaires dans le domaine des TIC (projet HIPCAR) a été mis en oeuvre pour les pays des Caraïbes.[1144] Enfin, les pays du Pacifique ont également reçu un soutien avec le projet sur le renforcement des capacités politiques, réglementaires et législatives dans le domaine des TIC des Etats insulaires de la région Pacifique (projet ICB4PAC).

Les trois projets étaient divisés en deux grandes phases. Au cours de la première phase, une évaluation régionale de la législation existante a été réalisée, ainsi qu'une comparaison avec les bonnes pratiques internationales. À partir de cette évaluation et de consultations approfondies, des politiques et législations types ont été élaborées. Pendant la seconde phase, les pays ont bénéficié d'un soutien en vue de la transposition au niveau national des politiques types et de la législation type.

Harmonisation des politiques relatives aux TIC en Afrique subsaharienne (projet HIPSSA)

En 2004 déjà, l'UIT et l'UE ont lancé un projet pilote régional d'aide à la création d'un marché intégré des TIC en Afrique de l'Ouest (Harmonisation des marchés TIC pour les pays de la CEDEAO/UEMOA).[1145] En 2005, des lignes directrices relatives aux bonnes pratiques ont été adoptées[1146], suite à quoi les Ministres des TIC des pays de la CEDEAO ont adopté les décisions réglementaires harmonisées sur les TIC en 2006[1147] et l'Autorité des Chefs d'Etat et de Gouvernement de la CEDEAO a adopté les décisions sous la forme d'un acte additionnel en 2007.[1148]

Le projet HIPSSA, dont les pays bénéficiaires comptaient 42 pays d'Afrique subsaharienne[1149], a été conçu pour élargir le projet pilote susmentionné. Ce projet visait à l'élaboration et la promotion de politiques et lignes directrices relatives aux TIC harmonisées, afin de créer un environnement commercial durable[1150], ainsi qu'au renforcement des capacités humaines et institutionnelles dans le domaine des TIC grâce à une série de mesures en matière de formation, d'éducation et de partage des connaissances.

Renforcement de la compétitivité des pays des Caraïbes (projet HIPCAR)

En 2008, le projet HIPCAR, qui concerne 15 pays des Caraïbes, a été lancé.[1151] Ce projet vise à aider les pays du CARIFORUM[1152] à harmoniser leurs politiques et cadres juridiques dans le domaine des TIC. Au cours de son élaboration, neuf domaines de travail ont été identifiés[1153] ; pour chacun d'eux, des politiques et textes législatifs types ont été préparés au cours de la première phase du projet, afin de faciliter l'élaboration et l'harmonisation de la législation dans la région. Ces neuf domaines étaient les suivants : transactions électroniques (commerce), preuves électroniques, respect de la vie privée et protection des données, interception de communications, cybercriminalité, accès à l'information publique/liberté d'information, accès universel, interconnexion et, enfin, octroi de licences. Au cours de la seconde phase, plusieurs pays (dont la Barbade, la Grenade, Saint-Kitts-et-Nevis, Sainte-Lucie et la Trinité) ont reçu un appui pour le processus de transposition nationale.[1154]

Renforcement des capacités politiques, réglementaires et législatives dans le domaine des TIC des Etats insulaires de la région Pacifique (projet ICB4PAC)

A la demande des **Etats insulaires de la région Pacifique,** un projet apparenté baptisé ICB4PAC[1155] a prévu un renforcement des capacités en matière de politiques et de réglementations dans le domaine des TIC. Il était axé sur le renforcement des capacités humaines et institutionnelles dans le domaine des TIC grâce à la mise en œuvre de mesures en matière de formation, d'éducation et de partage des connaissances dans 15 Etats insulaires de la région Pacifique.[1156] Les domaines de travail visés sont par exemple l'octroi de licences et le numérotage, l'accès universel, l'interconnexion et la modélisation des coûts, ainsi que la cybercriminalité.

5.2 Approches régionales

Outre les organisations internationales qui œuvrent à l'échelle de la planète, plusieurs organisations internationales actives au niveau régional font progresser la problématique de la cybercriminalité.

5.2.1 Conseil de l'Europe[1157]

Le Conseil de l'Europe joue un rôle actif dans le combat contre la cybercriminalité.

Activités antérieures à 1995

En 1976, le Conseil de l'Europe soulignait le caractère international des cyberdélits et examinait ce sujet à l'occasion d'une conférence portant sur les divers aspects de la criminalité économique. Cette question est depuis une préoccupation majeure de l'organisation.[1158] En 1985, le Conseil de l'Europe a désigné un comité d'experts [1159] chargé d'examiner les aspects juridiques de la cybercriminalité[1160]. En 1989, le Comité européen pour les problèmes criminels a adopté le « rapport sur la criminalité liée à l'informatique »[1161], qui analyse des dispositions juridiques de fond en droit pénal qu'il est nécessaire de mettre en place pour lutter contre les nouvelles formes d'infraction électronique, y compris la fraude et la falsification informatiques. La même année, le Comité des ministres a adopté une recommandation[1162] qui mettait spécifiquement en avant le caractère international de la cybercriminalité:

> *Le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe, Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;*
> *Reconnaissant l'importance d'une réponse adéquate et rapide au nouveau défi de la criminalité informatique; Considérant que la criminalité informatique a souvent un caractère transfrontalier; Conscient de la nécessité qui en résulte d'une harmonisation plus poussée des législations et pratiques, et d'une amélioration de la coopération juridique internationale, Recommande aux gouvernements des Etats membres:*
> *1. De tenir compte, lorsqu'ils réviseront leur législation ou en prépareront une nouvelle, du rapport sur la criminalité liée à l'informatique, élaboré par le Comité européen pour les problèmes criminels, et, en particulier, des principes directeurs pour les législateurs nationaux;*
> *2. De faire rapport au Secrétaire Général du Conseil de l'Europe en 1993 sur toute évolution de leur législation, de leur pratique judiciaire, et de leurs expériences en matière de coopération juridique internationale relative à la criminalité informatique.*

En 1995, le Comité des ministres a adopté une recommandation traitant des conséquences de la cybercriminalité transnationale[1163]. En annexe à cette recommandation figure un résumé des principes directeurs relatifs à l'élaboration de dispositions législatives adaptées[1164].

Convention du Conseil de l'Europe sur la cybercriminalité et premier Protocole additionnel

En 1996, le Comité européen pour les problèmes criminels (CDPC) a décidé de créer un Comité d'experts chargés de la cybercriminalité[1165]. À l'époque de la création de ce comité, il était déjà question de ne pas s'en tenir à une nouvelle recommandation, mais d'élaborer une convention[1166]. Entre 1997 et 2000, le

comité a tenu dix séances plénières et quinze séances de son Groupe de rédaction à participation non limitée. L'Assemblée a adopté le projet de convention lors de la deuxième partie de sa session plénière d'avril 2001[1167]. La version définitive du projet de convention a été présentée pour approbation au CDPC, à la suite de quoi le texte a été présenté au Comité des ministres pour adoption et ouverture à la signature[1168]. La convention a été ouverte à la signature lors d'une cérémonie de signature tenue à Budapest le 23 novembre 2001. Lors de cette cérémonie, trente pays ont signé la convention (notamment quatre États non membres du Conseil de l'Europe: Canada, États-Unis, Japon et Afrique du Sud). En juin 2014, 47 États[1169] avaient signé la convention sur la cybercriminalité et 42 États[1170] l'avaient ratifiée[1171], dont quatre Etats[1172] n'ayant pas signé la Convention précédemment. Au total, 12 Etats[1173] ont été invités à prendre part à la Convention sur la cybercriminalité, mais ne l'ont pas fait[1174]. Cette convention est aujourd'hui reconnue comme un instrument international important de la lutte contre la cybercriminalité, et plusieurs organisations internationales la soutiennent[1175]. La Convention sur la cybercriminalité a été suivie d'un premier protocole additionnel[1176]. Au cours des négociations sur le texte de la convention, il est apparu que la pénalisation du racisme et de la diffusion de contenus xénophobes étaient des sujets particulièrement polémiques[1177]. Certains États, dotés d'une législation forte en faveur de la protection de la liberté d'expression[1178], ont fait part de leurs préoccupations et ont indiqué qu'ils ne pourraient pas signer la convention si cette dernière incluait des dispositions allant à l'encontre de ce principe[1179]. Dans sa quatrième ébauche datant de 1998, la Convention comportait toujours une disposition invitant les parties à pénaliser le contenu illégal « concernant en particulier des domaines tels que la pédopornographie et la xénophobie »[1180]. Pour éviter un blocage de pays qui n'auraient pu signer cette Convention à cause de préoccupations ayant trait à la liberté d'expression, ces questions ont été supprimées de la Convention sur la cybercriminalité pendant le processus de rédaction et intégrées à un protocole distinct. En juin 2014, 38 États[1181] avaient signé le Protocole additionnel et 20 États[1182] l'avaient ratifié.

Le débat autour de la Convention sur la cybercriminalité du Conseil de l'Europe

Actuellement, la Convention sur la cybercriminalité du Conseil de l'Europe demeure l'instrument soutenu par différentes organisations internationales ayant la portée la plus large.[1183] Cependant, le débat au cours du 12e Congrès sur la criminalité a souligné que, 10 ans après son ouverture aux adhésions, l'impact de la Convention est limité.[1184]

Limitation de la portée de la Convention sur la cybercriminalité du Conseil de l'Europe

En janvier 2011, les États-Unis restaient le seul pays hors de l'Europe à avoir ratifié la convention. Il est cependant exact que l'impact de la Convention ne peut être mesuré uniquement par le nombre de signatures ou de ratifications, car des pays tels que l'Argentine,[1185] le Pakistan,[1186] les Philippines,[1187] l'Égypte,[1188] le Botswana[1189] et le Nigéria[1190] ont utilisé la Convention comme modèle et ont élaboré une partie de leur législation conformément à la Convention sur la cybercriminalité, sans y avoir formellement adhéré. Cependant, même dans le cas de ces pays, la mesure dans laquelle ils ont utilisé la Convention sur la cybercriminalité comme modèle reste difficile à apprécier. Certains de ces pays ont également utilisé d'autres textes juridiques, comme la Directive de l'Union européenne sur les attaques contre les systèmes d'information et le Modèle de loi du Commonwealth. Étant donné que ces lois présentent un certain nombre de similitudes avec la Convention sur la cybercriminalité, et, par ailleurs, que les dispositions n'ont été que très rarement reproduites mot à mot, mais plutôt ajustées pour répondre aux exigences des pays, il est pratiquement impossible de déterminer si un pays a utilisé la Convention comme ligne directrice, et, si oui, dans quelle mesure. Malgré cela, selon le Conseil de l'Europe, plus de 100 pays auraient signé, ratifié ou utilisé la Convention pour élaborer une législation nationale.[1191] Toutefois, ce nombre n'a pas pu être vérifié. Le Conseil de l'Europe ne divulgue pas les noms des pays concernés, et fait uniquement référence à une « liste interne ». Même le nombre précis de pays concernés n'est pas dévoilé. Même s'il était possible de prouver que 100 pays ont utilisé la Convention sur la cybercriminalité, cela ne signifie pas nécessairement qu'ils aient harmonisé leur législation conformément à cette Convention. Les informations relativement vagues publiées par le Conseil de l'Europe laissent également en suspend la question de savoir si toutes les dispositions de la Convention sur la cybercriminalité ont été mises en œuvre, ou seulement une de ces dispositions.

Rapidité du processus de ratification

La portée territoriale limitée n'était pas la seule question débattue lors du 12e Congrès des Nations Unies sur la criminalité. La rapidité de signature et de ratification demeure très certainement un sujet de préoccupation. Neuf ans après la signature initiale par 30 états le 23 novembre 2001, seuls 17 autres états ont signé la Convention sur la cybercriminalité. À ce jour, aucun pays non membre du Conseil de l'Europe n'a adhéré à la Convention, bien que huit pays aient été invités à le faire.[1192] L'évolution du nombre de ratifications est la suivante: 2002 (2^{1193}), 2003 (2^{1194}), 2004 (4^{1195}), 2005 (3^{1196}), 2006 (7^{1197}), 2007 (3^{1198}), 2008 (2^{1199}), 2009 (3^{1200}), 2010 (4^{1201}), 2011 (2^{1202}), 2012 (6^{1203}) et 2013 (3)[1204]. À l'image du processus de ratification, le processus de mise en œuvre est très lent. En moyenne, il s'écoule cinq années entre la signature et la ratification de la Convention par un pays. Les écarts entre les pays sont significatifs. Alors que l'Albanie a ratifié la Convention en un peu plus de six mois, il a fallu près de dix ans à l'Allemagne pour le faire.

Absence d'évaluation des ratifications

À ce jour, le Conseil de l'Europe n'a évalué aucun des pays ayant soumis leur instrument de ratification pour savoir s'ils avaient effectivement mis en œuvre la Convention sur la cybercriminalité conformément aux exigences du texte. De sérieux doutes subsistent quant à sa pleine mise en œuvre, en particulier dans le cas des premiers pays ayant ratifié la Convention. Même dans de grands pays comme l'Allemagne et les États-Unis, il est peu probable que la Convention ait été intégralement mise en œuvre. L'Allemagne, par exemple, contrairement à l'objet de l'article 2 de la Convention sur la cybercriminalité, ne pénalise pas l'accès illégal aux systèmes informatiques, mais uniquement l'accès illégal aux données informatiques.[1205] Le profil pays de la législation des États-Unis en matière de cybercriminalité, posté sur le site Internet du Conseil de l'Europe, indique que la loi 18 USC § 1030(a)(1) – (5) correspond à l'article 2.[1206] Cependant, contrairement à l'article 2 de la Convention sur la cybercriminalité, la loi 18 USC § 1030(a) ne criminalise pas l'accès pur et simple un système informatique. Outre l'« accès » à un système informatique, cette disposition suppose des actes supplémentaires (par exemple l'« obtention » d'informations).[1207]

Débat mondial

Un des aspects souvent critiqués de la Convention sur la cybercriminalité est la représentation insuffisante des pays en voie de développement dans le processus de rédaction[1208]. Malgré la dimension transnationale de la cybercriminalité, son impact dans les diverses régions du monde est différent. Cela est particulièrement vrai pour les pays en développement.[1209] La Convention sur la cybercriminalité a non seulement été négociée sans une implication large des pays en développement d'Asie, d'Afrique et d'Amérique latine, mais elle impose également des conditions restrictives à la participation des États non membres du Conseil de l'Europe, alors même qu'elle était censée être ouverte à ces pays. En vertu de son article 37, l'accession à la Convention sur la cybercriminalité suppose de consulter les États contractants à la Convention et d'obtenir leur consentement unanime. En outre, la participation aux délibérations sur des amendements futurs possibles est restreinte aux Parties à la Convention.[1210] Le débat qui a eu lieu dans le cadre de la préparation du 12e Congrès des Nations Unies sur la criminalité a montré que les pays en développement, en particulier, sont intéressés par une approche internationale plutôt que prendre part à des initiatives régionales. Pendant les réunions préparatoires au 12e Congrès des Nations Unies sur la prévention du crime et la justice pénale pour l'Amérique latine et les Caraïbes[1211], l'Asie occidentale[1212], l'Asie-Pacifique[1213] et l'Afrique,[1214] les pays ont appelé de leurs vœux l'élaboration d'une convention internationale sur la cybercriminalité. Des appels similaires ont été lancés dans les milieux universitaires.[1215]

Absence de réponse aux tendances récentes

La cybercriminalité est un domaine criminel en perpétuelle évolution.[1216] Dans les années 1990, époque à laquelle la Convention sur la cybercriminalité a été élaborée, l'utilisation d'Internet à des fins terroristes[1217], les attaques de zombies (botnet)[1218] et l'hameçonnage[1219] étaient inconnus ou ne jouaient pas un rôle aussi important qu'aujourd'hui,[1220] et ne pouvaient donc pas être réglés par des solutions spécifiques. Le Conseil de l'Europe lui-même reconnaît que la Convention sur la cybercriminalité est en partie obsolète. Cela peut être aisément démontré en comparant les dispositions ayant trait à la pédopornographie dans la

Convention sur la cybercriminalité de 2001 et la Convention sur la protection des enfants de 2007. L'article 20 (1)(f) de la Convention sur la protection des enfants criminalise « le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie enfantine ». Cet acte n'est pas criminalisé par la Convention sur la cybercriminalité, bien que la référence aux TIC souligne que ce crime peut être qualifié de cybercrime. Sur la base des explications fournies dans le Rapport explicatif, les rédacteurs ont décidé d'inclure cette disposition pour couvrir les cas où les délinquants visualisent des images d'enfants en ligne en accédant à des sites de pédopornographie, mais sans effectuer de téléchargement. Cela signifie, par conséquent, que la Convention sur la cybercriminalité ne couvre pas de tels actes et, donc, à cet égard, ne respecte même pas les normes actuelles propres du Conseil de l'Europe.

La même chose est vraie en matière d'instruments de procédure. L'interception de communications vocales sur IP (VoIP), l'admissibilité de la preuve numérique et les procédures visant à intégrer l'utilisation croissante des technologies de chiffrement et des moyens de communication anonymes sont autant de sujets d'une grande pertinence pour la Convention sur la cybercriminalité, et pour autant non traités dans cette dernière. En 10 années d'existence, la Convention n'a jamais été amendée, et, outre le Protocole additionnel relatif au contenu à caractère xénophobe, aucune disposition où aucun instrument supplémentaire n'a été ajouté.

Avec l'évolution des technologies et des comportements criminels, le droit pénal doit être ajusté. Comme cela a été souligné précédemment, les exigences en matière de législation anticybercriminalité ont évolué au cours des dix dernières années. La nécessité d'une actualisation de la Convention sur la cybercriminalité est donc impérieuse. D'autres organisations régionales, comme l'Union européenne, viennent tout juste de réviser leurs instruments juridiques relatifs à la cybercriminalité, qui ont été intégrés plus récemment, il y a environ cinq ans. Malgré l'urgence de cette actualisation, il y a peu de chances pour que ce processus ait lieu. L'Union européenne, fervente défenseur de la Convention sur la cybercriminalité, a déclaré récemment que, de son point de vue, « actualiser la Convention [sur la cybercriminalité] [...] ne peut être considéré comme une option réalisable ».[1221]

Priorité à l'accession de pays capables de fournir une infrastructure contrairement aux pays en développement

Au cours des 10 dernières années le Conseil de l'Europe a échoué à obtenir l'adhésion de petits pays et de pays en développement. L'une des raisons est le fait que la Convention a été négociée avec une représentation insuffisante de pays en développement.[1222] En particulier, l'Asie et l'Afrique ont été sous-représentées, et l'Amérique latine n'a pas été représentée du tout. Bien que le Conseil de l'Europe invite les représentants des pays en développement à sa principale Conférence sur la cybercriminalité, ces pays ne sont pas autorisés à prendre part aux délibérations sur les amendements futurs possibles, car ces réunions sont réservées aux Parties à la Convention.[1223]

On observe également des différences dans le processus d'accession lorsque l'on compare avec des instruments réellement internationaux tels que les Conventions des Nations Unies. Malgré le processus d'adhésion à la Convention — conçu pour être ouvert aux états non membres —, des restrictions s'appliquent. Contrairement à une convention des Nations Unies, l'accession à la Convention sur la cybercriminalité suppose de consulter les états contractants à la Convention et d'obtenir leur consentement unanime.[1224] Par conséquent les pays en développement, en particulier, ont appelé, lors de la préparation du 12e Congrès des Nations Unies sur la criminalité, à une approche (plus) internationale. Pendant les réunions préparatoires régionales pour le Congrès pour l'Amérique latine et les Caraïbes[1225], l'Asie occidentale[1226], l'Asie-Pacifique[1227] et l'Afrique,[1228] les pays participants ont réclamé l'élaboration d'un instrument international.

Bien que la stratégie du Conseil de l'Europe consistant à donner la priorité aux pays occidentaux puisse sembler logique, car ils disposent de l'infrastructure, l'implication des pays émergeant est cruciale si la priorité doit intégrer les victimes potentielles. En 2005, le nombre d'utilisateurs d'Internet dans les pays en développement dépasse celui des nations industrielles.[1229] En excluant les pays en développement et en donnant la priorité aux pays développés qui fournissent (actuellement) la majeure partie de l'infrastructure et des services, deux aspects primordiaux sont ignorés: l'importance de protéger les (la majorité des)

utilisateurs de services Internet, et, en second lieu, l'influence de plus en plus croissante des pays émergents comme l'Inde, la Chine et le Brésil. Si l'on n'aide pas les pays en développement à élaborer une législation qui leur permette d'enquêter sur des affaires impliquant des citoyens de leurs pays et de coopérer internationalement avec d'autres services de répression en matière d'identification des délinquants, les enquêtes de cybercriminalité impliquant ces pays seront plus difficiles à mener. Le fait qu'aucun pays en développement n'ait adhéré à la Convention au cours des 10 dernières années montre les limites d'une approche régionale. Si l'on considère, en outre, qu'au cours de la dernière décennie le Conseil de l'Europe n'a invité que huit pays (sur 146 états membres des Nations Unies n'ayant pas ratifié la Convention) à adhérer à la Convention, le peu d'énergie investie sur cette question est flagrant. Cela est certainement lié au fait que les besoins des pays en développement, tant en termes de législation et de renforcement de capacités que d'assistance technique, vont généralement au-delà des mécanismes de la Convention. Jusqu'à aujourd'hui, le Conseil de l'Europe s'attache à aider les pays à aligner leur législation sur la Convention, mais n'offre aucune assistance dans l'élaboration d'une législation allant au-delà de la Convention (par exemple pour réduire les écarts mentionnés précédemment). Par ailleurs, les pays peuvent déjà avoir besoin d'aide pour élaborer une législation nationale, car les dispositions de la Convention nécessitent un ajustement pendant la phase de mise en œuvre. Certains pays, par exemple, ont besoin de déterminer qui est autorisé à ordonner certaines enquêtes (juges, procureurs, services de police) et sur quelles bases (témoignage sous serment, affidavit, information).

Cette question a été débattue en détail lors du 12e Congrès des Nations Unies sur la criminalité et a amené les États membres des Nations Unies à statuer sur l'élargissement du mandat de l'Office des Nations Unies contre la drogue et le crime (UNODC) en matière de renforcement de capacités dans le domaine de la cybercriminalité. [1230] D'autres organisations des Nations Unies comme l'Union internationale des télécommunications (UIT) ont récemment reçu des mandats similaires.[1231]

Peu adaptée aux petits pays et pays en développement

Les petits pays et les pays en développement rencontrent des difficultés dans la mise en œuvre des normes dictées par la Convention. Le fait que les plus petits États membres du Conseil de l'Europe n'aient pas ratifié[1232] la Convention au cours des 10 dernières années souligne clairement que cela présente des difficultés non seulement pour les petits pays hors de l'Europe, mais également pour les petits pays européens.

La nécessité d'établir un point de contact 24/7 est l'une des dispositions qui créent des difficultés pour la mise en œuvre de la convention dans les petits pays. Ces points de contact ont un effet extrêmement bénéfique sur la rapidité des enquêtes, et l'article 35 est, par conséquent, l'un des instruments les plus importants fournis par la Convention.[1233] Cependant, il faut noter que le Conseil de l'Europe a publié récemment une étude analysant l'efficacité de la coopération internationale dans la lutte contre la cybercriminalité [1234] et une étude sur le fonctionnement des points de contact 24/7 contre la cybercriminalité, [1235] et que le résultat de ces deux études démontre que les pays qui ont ratifié la Convention n'ont pas tous mis en place ce point de contact et que même les pays qui l'ont fait ne l'utilisent que de façon limitée.

Le principal problème pour les pays en développement est que la création de ce point de contact est obligatoire. Alors que, pour les pays développés, mettre en œuvre et maintenir ce point de contact ne posera vraisemblablement aucun problème en ayant recours à une force de police spécialisée dans la cybercriminalité affectée jour et nuit à cette tâche, cela pose un problème pour les pays où les forces de police spécialisées dans la cybercriminalité se limitent à un seul et unique agent de police. Dans ces cas, cette obligation entraînera des investissements importants. Que l'adhésion à la Convention et sa mise en œuvre n'entrainent pas de coûts associés pour les pays, comme cela a été déclaré récemment par un représentant du Conseil de l'Europe lors d'une conférence dans la région pacifique[1236], n'est donc vrai que si les coûts indirects, par exemple pour maintenir un point de contact 24/7 ou pour déployer une technologie afin d'enregistrer les données de trafic en temps réel, sont exclus.

Absence d'approche exhaustive

L'une des intentions au cœur de la Convention était de fournir une approche juridique exhaustive qui prenne en compte tous les domaines de la cybercriminalité.[1237] Mais comparer la Convention à d'autres approches — en particulier le modèle de loi du Commonwealth sur informatique et la criminalité informatique [1238] et des instruments de l'UE comme la Directive sur le commerce électronique[1239] — montre que des aspects importants n'ont pas été pris en compte. À titre d'exemple, on peut citer les dispositions ayant trait à l'admissibilité de la preuve électronique[1240] ou à la responsabilité des fournisseurs d'accès Internet (FAI). En particulier, l'absence d'une disposition contenant, au minimum, un cadre réglementaire de base ayant trait à l'admissibilité de la preuve électronique a des conséquences significatives, car la preuve électronique est largement caractérisée comme une nouvelle catégorie de preuve. [1241] Or, à moins qu'un pays ne dispose d'autres instruments ou que ses tribunaux ne déclarent ces preuves admissibles, ce pays ne pourra condamner aucun délinquant bien qu'il ait pleinement mis en œuvre la Convention.

Convention sur la protection des enfants

Dans le cadre de son approche visant à renforcer la protection des mineurs contre l'exploitation sexuelle, le Conseil de l'Europe a présenté une nouvelle Convention en 2007.[1242] Au premier jour de l'ouverture de la Convention sur la protection des enfants aux adhésions, 23 états ont signé la Convention. En juin 2014, elle comptait 47 états signataires,[1243] dont31 avaient ratifié la Convention.[1244] L'un des objectifs principaux de la Convention sur la protection des enfants est l'harmonisation des dispositions du droit pénal visant à protéger les enfants contre l'exploitation sexuelle.[1245] Pour atteindre cet objectif, la Convention contient un éventail de dispositions de droit pénal. À part la criminalisation des abus sexuels commis à l'encontre des enfants (article 18), la Convention contient des dispositions ayant trait à l'échange de contenus à caractère pédopornographique (article 20) et la sollicitation d'enfants à des fins sexuelles (article 23).

Négociations portant sur un autre protocole additionnel

Dès 2012, le Comité de la Convention sur la cybercriminalité[1246] a adopté un rapport portant sur l'accès transfrontalier et la compétence. [1247] Bien que la question de l'accès transfrontalier soit source de nombreuses préoccupations, il a été proposé dans le rapport que soit adopté un protocole additionnel spécifique. [1248] Alors que la Convention sur la cybercriminalité avait été négociée dans le cadre de discussions étroites, il a été proposé de recourir à un processus de consultation plus ouvert.[1249] En juin 2013, le Conseil de l'Europe a organisé des consultations publiques relatives à l'accès transfrontalier. D'après les rapports des participants, presque tous les experts se sont montrés critiques, à savoir les experts d'ONG, d'entreprises, d'Etats membres du Conseil de l'Europe, de la Commission européenne et les experts en protection des données du Conseil de l'Europe.[1250]

En 2013, un rapport du groupe de travail sur l'accès transfrontalier a été publié.[1251] Il propose une liste des composantes possibles d'un protocole additionnel, qui vont de l'accès transfrontalier avec consentement à différentes variations d'accès sans consentement.[1252] En novembre 2013, une note d'orientation relative à l'accès transfrontalier a été publiée.[1253]

5.2.2 Union européenne [1254]

Au cours de la décennie passée, l'Union européenne (UE) a élaboré plusieurs instruments juridiques traitant des aspects de la cybercriminalité. Bien que ces instruments ne soient généralement contraignants que pour les 27 états membres de l'UE, plusieurs pays et régions utilisent les normes de l'UE comme référence dans leurs discussions nationales et régionales sur l'harmonisation des législations.[1255]

Situation avant décembre 2009

Jusqu'à 2009, le mandat de l'UE en matière de droit pénal était limité et contesté.[1256] Outre le problème posé par la limitation de ce mandat, l'incertitude demeurait quant à savoir si le mandat pour toute législation pénale, y compris en matière de cybercriminalité, incombait à ce que l'on appelle le « premier

pilier » (Communauté européenne) ou au « troisième pilier » (Union européenne).[1257] L'opinion prévalent alors étant que le troisième pilier était responsable, l'harmonisation n'était, par conséquent, possible que sur la base d'une coopération intergouvernementale à l'intérieur du troisième pilier de l'Union européenne chargé de la police et de la coopération judiciaire dans les affaires criminelles.[1258] Quand, en 2005, la Cour de justice a déclaré illégal un instrument relevant du troisième pilier dans le domaine du droit pénal (la Décision-cadre du Conseil sur la protection de l'environnement par le droit pénal[1259])[1260], la distribution des pouvoirs a été remise en question pour la première fois. La cour décida que la Décision-cadre, étant indivisible, enfreignait l'article 47 de l'UE, car elle empiétait sur les pouvoirs conférés à la Communauté par l'article 175 de la CE. Cette décision a eu une influence majeure sur le débat sur l'harmonisation du droit pénal au sein de l'Union européenne. La Commission européenne (CE), chargée de faire respecter les traités de l'Union, a souligné que, à la suite du jugement, un certain nombre de décisions-cadres ayant trait au droit pénal étaient entièrement ou partiellement erronées, puisque tout ou partie de leurs dispositions ont été adoptées sur une base juridique fausse.[1261] Cependant, malgré la reconnaissance de nouvelles possibilités d'évaluation d'un mandat au sein du premier pilier, les initiatives de la CE ont été rares en raison de l'absence de traitement de cette thématique dans le premier pilier. En 2007, la Cour de justice a confirmé cette pratique juridique dans un second jugement.[1262]

Situation après la ratification du Traité de Lisbonne

Le Traité de Lisbonne (le « traité modificatif »),[1263] entré en vigueur en décembre 2009, a modifié le fonctionnement de l'Union européenne de façon significative. Outre l'abrogation de la distinction entre le « premier pilier » et le « troisième pilier », le traité conférait pour la première fois un mandant clair à l'UE dans le domaine de la criminalité informatique. Les articles 82 à 86 du Traité sur le fonctionnement de l'Union européenne (TFEU) confèrent à l'UE un mandat pour l'harmonisation du droit pénal (droit pénal matériel et droit procédural). L'article 83 du TFEU est particulièrement pertinent en matière de cybercriminalité.[1264] Il autorise l'UE à établir des règles minimales concernant les définitions des délits criminels et des sanctions relatives aux crimes sérieux ayant une dimension transnationale. La criminalité informatique est spécifiquement mentionnée comme l'un des domaines de la criminalité à l'article 83, paragraphe 1. Le terme « criminalité informatique » étant plus large que le terme « cybercriminalité », il autorise l'UE à réglementer ces deux domaines. En vertu de l'article 4, paragraphe 2j, l'élaboration d'une législation en matière de criminalité informatique relève de la compétence partagée entre l'UE et les États membres. Cela permet à l'UE d'adopter des actes juridiquement contraignants (article 2, paragraphe 2) et limite la capacité des États membres à exercer leur compétence dans la mesure où l'UE n'a pas exercé la sienne.

Dans le « Programme de Stockholm », adopté par le Conseil européen en 2009, l'UE précise qu'elle entend faire usage de son nouveau mandat.[1265] Le programme définit la priorité du travail de l'UE dans le domaine de la justice et des affaires intérieures pour une période de cinq ans, et fait suite au Programme de La Haye expiré en 2009.[1266] Il souligne l'intention de l'UE de faire usage de son mandat en faisant référence aux domaines de la criminalité mentionnés à l'article 83 du TFEU, paragraphe 1, et donne la priorité aux domaines de la pédopornographie et de la criminalité informatique.[1267]

Vue d'ensemble des instruments et directives de l'UE

Malgré les changements fondamentaux dans la structure de l'UE, les instruments adoptés dans le passé sont toujours en vigueur. En vertu de l'article 9 du Protocole sur les dispositions transitoires, les instruments adoptés sur la base du Traité sur l'Union européenne avant l'entrée en vigueur du Traité de Lisbonne sont maintenus jusqu'à ce qu'ils soient abrogés, annulés ou amendés pour la mise en oeuvre de ces traités. Le chapitre suivant fournit donc un aperçu de l'ensemble les instruments de l'UE en vigueur.

Politiques générales

Dès 1996, l'UE prenait acte des risques liés à Internet dans une communication traitant du contenu illégal et préjudiciable sur Internet.[1268] L'UE soulignait l'importance d'une coopération entre les États membres pour combattre le contenu illégal en ligne.[1269] En 1999, Le Parlement européen et le Conseil ont adopté un plan d'action pour promouvoir une utilisation plus sûre d'Internet et combattre le contenu illégal et

préjudiciable sur les réseaux mondiaux.[1270] Le plan d'action insistait sur l'autorégulation plutôt que sur la criminalisation. En 1999 encore, l'UE lançait l'initiative « eEurope », adoptant la communication de la Commission européenne « eEurope – une société de l'information pour tous ».[1271] L'initiative définissait les objectifs clés, mais ne traitait pas de la criminalisation des actes illégaux commis en utilisant des technologies de l'information. En 2001, la Commission européenne (CE) a publié une communication intitulée « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la criminalité informatique ».[1272] Dans cette communication, la CE analysait et traitait le problème de la cybercriminalité et soulignait la nécessité de mettre en oeuvre une action efficace pour répondre aux menaces pour l'intégrité, la disponibilité et la fiabilité des systèmes et réseaux d'information.

Les infrastructures de l'information et de la communication sont devenues une composante essentielle de nos économies, qui, malheureusement, n'est pas sans faiblesses et ouvre la voie aux comportements criminels. Ces activités criminelles peuvent prendre des formes très variées et franchir nombre de frontières. Bien qu'il n'existe, pour certaines raisons, aucune donnée statistique fiable, il ne fait aucun doute que ces infractions constituent une menace pour les investissements et les actifs des entreprises, ainsi que pour la sécurité et la confiance dans la société de l'information. On rapporte que certains exemples récents de refus de service et d'attaques de virus auraient causé d'importants préjudices financiers.
Plusieurs actions sont envisageables, tant par la prévention des activités criminelles en renforçant la sécurité des infrastructures de l'information qu'en dotant de moyens d'action appropriés les autorités chargées de l'application des lois, tout en respectant intégralement les droits fondamentaux de la personne.[1273]
La Commission, qui a pris part aux discussions du Conseil de l'Europe comme à celles du G8, reconnaît la complexité des questions de droit procédural et les difficultés qui s'y attachent. Il est toutefois vital qu'au sein de l'Union européenne, la lutte contre la cybercriminalité soit menée dans le cadre d'une coopération efficace, si l'on veut rendre la société de l'information plus sûre et créer un espace de liberté, de sécurité et de justice[1274].
La Commission présentera des propositions législatives en vertu du titre VI du traité sur l'Union européenne: [...] pour rapprocher davantage les systèmes de droit pénal matériel dans le domaine de la criminalité utilisant de hautes technologies. Ceci pourrait englober les infractions concernant, entre autres, le piratage et les attaques par déni de service. La Commission va également étudier les possibilités de lutter contre le racisme et la xénophobie sur l'Internet afin de présenter, en vertu du titre VI du traité sur l'Union européenne, une décision-cadre s'appliquant aux activités racistes et xénophobes tant hors ligne qu'en ligne. Enfin, le problème des drogues illicites sur l'Internet sera également examiné.[1275]
La Commission continuera à jouer pleinement son rôle en veillant à ce que les Etats membres coordonnent leur action dans d'autres enceintes internationales où la question de la cybercriminalité est examinée, telles que le Conseil de l'Europe et le G8. Les initiatives que prendra la Commission au niveau de l'Union européenne tiendront dûment compte des progrès réalisés au sein d'autres enceintes internationales, tout en s'attachant à rapprocher les positions à l'intérieur de l'Union européenne.[1276]

Outre la communication sur la cybercriminalité, la Commission a publié en 2001 une communication sur la « Sécurité des réseaux et de l'information »[1277], qui analyse les problèmes de sécurité dans les réseaux et propose des grandes lignes stratégiques pour l'action dans ce domaine.

Ces deux communications soulignent la nécessité d'un rapprochement des législations de fond en droit pénal au sein de l'Union européenne, notamment en ce qui concerne les attaques visant des systèmes d'information. En matière de lutte contre la cybercriminalité, il est admis que l'harmonisation de ces législations est un élément clé de tous les projets entrepris au niveau de l'Union[1278].

En 2007, la CE publiait une communication allant dans le sens d'une politique générale sur la lutte contre la cybercriminalité.[1279] La communication résume la situation actuelle et insiste sur l'importance de la Convention du Conseil de l'Europe sur la cybercriminalité en tant qu'instrument international prédominant dans la lutte contre la cybercriminalité. Par ailleurs, la communication souligne les questions sur lesquelles la CE portera ses efforts dans ses activités futures:

- renforcer la coopération internationale dans la lutte contre la cybercriminalité ;

- mieux coordonner le soutien financier pour les activités de formation ;
- organisation d'une réunion des experts en application de la loi ;
- renforcer le dialogue avec l'industrie ;
- surveiller l'évolution des menaces de cybercriminalité pour évaluer la nécessité de nouvelles législations.

Directive sur le commerce électronique (2000)

La directive de l'UE sur le commerce électronique[1280] traite, entre autres, de la responsabilité des fournisseurs d'accès Internet (FAI) pour les actes commis par des tiers (article 12 *et seq.*). Prenant en compte les défis découlant de la dimension internationale du réseau, les rédacteurs ont décidé d'élaborer des normes juridiques pour constituer un cadre pour le développement global de la société de l'information et pour soutenir le développement économique global ainsi que le travail des agences de répression.[1281] Cette démarche est fondée sur le constat qu'un certain nombre d'obstacles juridiques au bon fonctionnement du marché interne entravent le développent des services de la société de l'information, ce qui confère à la Communauté européenne son mandat.[1282] L'encadrement de la responsabilité est fondé sur le principe de responsabilité progressive.[1283] Bien que la directive souligne qu'il n'existe aucune intention d'harmoniser le domaine du droit pénal en tant que tel, elle réglemente par ailleurs la responsabilité en vertu du droit pénal.[1284]

Décision du Conseil pur lutter contre la pédopornographie sur Internet (1999)

En 2000, le Conseil de l'Union européenne a entamé une démarche pour traiter de la pédopornographie sur Internet. La décision adoptée était une suite à la communication de 1996 sur le contenu illégal et préjudiciable sur Internet[1285] et le plan d'action de 1999 y afférent visant à promouvoir une utilisation plus sûre d'Internet et à combattre le contenu illégal et préjudiciable sur les réseaux mondiaux.[1286] Toutefois, la décision ne contient aucune obligation à l'égard à l'adoption de dispositions pénales spécifiques.

Décision-cadre du Conseil de l'Union européenne relative à la lutte contre la fraude (2001)

En 2001, l'UE a adopté le premier cadre juridique traitant directement des différents aspects de la cybercriminalité. La décision-cadre de l'UE concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[1287] contient des obligations d'harmonisation du droit pénal eu égard aux spécificités de la fraude informatique et à la production d'instruments, tels que les programmes informatiques, spécialement conçus aux fins de commettre des infractions nommées dans la décision-cadre[1288].

> ***Article 3*** *– Infractions liées à l'utilisation de l'informatique*
> *Chaque État membre prend les mesures nécessaires pour que les agissements visés ci-après constituent une infraction pénale s'ils sont intentionnels:*
> *effectuer ou faire effectuer un transfert d'argent ou de valeur monétaire, causant ainsi de manière illicite une perte de propriété à un tiers dans le but de procurer un avantage économique illégal à la personne qui commet l'infraction ou à une tierce partie, en:*
> *— introduisant, altérant, effaçant ou supprimant des données informatiques, en particulier des données permettant l'identification, ou*
> *— perturbant le fonctionnement d'un logiciel ou d'un système informatique.*

Conformément à l'opinion majoritaire à cette époque, et en raison de l'absence de mandat au sein du premier pilier, cet instrument a été élaboré en vertu du troisième pilier, soulignant ainsi que, eu égard à la dimension internationale du phénomène impliqué, ces sujets ne peuvent être traités de manière appropriée par les États membres eux-mêmes.

Décision-cadre du Conseil de l'Union européenne relative aux attaques visant les systèmes d'information (2005)[1289]

Après la publication de sa politique générale en 2001, la CE a présenté une proposition de décision-cadre relative aux attaques visant les systèmes d'information.[1290] Elle fut modifiée et adoptée par le Conseil en 2005.[1291] Cet instrument a depuis été remplacé par la Directive de 2012 (voir ci-après).Bien qu'elle prenne acte de la Convention du Conseil de l'Europe sur la cybercriminalité,[1292] la décision-cadre s'attache à l'harmonisation des dispositions du droit pénal matériel censées protéger les éléments d'infrastructure. Certains aspects du droit pénal procédural (en particulier l'harmonisation des instruments nécessaires aux enquêtes de cybercriminalité et aux poursuites de leurs auteurs) et des instruments de coopération internationale n'ont pas été intégrés à la décision-cadre. Cela souligne les écarts et les différences entre les cadres juridiques des États membres et la nécessité d'une police et d'une coopération judiciaire efficace dans le domaine des attaques contre les systèmes d'information.[1293]

Article 2 *– Accès illicite à des systèmes d'information*
1. Les Etats membres prennent les mesures nécessaires pour faire en sorte que l'accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un système d'information devienne une infraction pénale punissable, au moins dans les cas où les faits ne sont pas sans gravité.
2. Les Etats membres peuvent décider que le comportement visé au paragraphe 1 ne soit érigé en infraction pénale qu'en cas d'infraction à une mesure de sécurité.
Article 3 *– Atteinte à l'intégrité du système*
Les Etats membres prennent les mesures nécessaires pour faire en sorte que le fait de provoquer intentionnellement une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données informatiques devienne une infraction pénale punissable lorsque l'acte est commis sans que l'auteur en ait le droit, au moins dans les cas où les faits ne sont pas sans gravité.
Article 4 *– Atteinte à l'intégrité des données*
Les Etats membres prennent les mesures nécessaires pour faire en sorte que le fait d'effacer, d'endommager, de détériorer, de modifier, de supprimer ou de rendre inaccessibles des données informatiques d'un système d'information de manière intentionnelle devienne une infraction pénale punissable lorsque l'acte est commis sans que l'auteur en ait le droit, au moins dans les cas où les faits ne sont pas sans gravité.

Directive relative à la conservation des données (2005)

En 2005, le Conseil a adopté la Directive européenne relative à la conservation des données[1294]. L'élément clé de cette directive est l'obligation faite aux fournisseurs de services Internet de stocker les données de trafic qui sont nécessaires à l'identification des délinquants dans le cyberespace. En 2014, la Cour de justice des Communautés européennes a déclaré la directive invalide.[1295]

Article 3 *– Obligation de conservation de données*
1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les Etats membres prennent les mesures nécessaires pour que les données visées à l'article 5 de la présente directive soient conservées, conformément aux dispositions de cette dernière, dans la mesure où elles sont générées ou traitées dans le cadre de la fourniture des services de communication concernés par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans leur ressort.
2. L'obligation de conserver les données visées au paragraphe 1 inclut la conservation des données visées à l'article 5 relatives aux appels téléphoniques infructueux, lorsque ces données sont générées ou traitées, et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet), dans le cadre de la fourniture des services de communication concernés, par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'Etat membre concerné. La présente directive n'impose pas la conservation des données relatives aux appels non connectés.

Le fait que les informations clés concernant toute communication sur Internet entrent dans le champ d'application de cette directive a donné lieu à de vives critiques de la part d'organisations de défense des droits de l'homme et pourrait entraîner une révision de la directive et de sa mise en œuvre par certaines cours constitutionnelles[1296]. Dans la conclusion de l'affaire *Productores de Música de España (Promusicae)* v. *Telefónica de España*,[1297] le conseiller auprès de la Cour de justice européenne, l'avocat général Juliane Kokott, a souligné que la mise en œuvre de l'obligation de conservation de données sans violation des droits fondamentaux était discutable[1298]. Les difficultés éventuelles concernant la mise en œuvre de ces réglementations avaient déjà été soulignées par le G8 en 2001.[1299]

La directive était fondée sur le mandat de la Communauté européenne pour le marché intérieur (article 95).[1300] Les rédacteurs ont souligné que les différences entre les normes juridiques et techniques en matière de rétention de données aux fins d'enquêtes de cybercriminalité constituent des obstacles au marché intérieur pour les communications électroniques, dans la mesure où les fournisseurs de service sont confrontés à des exigences différentes, entraînant des investissements différents.[1301] L'Irlande, soutenue par la Slovaquie, a demandé à la Cour de justice européenne d'annuler la Directive au motif qu'elle n'avait pas été adoptée sur une base juridique appropriée. Les deux pays ont argumenté que l'article 95 n'était pas une base suffisante, puisque la priorité de ce texte n'était pas le fonctionnement du marché intérieur, mais l'enquête, la détection et la poursuite d'actes criminels. La Cour européenne de justice a rejeté l'action au motif qu'elle était infondée, soulignant que les différences eu égard aux obligations de rétention de données auraient un impact direct sur le fonctionnement du marché intérieur.[1302] Elle soulignait par ailleurs que cette situation justifiait la législature de la Communauté visant à atteindre l'objectif de sauvegarde du bon fonctionnement du marché intérieur par l'adoption de règles harmonisées.

En 2014, la Cour de justice des Communautés européennes a finalement constaté la nullité de la directive.[1303] D'après les conclusions de la Cour, la directive comporte une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux liés au respect de la vie privée et à la protection des données à caractère personnel, sans que cette ingérence soit limitée au strict nécessaire. Les Etats membres ne sont par conséquent plus liés par cette directive, mais les lois nationales mises en œuvre conformément à cette dernière ne sont pas automatiquement invalidées. On ne sait pas pour l'heure si l'Union européenne présentera et adoptera une nouvelle directive.

Modification de la décision-cadre du Conseil de l'Union européenne relative à la lutte contre le terrorisme (2007)

En 2007, l'Union européenne a entamé des discussions sur un projet de modification de la décision-cadre sur la lutte contre le terrorisme[1304]. Dans l'introduction du projet de modification, l'Union européenne souligne que le cadre juridique existant sanctionne pénalement l'aide ou la complicité et l'incitation, mais pas la diffusion de savoir-faire terroriste par Internet[1305]. Par ce projet, l'Union européenne vise à combler l'écart et à rapprocher les législations nationales de la Convention du Conseil de l'Europe pour la prévention du terrorisme.

> ***Article 3*** *– Infractions liées aux activités terroristes*
> *1. Aux fins de la présente décision-cadre, on entend par:*
>
> *a) "provocation publique à commettre une infraction terroriste", la diffusion ou toute autre forme de mise à disposition du public d'un message, avec l'intention d'inciter à la commission d'un des actes énumérés à l'article 1er, paragraphe 1, points a) à h), lorsqu'un tel comportement, qu'il préconise directement ou non la commission d'infractions terroristes, crée un danger qu'une ou plusieurs de ces infractions puissent être commises;*
>
> *b) "recrutement pour le terrorisme", le fait de solliciter une autre personne pour commettre l'un des actes énumérés à l'article 1er, paragraphe 1, ou à l'article 2, paragraphe 2;*
>
> *c) "entraînement pour le terrorisme", le fait de fournir des instructions pour la fabrication ou l'utilisation d'explosifs, d'armes à feu, d'autres armes ou de substances nocives ou dangereuses, ou pour d'autres méthodes ou techniques spécifiques, en vue de commettre l'un des actes énumérés à l'article 1er, paragraphe 1, en sachant que la formation dispensée a pour but de servir à la réalisation d'un tel objectif.*

2. Chaque Etat membre prend les mesures nécessaires pour que soient également considérés comme des infractions liées aux activités terroristes les actes intentionnels suivants:

a) la provocation publique à commettre une infraction terroriste;

b) le recrutement pour le terrorisme;

c) l'entraînement pour le terrorisme;

d) le vol aggravé commis en vue de réaliser l'un des actes énumérés à l'article 1er, paragraphe 1

e) le chantage en vue de réaliser l'un des actes énumérés à l'article 1er, paragraphe 1;

f) l'établissement de faux documents administratifs en vue de réaliser l'un des actes énumérés à l'article 1er, paragraphe 1, points a) à h), ainsi qu'à l'article 2, paragraphe 2, point b).

3. Pour qu'un acte soit passible de poursuites comme prévu au paragraphe 2, il n'est pas nécessaire qu'une infraction terroriste soit effectivement commise."

En vertu de l'article 3, paragraphe .1, point c)[1306] de la décision-cadre, les États membres sont tenus, par exemple, d'ériger en infraction pénale la publication d'instructions sur l'utilisation d'explosifs lorsque ces informations sont destinées à servir à des fins terroristes. La nécessité de prouver que les informations sont destinées à servir à des fins terroristes permet très probablement d'assurer que la majorité des informations disponibles en ligne sur le maniement des armes – qui ne sont pas directement liées à des attaques terroristes – n'entrent pas dans le champ de la disposition. La plupart des armes et des explosifs pouvant servir à commettre à la fois des infractions « ordinaires » et des attentats terroristes (double usage), l'information seule peut difficilement constituer une preuve du fait que la personne qui l'a publiée avait connaissance de son utilisation ultérieure. Il est donc nécessaire de tenir compte du contexte de diffusion (site Internet géré par une organisation terroriste par exemple).

Directive sur la pédopornographie (2011)

Le premier projet de cadre juridique relatif à la cybercriminalité présenté après la ratification du Traité de Lisbonne était la proposition de Directive relative au combat contre les abus sexuels et l'exploitation sexuelle des enfants et la pédopornographie[1307] qui a été adoptée en 2011.[1308] Les rédacteurs ont souligné que les technologies de l'information permettaient aux délinquants de produire et de distribuer de la pornographie infantile plus facilement[1309] et insistaient sur l'importance d'apporter une réponse aux problèmes en résultant par des dispositions spécifiques. La directive adopte des normes internationales, comme la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.[1310]

Article 5 – *Infractions liées à la pédopornographie*

1. Les États membres prennent les mesures nécessaires pour que les comportements intentionnels visés aux paragraphes 2 à 6, lorsqu'ils sont commis sans droit, soient punissables.

2. L'acquisition ou la détention de pédopornographie est passible d'une peine maximale d'au moins un an d'emprisonnement.

3. Le fait d'accéder, en connaissance de cause et par le biais des technologies de l'information et de la communication, à de la pédopornographie est passible d'une peine maximale d'au moins un an d'emprisonnement.

4. La distribution, la diffusion ou la transmission de pédopornographie est passible d'une peine maximale d'au moins deux ans d'emprisonnement.

5. Le fait d'offrir, de fournir ou de mettre à disposition de la pédopornographie est passible d'une peine maximale d'au moins deux ans d'emprisonnement.

6. La production de pédopornographie est passible d'une peine maximale d'au moins trois ans d'emprisonnement.

7. Il appartient aux États membres de décider si le présent article s'applique aux cas de pédopornographie visés à l'article 2, point c) iii), lorsque la personne qui paraît être un enfant était en fait âgée de 18 ans ou plus au moment de la représentation.

8. Il appartient aux États membres de décider si les paragraphes 2 et 6 du présent article s'appliquent aux cas où il est établi que du matériel pornographique tel que visé à l'article 2, point c) iv), est produit et détenu par le producteur uniquement pour son usage privé, pour autant qu'aucun matériel pornographique tel que visé à l'article 2, point c), i), ii) ou iii), n'a été utilisé aux fins de la production, et à condition que cet acte ne comporte aucun risque de diffusion du matériel.

Comme la Convention, la Directive propose de criminaliser l'accès au contenu à caractère pédopornographique par l'utilisation de technologies d'information et de communication.[1311] Cela permet aux services de répression de poursuivre les délinquants lorsqu'ils sont en mesure de prouver que le délinquant a ouvert des sites Internet proposant du contenu pédopornographique, mais pas que le délinquant a téléchargé du contenu. Ce genre de difficulté à réunir des preuves survient, par exemple, lorsque le délinquant utilise une technologie de chiffrement pour protéger les fichiers téléchargés sur son dispositif de stockage de données.[1312] Le rapport explicatif de la Convention relative à la protection de l'enfance souligne que cette disposition doit également être appliquée dans les cas où le délinquant se contente de visualiser des images de pédopornographie en ligne sans les télécharger.[1313] En général, l'ouverture d'un site Web déclenche automatiquement un processus de téléchargement — souvent sans que l'utilisateur le sache.[1314] Par conséquent, cette disposition s'applique principalement dans les cas où la consommation de pédopornographie peut avoir lieu sans téléchargement de contenu. Cela peut être le cas, par exemple, des sites Web permettant la lecture de vidéos en flux continu, le processus technique de la lecture en flux (streaming) consistant à ne pas stocker en mémoire tampon l'information et à l'ignorer immédiatement après la transmission.[1315]

Article 25 – *Mesures contre les sites internet contenant ou diffusant de la pédopornographie*
1. Les États membres prennent les mesures nécessaires pour faire rapidement supprimer les pages internet contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire et s'efforcent d'obtenir la suppression des pages hébergées en dehors de celui-ci.
2. Les États membres peuvent prendre des mesures pour bloquer l'accès par les internautes sur leur territoire aux pages internet contenant ou diffusant de la pédopornographie. Ces mesures doivent être établies par le biais de procédures transparentes et fournir des garanties suffisantes, en particulier pour veiller à ce que les restrictions soient limitées à ce qui est nécessaire et proportionné, et que les utilisateurs soient informés de la raison de ces restrictions. Ces garanties incluent aussi la possibilité d'un recours judiciaire.

Outre la criminalisation des actes ayant trait à la pédopornographie, le projet initial contenait une disposition obligeant les États membres à mettre en oeuvre le processus de blocage des sites Web proposant du contenu à caractère pédopornographique.[1316] Plusieurs pays européens,[1317] de même que des pays non européens comme la Chine,[1318] l'Iran[1319] et la Thaïlande,[1320] utilisent une approche similaire. Le fait qu'aucun de ces concepts techniques n'ait prouvé son efficacité suscite des interrogations,[1321] et cette approche implique un risque concomitant de surblocage.[1322] Par conséquent, l'obligation de surblocage a été supprimée et la décision de mettre en oeuvre le blocage obligatoire au niveau national est laissée aux États membres.

Directive relative aux attaques contre les systèmes d'information (2013)

En septembre 2010, l'Union européenne a présenté une proposition de Directive relative aux attaques contre les systèmes d'information[1323], qui a été adoptée en 2013.[1324] Comme cela a été décrit en détail précédemment, l'UE a adopté en 2005 une Décision-cadre du Conseil relative aux attaques contre les systèmes d'information.[1325] Le mémoire explicatif à la proposition précise que l'intention des rédacteurs était d'actualiser et de renforcer le cadre juridique pour lutter contre la cybercriminalité dans l'Union européenne en apportant une réponse aux nouvelles méthodes utilisées pour commettre ce genre de délits.[1326] Outre la criminalisation de l'accès illégal (article 3), l'atteinte illégale à l'intégrité des systèmes (article 4) et l'atteinte illégale à l'intégrité des données (article 5) déjà introduites par la Décision-cadre de 2005, le projet de Directive de 2010 inclut deux infractions supplémentaires.

Article 6 *– Interception illégale*
Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'interception, effectuée par des moyens techniques, de transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques, lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.
Article 7 *– Outils utilisés pour commettre les infractions*
Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition intentionnelles d'un des outils suivants lorsque l'acte est commis sans droit et dans l'intention de l'utiliser pour commettre l'une des infractions visées aux articles 3 à 6, au moins lorsqu'il ne s'agit pas de cas mineurs:
a) un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées aux articles 3 à 6;
b) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information.

Ces deux dispositions sont en grande partie conformes aux dispositions correspondantes de la Convention sur la cybercriminalité.

Points communs avec la Convention du Conseil de l'Europe sur la cybercriminalité

Comme cela a été souligné précédemment, la Convention du Conseil de l'Europe sur la cybercriminalité a été négociée entre 1997 et 2000. En 1999, l'Union européenne a exprimé son point de vue à propos de la Convention sur la cybercriminalité.[1327] Elle a appelé les États membres à soutenir l'élaboration du projet de Convention du Conseil de l'Europe sur la cybercriminalité.[1328] À cette époque, l'UE elle-même ne disposait d'aucun mandat pour développer un cadre juridique similaire. La ratification du Traité de Lisbonne a modifié cette situation. Cependant, à ce jour l'UE n'a pas décidé de revoir sa position concernant la Convention sur la cybercriminalité. Dans le Programme de Stockholm, elle soulignait que l'UE appelait non seulement les États membres à ratifier la Convention sur la cybercriminalité, mais déclarait également que, du point de vue de l'UE, elle devrait devenir le cadre juridique de référence pour la lutte contre la cybercriminalité au plan mondial.[1329] Toutefois, cela n'implique pas que l'UE ne puisse proposer une approche exhaustive de la cybercriminalité, puisque les approches de l'UE présentent deux avantages majeurs. En premier lieu, les directives de l'UE doivent être mises en oeuvre dans un délai court et précis, alors que le Conseil de l'Europe ne dispose d'aucun moyen pour exiger la signature et la ratification des conventions, hormis les pressions politiques.[1330] En second lieu, l'UE a pour pratique d'actualiser en permanence ses instruments, alors que la Convention du Conseil de l'Europe sur la cybercriminalité n'a fait l'objet d'aucune actualisation au cours des 13 dernières années.

5.2.3 Organisation de coopération et de développement économiques[1331]

En 1983, l'Organisation de coopération et de développement économiques (OCDE) a lancé une étude sur la possibilité d'une harmonisation internationale du droit pénal afin de faire face au problème de la cybercriminalité[1332]. En 1985, elle a publié un rapport contenant une analyse de la législation en vigueur à l'époque ainsi que des propositions pour lutter contre la cybercriminalité[1333]. Elle recommandait aux États d'envisager la pénalisation d'une liste minimale d'infractions, notamment la fraude informatique, la falsification informatique, la modification de programmes et de données informatiques et l'interception de communications. En 1990, le Comité de la politique de l'information, de l'informatique et des communications (PIIC) a mis en place un groupe d'experts chargé d'élaborer un ensemble de lignes directrices régissant la sécurité de l'information, lesquelles ont été adoptées par le Conseil de l'OCDE en 1992[1334]. Les lignes directrices abordent, entre autres, la question des sanctions:

Les sanctions pour utilisation abusive des systèmes d'information sont un moyen important de protection des intérêts des personnes dépendant de ces systèmes contre les préjudices causés par des attaques visant la disponibilité, la confidentialité et l'intégrité de ces systèmes et de leurs composants. Ces attaques concernent notamment le fait de causer aux systèmes d'information des dommages ou des perturbations par insertion de virus ou de vers, altération de données, accès illégal à des données, fraude ou falsification informatique, et reproduction non autorisée de programmes informatiques. Pour lutter contre ces menaces, les Etats ont décidé de décrire ces actes de malveillance et de riposter contre ces actes de diverses manières. On s'accorde de plus en plus au niveau international sur le noyau minimal des infractions informatiques devant entrer dans le champ des législations pénales nationales. En témoigne l'évolution de la législation relative aux infractions informatiques et à la protection des données dans les pays membres de l'OCDE au cours des vingt dernières années ainsi que les travaux de l'OCDE et d'autres organisations internationales sur la législation en matière de lutte contre la cybercriminalité [...]. Il convient de passer périodiquement en revue les législations nationales afin de veiller à ce qu'elles couvrent correctement les risques que présente l'utilisation abusive des systèmes d'information.

Les lignes directrices ont été réexaminées en 1997, puis actualisées par un deuxième groupe d'experts mis en place par le PIIC en 2001. En 2002, une nouvelle version intitulée « Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité » a été adoptée en tant que recommandation du Conseil de l'OCDE [1335]. Ces lignes directrices contiennent neuf principes complémentaires:

1) Sensibilisation
Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.
2) Responsabilité
Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.
3) Réaction
Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.
4) Ethique
Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.
5) Démocratie
La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.
6) Evaluation des risques
Les parties prenantes doivent procéder à des évaluations des risques.
7) Conception et mise en œuvre de la sécurité
Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.
8) Gestion de la sécurité
Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.
9) Réévaluation
Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

En 2005, l'OCDE a publié un rapport dans lequel elle analyse les effets du spam sur les pays en développement.[1336] Ce rapport montre que le spam est un problème beaucoup plus grave dans les pays en développement que dans les pays occidentaux comme les États membres de l'OCDE, car les ressources y sont plus limitées et plus coûteuses[1337]. Pour faire suite à la demande du Groupe de la planification stratégique du Bureau exécutif du Secrétaire général des Nations Unies concernant l'élaboration d'un exposé comparatif des solutions législatives internes en matière d'utilisation d'Internet à des fins terroristes, l'OCDE a publié en 2007 un rapport sur le traitement législatif du « cyberterrorisme » dans la législation interne des États[1338]. En 2008, l'OCDE a publié un document d'orientation sur le vol d'identité en

ligne.[1339] Ce document fournit une vue d'ensemble des caractéristiques du vol d'identité, des différentes formes de vol d'identité, des questions ayant trait aux victimes ainsi que des mécanismes d'application des lois. Ce document souligne que la plupart des pays de l'OCDE ne traitent pas ce problème *per se* par des dispositifs spécifiques, et que la criminalisation éventuelle du vol d'identité de façon autonome doit être envisagée.[1340] En 2009, l'OCDE a publié un rapport sur les logiciels malveillants.[1341] Bien que ce rapport traite brièvement des différents aspects de la criminalisation, sa priorité est d'étudier la portée des logiciels malveillants (maliciels) et leur impact économique.

5.2.4 Coopération économique pour l'Asie-Pacifique[1342]

La Coopération économique pour l'Asie-Pacifique (APEC) a identifié, parmi ses domaines d'activité clés, la cybercriminalité, et les dirigeants de l'APEC se sont exprimés en faveur d'une coopération plus étroite des agents impliqués dans la lutte contre la cybercriminalité[1343]. La déclaration de la réunion des ministres des Télécommunications et de l'information de l'APEC de 2008 à Bangkok, Thaïlande, a souligné l'importance d'une collaboration permanente pour lutter contre la cybercriminalité.[1344] À ce jour, l'APEC n'a proposé aucun cadre juridique sur la cybercriminalité, mais s'est référée à des normes internationales comme la Convention de Budapest sur la cybercriminalité. En outre, l'APEC a soigneusement étudié la législation nationale de divers pays en matière de cybercriminalité[1345] dans le cadre d'un sondage sur la législation dans ce domaine, et a développé une base de données sur les différentes approches permettant d'aider les états à élaborer et modifier une législation.[1346] Le questionnaire utilisé était basé sur le cadre juridique proposé par la Convention de Budapest sur la cybercriminalité.

Déclaration sur la lutte contre le terrorisme (2002)

En 2002, les dirigeants de la Coopération économique pour l'Asie-Pacifique (APEC) ont publié une « déclaration sur la lutte contre le terrorisme et la promotion de la croissance » (*Statement on Fighting Terrorism and Promoting Growth*) dans le but d'adopter des législations globales en matière de cybercriminalité et de renforcer les capacités nationales d'enquête sur les cyberdélits[1347]. Ils se sont engagés à faire tout leur possible pour adopter un ensemble complet de lois en matière de cybersécurité et de cybercriminalité, qui soient conformes aux dispositions figurant dans des instruments législatifs internationaux, notamment la Résolution 55/63 (2000) de l'Assemblée générale des Nations Unies et la Convention du Conseil de l'Europe sur la cybercriminalité (2001), et ce, d'ici octobre 2003. En outre, ils se sont engagés à identifier des unités nationales de lutte contre la cybercriminalité et des points de contact internationaux pouvant offrir une assistance dans le domaine de la haute technologie, et mettre en place ces moyens dans la mesure où ils n'existent pas déjà, et ce, d'ici octobre 2003, et à mettre en place des organes qui évaluent la menace et la vulnérabilité, et échangent leurs informations (tels que des équipes d'interventions en cas d'urgence informatique) d'ici octobre 2003.

Conférence sur la législation en matière de cybercriminalité (2005)

L'APEC a organisé diverses conférences[1348] et a appelé à une coopération plus étroite entre les agents impliqués dans la lutte contre la cybercriminalité.[1349] En 2005, l'APEC a organisé une conférence sur la législation en matière de cybercriminalité. [1350] Les objectifs principaux de la conférence étaient de promouvoir le développement de cadres juridiques exhaustifs pour combattre la cybercriminalité et promouvoir la cybersécurité; assister les autorités de répression pour répondre aux questions cruciales et aux défis posés par les avancées technologiques; promouvoir la coopération entre les enquêteurs chargés de la cybercriminalité dans la région.

Groupe de travail télécommunications et information

Le groupe de travail Télécommunications et information de l'APEC[1351] a participé activement à l'élaboration des approches adoptées par l'APEC pour renforcer la cybersécurité.[1352] En 2002, il adoptait la Stratégie cybercriminalité de l'APEC.[1353] Le groupe de travail exprimait sa position concernant la législation en matière de cybercriminalité en se référant aux approches internationales existantes des Nations Unies et du Conseil de l'Europe.[1354] Les diverses expériences en matière d'élaboration de législation relative à la

cybercriminalité ont été débattues au sein du groupe chargé de la sécurité numérique du groupe de travail Télécommunications et Information lors de deux conférences organisées[1355] en Thaïlande en 2003.[1356]

5.2.5 Commonwealth

La cybercriminalité fait partie des sujets traités par le Commonwealth. Ses activités sont centrées en particulier sur l'harmonisation des législations. Cette approche de l'harmonisation juridique au sein du Commonwealth et de promotion de la coopération internationale a été influencée, entre autres, par le fait que, en l'absence d'une telle approche, il faudrait conclure pas moins de 1272 traités bilatéraux au sein du Commonwealth pour traiter de la coopération internationale dans ce domaine.[1357]

Conscients de l'augmentation de la cybercriminalité, les ministres de la Justice du Commonwealth ont décidé de mandater un groupe d'experts pour élaborer un cadre juridique de lutte contre ce fléau reposant sur la Convention du Conseil de l'Europe sur la cybercriminalité[1358]. Le groupe d'experts a présenté son rapport et ses recommandations en mars 2002[1359]. Le projet de loi type sur la criminalité informatique et en relation avec l'ordinateur (*Draft Model Law on Computer and Computer Related Crime*) a été présenté la même année[1360]. La loi type est conforme aux normes définies par la Convention sur la cybercriminalité, car elle contient des instructions précises et repose sur la reconnaissance de la convention par le groupe d'experts en tant que norme internationale. Cependant, il demeure certaines différences qui seront présentées en détail au chapitre 6.

Lors de la réunion de 2000, les ministres de la Justice et les procureurs généraux des petites juridictions du Commonwealth ont décidé de créer un groupe d'experts pour élaborer un modèle de loi sur la preuve numérique. Le modèle de loi a été présenté en 2002.[1361]

En plus de proposer un cadre juridique, le Commonwealth organisé plusieurs sessions de formation. Le Réseau de TI et de développement du Commonwealth (COMNET-IT) a coorganisé la formation sur la cybercriminalité en 2007.

En 2009, le Programme de formation du Commonwealth destiné aux pays tiers sur le cadre juridique pour les TIC s'est déroulé à Malte, avec le soutien du Fonds de coopération technique du Commonwealth (CFTC). Une autre session de formation a été organisée en 2011.

En 2011 le Commonwealth a présenté « L'initiative du Commonwealth en matière de cybercriminalité ». Le principal objectif de cette initiative est d'aider les pays du Commonwealth à bâtir leurs capacités institutionnelles, humaines et techniques en matière de politique, de législation, de réglementation, d'enquête et de répression.[1362] Elle vise à permettre à tous les pays du Commonwealth de coopérer efficacement dans le cadre de la lutte mondiale contre la cybercriminalité.

5.2.6 Union africaine

Pendant la conférence extraordinaire des ministres de l'Union africaine chargés des technologies de l'information et de la communication, qui s'est tenue à Johannesburg en 2009, les ministres ont abordé différents sujets ayant trait à l'intensification de l'utilisation des TIC dans les pays africains. Il a été décidé que la Commission de l'Union africaine devait — conjointement avec la Commission économique des Nations Unies pour l'Afrique — élaborer un cadre juridique traitant de sujets comme les transactions électroniques, la cybersécurité et la protection des données, pour les pays africains.[1363]

En 2011, l'Union africaine a présenté le projet de Convention de l'Union africaine sur la mise en place d'un cadre juridique de confiance pour la cybersécurité en Afrique.[1364] L'intention des rédacteurs est de renforcer la législation existante dans les États membres concernant les technologies de l'information et de la communication. Concernant son mandat, celui-ci n'était pas limité à la cybercriminalité, mais incluait également d'autres problèmes liés à la société de l'information comme la protection des données et les transactions électroniques — La Convention est à cet égard bien plus exhaustive que la plupart des autres approches régionales. Elle est articulée autour de quatre parties, dont la première concerne le commerce électronique. Elle aborde divers aspects tels que la responsabilité contractuelle du fournisseur électronique de biens et de services[1365], les obligations du contrat sous forme électronique[1366] et la sécurité des transactions électroniques.[1367] La seconde partie traite des questions de protection des données.[1368] La

troisième partie a trait à la lutte contre la cybercriminalité. La section 1 contient cinq chapitres, qui comporte six définitions (communication électronique, données informatiques, racisme et xénophobie dans les TIC, mineur, pédopornographie et système informatique).[1369]

Article III – 1:
Au sens de la présente convention, les expressions ci-dessous sont définies comme suit:
1) Communication électronique: vise toute mise à disposition du public ou d'une catégorie de public, par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature;
2) Données informatisées: vise toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique;
3) Raciste et xénophobe en matière des TIC: vise tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconisent ou encouragent la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou incite à de tels actes;
4) Mineur: vise toute personne âgée de moins de 18 ans au sens de la convention des Nations Unies sur les droits de l'enfant;
5) Pornographie enfantine: vise toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite;
6) Système informatique: vise tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme.

En outre, la troisième partie traite de la nécessité d'une politique nationale en matière de cybersécurité et d'une stratégie correspondante.[1370] Le second chapitre aborde les questions générales ayant trait aux mesures juridiques, notamment les normes relatives aux autorités statutaires, aux principes démocratiques, à la protection des infrastructures d'information essentielles, à l'harmonisation, à la double incrimination et à la coopération internationale.[1371] Le troisième chapitre aborde les questions relatives au système de cybersécurité nationale. Cela englobe la culture de la sécurité, le rôle du gouvernement, les partenariats public-privé, l'éducation et la formation ainsi que la sensibilisation du public.[1372] Le quatrième chapitre est consacré aux structures de contrôle de la cybersécurité nationale. Le cinquième chapitre traite de la coopération internationale. La principale différence avec des cadres régionaux comparables tels que la Convention du Conseil de l'Europe sur la cybercriminalité est que le projet de Convention de l'Union africaine — lorsqu'aucun autre instrument de coopération internationale n'est mis en place — ne peut être utilisé à ces fins. La différence de conception est exprimée en particulier par l'article 21 et l'article 25.

Article III – 1 – 21: *Coopération internationale*
Chaque État membre devra adopter les mesures légales qu'il jugera nécessaires pour permettre des échanges d'informations ainsi que le partage des données rapides, expéditifs et réciproques par les organisations des États membres et par des organisations similaires d'autres États membres chargées de faire appliquer la loi sur le territoire sur une base bilatérale ou multilatérale.

Article III – 1 – 25: *Modèle de coopération internationale*
Chaque État membre devra adopter les mesures et les stratégies qui lui seront nécessaires pour prendre part à la coopération régionale et internationale en matière de cybersécurité. Les résolutions promouvant la participation des États membres dans ce cadre de relations ont été adoptées par un grand nombre d'organismes gouvernementaux internationaux comprenant notamment les Nations Unies, l'Union africaine, l'Union européenne et le groupe d'États du G8. Des organisations telles que l'Union internationale des télécommunications, le Conseil de l'Europe, le Commonwealth des Nations ont mis en place des cadres types pour la coopération internationale que l'État membre peut adopter à titre de guide.

La section II de la troisième partie est consacrée au droit pénal matériel. La section 1 inclut la criminalisation de l'accès illégal à un système informatique[1373], de la présence illégale dans un système informatique[1374], de l'atteinte à l'intégrité d'un système[1375], de la saisie illégale de données[1376], de l'interception illégale de données[1377] et de l'atteinte à l'intégrité des données.[1378] Ces dispositions présentent de nombreuses similitudes avec les bonnes pratiques adoptées dans d'autres régions — y compris des normes utilisées en Afrique. À titre d'exemple, on peut citer la criminalisation de la présence illégale dans un système informatique introduite par le projet de directive ECOWAS.[1379]

Article III – 3:
Chaque État membre de l'Union africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique.

L'obligation faite aux entreprises de soumettre leur produit à un test de vulnérabilité est un nouveau concept, qui n'est toutefois pas une disposition du droit pénal, mais une mesure accessoire, qui n'a pas été empruntée à d'autres cadres de référence régionaux.

Article III-7:
[...]
2) Les États membres devront adopter les règles qui imposent aux vendeurs de produits TIC de faire réaliser, par des experts et des chercheurs en sécurité informatique indépendants, un essai de vulnérabilité et une évaluation de la garantie de sécurité, et de divulguer aux consommateurs toutes les vulnérabilités décelées dans les produits ainsi que les solutions recommandées pour y remédier.

La section 2 inclut la criminalisation de certains aspects de la contrefaçon informatique[1380], de l'utilisation illégale de données[1381], de l'atteinte à l'intégrité d'un système avec l'intention d'en tirer un avantage[1382], des viols de protections de données[1383], des dispositifs illégaux[1384] et de la participation à une organisation criminelle.[1385]

Article III – 9:
Chaque État membre de l'Union africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait, en connaissance de cause, de faire usage des données obtenues.

En particulier, la criminalisation de l'utilisation illégale de données informatiques va au-delà des normes définies par la plupart des autres instruments régionaux.

La section 3 est consacrée à la criminalisation du contenu illégal. Le projet de Convention africaine introduit le principe de criminalisation de la production et de la diffusion de pédopornographie[1386], de l'achat et de l'importation de pédopornographie[1387], de la possession de pédopornographie[1388], de l'acte de faciliter l'accès à la pornographie aux mineurs[1389], de la diffusion de contenus à caractère raciste ou xénophobe[1390], des attaques racistes perpétrées en utilisant des systèmes informatiques[1391], des abus racistes commis en utilisant des systèmes informatiques[1392] et de la négation ou l'approbation des génocides ou crimes contre l'humanité.[1393]

La dernière section du chapitre 1 contient des dispositions qui traitent de façon large de la législation relative à la cybercriminalité et à l'admissibilité de la preuve électronique (« contenu électronique écrit »).

Article III – 23 – 1: *Lois contre la cybercriminalité*
Chaque État membre devra adopter les mesures législatives qu'il jugera efficaces en considérant comme infractions criminelles substantielles des actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes TIC et des infrastructures réseau sous-jacentes, ainsi que les mesures procédurales qu'il jugera efficaces pour rechercher et poursuivre les contrevenants. Les États membres sont invités à prendre en considération le choix du langage approuvé dans les modèles mondiaux de législations en matière de cybercriminalité tel que celui adopté par le Conseil de l'Europe et le Commonwealth des Nations s'il y a lieu.

***Article III – 23 – 2**:*
Chaque État membre de l'Union africaine doit prendre les mesures législatives nécessaires pour faire en sorte que l'écrit électronique en droit pénal soit admis à établir les infractions à la loi pénale sous réserve qu'il soit apporté au cours des débats et discuté devant le juge et que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Eu égard à l'article III-23-1 en particulier, l'intention des rédacteurs n'est pas totalement claire puisque les délits mentionnés dans les paragraphes précédents du chapitre 1 sont définis comme des délits portant atteinte à l'intégrité et à la disponibilité des systèmes informatiques. La question de savoir dans quelle mesure l'article III-23-1 – eu égard à la criminalisation — impose aux pays d'aller au-delà des délits déjà définis plus en détail par le projet de Convention africaine demeure incertaine.

Le second chapitre contient des dispositions visant à actualiser les dispositions traditionnelles pour garantir leur applicabilité s'agissant de l'implication de systèmes informatiques et de données. Cela impose aux pays de définir une aggravation des peines lorsque des délits traditionnels sont commis en utilisant des technologies de l'information et de la communication[1394], de criminaliser la violation de propriété par des infractions telles que le vol, l'abus de confiance ou le chantage impliquant l'utilisation de données informatiques[1395], d'adopter des dispositions qui incluent les moyens de diffusion en masse pour garantir que l'utilisation de moyens de communication électronique numériques soit couverte[1396] et veiller à ce que des dispositions visant à protéger le secret dans l'intérêt de la sécurité nationale soient applicables concernant les données informatiques.[1397] Ces dispositions sont absentes des autres cadres régionaux. Eu égard à l'article III-24, la raison pour laquelle le simple fait qu'un système informatique ait été utilisé à un moment donné pour commettre une infraction traditionnelle (par exemple lorsque les délinquants expédient un courriel avant de braquer une banque au lieu de passer un appel téléphonique) puisse entraîner une peine aggravée, demeure incertaine.

Article III – 24:
Chaque État membre de l'Union africaine doit prendre les mesures législatives nécessaires en vue d'ériger en circonstance aggravante l'utilisation des TIC en vue de commettre des infractions de droit commun, comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le terrorisme, le blanchiment de capitaux notamment.

Articles III-28 à III-35: ces articles sont consacrés à la responsabilité et aux sanctions.

La section III traite du droit procédural. Elle demande aux États membres de mettre en oeuvre la conservation des données informatiques[1398], la saisie des données informatiques[1399], la préservation et l'interception rapide[1400] de communication de données.[1401] L'adoption de la Convention a été reportée à plusieurs reprises. Toutefois le 27 juin 2014, la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles a été adoptée adoptée.[1402]

5.2.7 Ligue des États arabes et Conseil de coopération du Golfe [1403]

Plusieurs États de la région arabe ont déjà pris des mesures nationales et adopté une stratégie de lutte contre la cybercriminalité, ou s'emploient actuellement à élaborer une législation en la matière[1404]. C'est notamment le cas du Pakistan,[1405] de l'Égypte[1406] et des Émirats Arabes Unis (EAU).[1407] En vue d'harmoniser la législation dans la région, les E.A.U. ont soumis à la Ligue des États arabes une loi type (Loi d'orientation pour lutter contre la cybercriminalité).[1408] En 2003, Le Conseil des ministres de l'Intérieur des États arabes et le Conseil des ministres de la Justice des États arabes ont adopté cette loi.[1409] Lors d'une conférence en 2007, le Conseil de coopération du Golfe (CCG) [1410] a recommandé à ses États membres d'adopter une démarche conjointe qui prenne en considération les normes internationales[1411].

5.2.8 Organisation des Etats américains [1412]

Depuis 1999, l'Organisation des États américains (OEA) s'emploie activement à résoudre la question de la cybercriminalité dans la région. L'organisation a notamment tenu plusieurs réunions dans le cadre du mandat des ministres de la Justice ou ministres ou procureurs généraux des Amériques (REMJA)[1413].

Groupe d'experts intergouvernemental sur la cybercriminalité

En 1999, le REMJA a recommandé la création d'un groupe d'experts intergouvernemental sur la cybercriminalité. Le groupe d'experts était chargé de dresser un état des lieux des activités criminelles qui visent les ordinateurs et les données informatiques ou qui consistent à utiliser des ordinateurs pour commettre une infraction; de dresser un état des lieux des législations, politiques et pratiques nationales concernant ces activités; de recenser les entités nationales et internationales spécialisées en la matière; et enfin de recenser les mécanismes de coopération du système interaméricain dans la lutte contre la cybercriminalité.

Recommandations des ministres de la Justice

En 2010, le REMJA s'était réuni à huit reprises.[1414] Lors de leur troisième réunion, en 2000, les ministres de la Justice ou ministres ou procureurs généraux des Amériques se sont penchés sur la question de la cybercriminalité et ont adopté plusieurs recommandations [1415]. Ces recommandations prévoyaient de soutenir les recommandations faites par le groupe d'experts gouvernementaux à sa première réunion en tant que contribution du REMJA à l'élaboration de la stratégie interaméricaine de lutte contre les menaces qui pèsent sur la cybersécurité, stratégie mentionnée dans la Résolution AG/RES. 1939 /XXXIII-O/03 de l'Assemblée générale de l'OEA, et de demander au groupe, via son/sa président(e), de continuer de soutenir la préparation de cette stratégie. Le REMJA recommandait également de faire le point sur les mécanismes visant à promouvoir entre eux une coopération large et efficace en matière de lutte contre la cybercriminalité et d'envisager, le cas échéant, de renforcer les capacités techniques et juridiques afin de rejoindre le réseau 24/7 mis en place par le G8 pour soutenir les enquêtes sur les cyberdélits. Les États membres étaient également invités à évaluer l'opportunité de mettre en œuvre les principes contenus dans la Convention du Conseil de l'Europe sur la cybercriminalité (2001) et d'envisager la possibilité d'adhérer à cette convention. Outre les États-Unis et le Canada, qui ont signé la Convention sur la cybercriminalité en 2001, le Chili, le Costa Rica, la République dominicaine et le Mexique ont été entre temps invités par le Conseil de l'Europe à adhérer à cette Convention. Enfin, les recommandations invitaient les États membres de l'OEA à examiner et, le cas échéant, faire évoluer la structure et les missions des organes nationaux ou des agences de répression de façon à tenir compte du caractère évolutif de la cybercriminalité, notamment en dressant un état des lieux des rapports qui existent entre les organes de lutte contre la cybercriminalité et ceux qui fournissent une aide policière ou une entraide juridique traditionnelle.

Lors de leur quatrième réunion, les ministres de la Justice ou ministres ou procureurs généraux des Amériques ont recommandé aux États, en 2002, dans le cadre des activités du groupe de travail de l'OEA faisant suite aux recommandations du REMJA, de mandater de nouveau le groupe d'experts gouvernementaux [1416] sur la cybercriminalité pour assurer le suivi de la mise en œuvre des recommandations élaborées par ce groupe et adoptées à la REMJA-III, étudier la préparation de législations types et d'instruments juridiques interaméricains pertinents afin de renforcer la coopération panaméricaine dans la lutte contre la cybercriminalité, en envisageant l'élaboration de normes en matière de vie privée, de protection de l'information, de procédures et de prévention de la criminalité.

Lors de leur sixième réunion, les ministres de la Justice [1417] ont appelé à continuer de renforcer la coopération avec le Conseil de l'Europe de sorte que les États membres de l'OEA puissent envisager d'appliquer les principes de la Convention du Conseil de l'Europe sur la cybercriminalité[1418] et d'y adhérer, et d'adopter les mesures juridiques et autres nécessaires à sa mise en œuvre; de même, poursuivre les efforts visant à renforcer les mécanismes d'échange d'informations et de coopération avec d'autres organisations et institutions internationales dans le domaine de la cybercriminalité, notamment les Nations Unies, l'Union européenne, le Forum de coopération économique Asie-Pacifique, l'OCDE, le G8, le Commonwealth et Interpol, de sorte que les États membres de l'OEA puissent bénéficier des avancées accomplies dans ces enceintes. Par ailleurs, les États membres ont été priés de mettre en place des unités

spécialisées pour enquêter sur les cyberdélits et identifier les autorités qui feront office de points de contact en la matière et faciliteront l'échange d'informations et l'obtention de preuve. En outre, promouvoir la coopération, dans les initiatives de lutte contre la cybercriminalité, entre les pouvoirs publics, les fournisseurs d'accès à Internet et les autres entreprises du secteur privé qui fournissent des services de transmission de données.

Ces recommandations ont été réitérées à la réunion de 2008,[1419] au cours de laquelle il a de plus été noté que, compte tenu des recommandations adoptées par le groupe d'experts gouvernementaux et par le REMJA lors de ses précédentes réunions, les États envisagent d'appliquer les principes de la Convention du Conseil de l'Europe sur la cybercriminalité, d'adhérer à cette convention et d'adopter les mesures juridiques et autres nécessaires à sa mise en œuvre. De même, à cette fin, que les activités de coopération technique se poursuivent sous les auspices du Secrétariat général de l'OEA – via le Secrétariat pour les affaires juridiques – et du Conseil de l'Europe. De même, qu'il convient de poursuivre les efforts visant à renforcer l'échange d'informations et la coopération avec d'autres organisations et institutions internationales dans le domaine de la cybercriminalité, de sorte que les membres de l'OEA puissent bénéficier des avancées accomplies dans ces enceintes. Enfin, que les secrétariats du Comité interaméricain de lutte contre le terrorisme (CICTE) et de la Commission interaméricaine pour les télécommunications (CITEL) et le groupe de travail sur la cybercriminalité poursuivent leur coordination et leurs actions de coopération pour assurer la mise en œuvre de la Stratégie interaméricaine intégrée pour combattre les menaces à la cybersécurité adoptée par l'Assemblée générale de l'OEA via sa résolution AG/RES. 2004 (XXXIV-O/04).

En 2010, à l'occasion de sa huitième réunion, la REMJA a traité la question de la cybercriminalité.[1420] Ont été débattus brièvement l'importance de poursuivre la consolidation et l'actualisation du Portail interaméricain pour la coopération en matière de cybercriminalité au travers de la page Internet de l'OAS, et le renforcement de la capacité des États à élaborer une législation et des dispositifs procéduraux relatifs à la cybercriminalité et à la preuve électronique. En outre, les recommandations de la réunion soulignaient le désir de renforcer les mécanismes permettant l'échange d'informations et la coopération avec d'autres organisations et agences internationales dans le domaine de la cybercriminalité, tels que le Conseil de l'Europe, les Nations Unies, l'UE, l'APEC, l'OCDE, le G8, le Commonwealth et Interpol, ainsi les états membres de l'OAS pourront tirer parti des avancées réalisées par ces entités.

Lors de la réunion de 2012, les Ministres de la justice ont de nouveau examiné plusieurs aspects de la cybercriminalité. [1421] Les participants ont compris l'importance des unités de cybercriminalité spécialisées.[1422] Ils ont en outre prié les Etats membres de procéder à un examen de leur système juridique et d'adopter la législation nécessaire pour ce qui est du droit procédural, des preuves électroniques et des procès au pénal. [1423] Ils ont aussi recommandé que soit adoptée une stratégie en matière de cybersécurité prévoyant des mesures de lutte contre la cybercriminalité. On comptait parmi les autres questions abordées l'éducation des citoyens et la reconnaissance des résultats obtenus par le Congrès des Nations Unies pour la prévention du crime et la justice pénale. Contrairement aux années précédentes, il n'est pas demandé dans les recommandations que soit ratifiée la Convention sur la cybercriminalité ; un libellé plus souple est utilisé et il est ainsi demandé aux Etats Membres "de rendre hommage aux États membres de l'OEA qui ont envisagé d'appliquer les principes contenus dans la Convention sur la cybercriminalité du Conseil de l'Europe et d'y adhérer…".[1424]

A la réunion de 2014[1425], les participants ont adopté des recommandations s'apparentant grandement à celles issues des réunions précédentes. Parmi les nouveaux points, il a été annoncé que l'élaboration d'une législation type était prise en considération.[1426]

5.2.9 Caraïbes

En décembre 2008, l'UIT et l'UE ont lancé le projet « Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures » (Projet « HIPCAR » — Amélioration de la compétitivité dans les Caraïbes au travers de l'harmonisation des politiques, législations et procédures réglementaires en matière de TIC) pour promouvoir le secteur des TIC dans la région Caraïbe.[1427] Le projet fait partie du programme « ACP-Technologies de l'information et la communication » et du neuvième Fonds européen de développement. Les pays bénéficiaires sont 15 pays des Caraïbes.[1428]

L'objectif du projet est d'aider les pays du CARIFORUM[1429] à harmoniser leurs politiques et leurs cadres juridiques dans le domaine des TIC.

Dans le cadre de ce projet, neuf domaines de travail ont été identifiés[1430] dans lesquels des modèles de politique et de textes législatifs ont été élaborés pour faciliter le développement et l'harmonisation des législations dans la région. La cybercriminalité était l'un de ses neuf domaines de travail. L'élaboration du modèle de textes législatifs s'est déroulée en trois phases. Dans la première phase, la législation existante dans les pays bénéficiaires a été réunie et examinée. Parallèlement, les bonnes pratiques régionales et internationales ont été identifiées. La priorité a été donnée aux normes directement applicables dans au moins certains des pays bénéficiaires (par exemple le Modèle de loi du Commonwealth de 2002). Cependant, l'examen incluait également les bonnes pratiques issues d'autres régions, comme l'Union européenne et l'Afrique. Le rapport d'évaluation[1431] proposait un aperçu des législations existantes, ainsi qu'une analyse juridique comparative de la législation existante par rapport aux bonnes pratiques régionales et internationales. Afin de préparer une analyse des écarts, le rapport d'évaluation identifiait par ailleurs les besoins spécifiques de la région (par exemple en matière de législation sur le spam) qui ne sont pas nécessairement pris en compte par les bonnes pratiques internationales. Lors d'un atelier organisé en 2010, le rapport d'évaluation a fait l'objet d'un débat avec les parties prenantes des pays bénéficiaires.[1432] Sur la base du rapport d'évaluation et de l'analyse des écarts, les parties prenantes ont rédigé un modèle d'orientations de politiques.

Dans la seconde phase, un modèle de texte législatif prenant en compte les orientations de politiques a été rédigé. Lors d'un second atelier, des experts en politique, des rédacteurs juridiques et d'autres acteurs des pays bénéficiaires ont débattu et amendé le projet de modèle de texte législatif préparé pour la réunion. Le modèle de texte législatif visait trois objectifs principaux: fournir un langage spécifique conforme aux bonnes pratiques internationales, refléter les demandes spéciales de la région et prendre en compte les pratiques rédactionnelles de la région dans le domaine juridique, afin de garantir une mise en oeuvre sans heurts. Le modèle de texte législatif comporte un éventail de définitions complexes, et des dispositions de droit pénal matériel, y compris des dispositions ayant trait à des questions comme le spam qui font l'objet d'un niveau de priorité élevé pour la région, mais ne sont pas nécessairement intégrées à des cadres de référence régionaux tels que la Convention du Conseil de l'Europe sur la cybercriminalité.

15. (1) Une personne qui, intentionnellement, sans excuse légitime ou justification:
a) lance intentionnellement la transmission de messages de courrier électronique multiples depuis ou par le biais d'un système informatique; ou
b) utilise un système informatique protégé pour relayer ou retransmettre des messages de courrier électronique multiples, avec l'intention de tromper ou d'induire en erreur les utilisateurs, ou tout fournisseur de courrier électronique ou fournisseur de services Internet, quant à l'origine de ces messages; ou
c) falsifie matériellement des informations d'en-tête dans de multiples messages de courrier électronique et lance intentionnellement la transmission de ces messages, commet une infraction punissable, sur déclaration de culpabilité, d'une peine d'emprisonnement pour une période ne dépassant pas [période], ou d'une amende ne dépassant pas [montant], ou les deux.
(2) Un pays peut limiter la criminalisation à l'égard de la transmission de messages électroniques multiples dans le cadre des relations clients ou d'affaires. Un pays peut décider de ne pas criminaliser les actes décrits au point 15 (1) (a) sous réserve que d'autres recours efficaces existent.

Par ailleurs, le texte contient des dispositions de droit procédural (y compris des instruments d'enquête sophistiqués tels que l'utilisation d'outils de criminalistique contrôlables à distance) et des dispositions sur la responsabilité des fournisseurs d'accès Internet (FAI).

5.2.10 Pacifique

Parallèlement au projet cofinancé par l'UIT et l'UE dans les Caraïbes, les mêmes organisations ont lancé un projet dans la région pacifique (le projet ICB4PAC).[1433] Le projet vise — sur la base d'une demande formulée par les pays insulaires du Pacifique — à offrir un renforcement des capacités en matière de politiques et de réglementations dans le domaine des TIC. À cet égard, sa priorité est de bâtir les moyens humains et

institutionnels dans le domaine des TIC grâce à la formation, l'éducation et des dispositifs de partage des connaissances. 15 États insulaires du Pacifique sont les bénéficiaires de ce projet.[1434] En mars 2011, un atelier sur l'état de la législation actuelle en matière de cybercriminalité dans la région Pacifique s'est déroulé en république du Vanuatu.[1435] Au cours de l'atelier, une analyse juridique comparée exhaustive fournissant une vue d'ensemble de la législation existante dans la région ainsi qu'une comparaison avec les bonnes pratiques d'autres régions a été proposée.[1436] Pour faire suite à cet atelier, une conférence sur les techniques d'élaboration de politiques et de législation en matière de cybercriminalité a été organisée en août 2011 à Samoa.[1437] Pendant cette conférence, les bonnes pratiques d'autres régions ont été présentées et les structures nécessaires pour élaborer une politique et une législation harmonisée en la matière ont été étudiées en détail. Étaient abordés les aspects du droit pénal matériel, du droit procédural, de la coopération internationale, de la responsabilité des fournisseurs d'accès Internet (FAI), de la preuve électronique et des dispositifs de prévention de la criminalité.

En avril 2011, le Secrétariat de la Communauté du Pacifique a organisé une conférence sur la lutte contre la cybercriminalité dans la région Pacifique.[1438] Cet évènement était coorganisé par le Conseil de l'Europe. Pendant la conférence, les aspects ayant trait au droit pénal matériel, au droit procédural et à la coopération internationale ont été abordés.[1439]

5.2.11 Communauté de développement de l'Afrique australe (SADC)

La Communauté de développement de l'Afrique australe (SADC) a adopté une législation type dont l'approche est similaire à celle de l'Union africaine. Elle traite des questions de la protection des données[1440], du commerce électronique[1441] et de la cybercriminalité. [1442]

5.3 Approches scientifiques et indépendantes

5.3.1 Projet de convention internationale de Stanford

Le Projet de convention internationale de Stanford (le « Projet Stanford ») est un exemple bien connu d'approche scientifique de l'élaboration d'un cadre juridique relatif à la cybercriminalité au plan mondial.[1443] Le Projet Stanford a été élaboré comme un prolongement de la conférence organisée par l'Université de Stanford aux États-Unis en 1999.[1444] La comparaison avec la Convention du Conseil de l'Europe sur la cybercriminalité[1445] permet de mettre en évidence un certain nombre de similitudes. Les deux textes couvrent certains aspects du droit pénal matériel, du droit procédural et de la coopération internationale. La principale différence réside dans le fait que les infractions et les instruments de procédure développés par le Projet Stanford ne sont applicables que dans le cadre d'attaques contre les infrastructures d'information et d'attaques terroristes, alors que les instruments relatifs au droit procédural et à la coopération internationale mentionnés dans la Convention du Conseil de l'Europe sur la cybercriminalité peuvent être aussi appliqués aux infractions conventionnelles.[1446]

5.3.2 Protocole mondial sur la cybersécurité et la cybercriminalité

Pendant le Forum sur la gouvernance de l'Internet qui s'est tenu en Égypte en 2009, *Scholberg* et *Ghernaouti-Helie* ont présenté une proposition de Protocole mondial sur la cybersécurité et la cybercriminalité.[1447] Les articles 1 à 5 ont trait à la cybercriminalité et recommandent la mise en oeuvre de dispositions de droit pénal matériel, de dispositions de droit procédural, de mesures contre l'utilisation d'Internet à des fins terroristes, de mesures de coopération mondiale et d'échange d'informations et de mesures sur la vie privée et les droits de l'homme.[1448] La législation type annexée au protocole est, dans une large mesure (articles 1-25), basée sur la formulation retenue pour les dispositions de la Convention du Conseil de l'Europe sur la cybercriminalité.

En juin 2014, M. Scholberg a présenté la 9ème édition d'un projet de traité des Nations Unies sur une cour ou un tribunal international pour le cyberespace.[1449] Dans ce document à l'approche scientifique, qui ne repose sur aucune mission officielle des Nations Unies, l'auteur met en exergue les problèmes liés à la question de la compétence dans le cyberespace et développe le concept d'une cour internationale disposant de compétences limitées, comparable à la Cour permanente de Justice internationale.

5.4 Relations entre différentes approches législatives internationales

Étant donné la reconnaissance dont jouissent certaines normes concernant des protocoles techniques, la question de savoir comment éviter les incompatibilités entre différentes approches internationales[1450] se pose. La Convention du Conseil de l'Europe sur la cybercriminalité et la Loi type du Commonwealth sur la cybercriminalité sont aujourd'hui les cadres adoptant l'approche la plus exhaustive, car ils couvrent le droit pénal substantiel, le droit procédural et la coopération internationale. Mais aucun de ces instruments n'a été modifié pour prendre en compte les développements intervenus ces dernières années. En outre, la portée de ces deux instruments est limitée. Le débat lors du dernier Congrès des Nations-Unies sur la criminalité a souligné l'intérêt des instruments internationaux pour les pays[1451]. Cela soulève des questions eu égard à la relation entre les approches régionales existantes et la possibilité d'une action à l'échelle internationale. Trois scénarios sont possibles.

Si une nouvelle approche juridique définit des normes qui ne sont pas conformes aux approches existantes correspondantes au plan régional et national, cela pourrait, au moins dans un premier temps, avoir un impact négatif sur le processus d'harmonisation nécessaire. Il est donc souhaitable que toute nouvelle approche analyse soigneusement les normes existantes pour garantir une certaine cohérence. La criminalisation de l'accès illégal, qui est défini d'une manière similaire dans la section 5 du Modèle de loi du Commonwealth sur la cybercriminalité et à l'article 2 de la Convention du Conseil de l'Europe sur la cybercriminalité, en est un exemple.

En outre, une nouvelle approche pourra veiller à éviter d'inclure des dispositions ayant déjà posé problème lors de leur mise en oeuvre, voire même ayant freiné certains pays dans leur démarche pour adhérer à un texte. La règlementation controversée reprise à l'article 32b de la Convention du Conseil de l'Europe sur la cybercriminalité en est un exemple. Cette disposition a été critiquée par la délégation russe lors de la réunion de 2007 du Comité sur la cybercriminalité.[1452]

Enfin, une nouvelle approche internationale peut — en plus d'inclure les normes de base similaires dans différentes approches juridiques — s'attacher à analyser les écarts afin d'identifier les domaines qui ne sont pas suffisamment traités, et ainsi criminaliser certains actes apparentés à la cybercriminalité et définir des instruments procéduraux qui ne sont pas encore couverts par les textes existants. Depuis 2001, un certain nombre d'avancées importantes ont été réalisées. Lorsque la Convention du Conseil de l'Europe sur la cybercriminalité a été rédigée, l'« hameçonnage », le « vol d'identité »,[1453] [1454] et les infractions liées au jeu en ligne et aux réseaux sociaux n'étaient pas d'actualité au point où ils le sont aujourd'hui. Une nouvelle approche internationale pourrait poursuivre le processus d'harmonisation en incluant d'autres infractions revêtant une dimension internationale.[1455]

5.5 Relations entre différentes approches législatives nationales et internationales

Comme cela a été mentionné précédemment, la cybercriminalité est un fléau véritablement transnational[1456]. Les cyberdélinquants peuvent, en général, cibler des utilisateurs dans n'importe quel pays du monde, il est donc essentiel que, dans les affaires relevant de la cybercriminalité internationale, les enquêteurs puissent compter sur la coopération internationale des services de répression,[1457] coopération qui est tributaire de l'harmonisation des législations. En raison du principe répandu de double incrimination[1458], une coopération efficace suppose tout d'abord l'harmonisation des dispositions de fond en droit pénal afin qu'il n'existe pas de refuges pour criminels.[1459] En outre, il est nécessaire d'harmoniser les mécanismes d'enquête de sorte que tous les pays concernés par une enquête internationale aient mis en place les mécanismes nécessaires à la conduite des enquêtes. Enfin, une coopération efficace des services de répression suppose des procédures pratiques efficaces[1460]. L'harmonisation des législations doit donc être le résultat d'une volonté et d'un processus participatif, principe souhaitable sinon nécessaire de toute stratégie nationale de lutte contre la cybercriminalité.

5.5.1 Raisons de la popularité des approches nationales

Bien que beaucoup reconnaissent l'importance de l'harmonisation, le processus de mise en œuvre de normes juridiques internationales est loin d'être terminé[1461]. Les approches nationales tiennent une place

importante dans la lutte contre la cybercriminalité, ce qui tient notamment au fait que les infractions n'ont pas partout le même effet. Les démarches adoptées pour lutter contre le spam en sont une bonne illustration[1462]. Les courriels de spam nuisent en effet tout particulièrement aux pays en développement, question qui a fait l'objet d'un rapport de l'OCDE[1463]. Ce rapport montre que le spam est un problème beaucoup plus grave dans les pays en développement que dans les pays occidentaux, car les ressources y sont plus limitées et plus coûteuses[1464]. Le nombre important des initiatives législatives nationales s'explique principalement par le fait que la cybercriminalité a de multiples conséquences selon les pays et chaque État possède déjà des structures et des traditions juridiques. Pour l'essentiel, ces initiatives nationales ne visent donc pas à la mise en œuvre de normes internationales.

5.5.2 Solutions nationales contre solutions internationales

À l'heure de la mondialisation technique, où quiconque souhaitant se connecter à Internet doit utiliser les protocoles standard (techniques) en place[1465], cette problématique peut sembler quelque peu surprenante. L'unicité des normes est, de fait, une condition essentielle au bon fonctionnement des réseaux. Cela étant, contrairement aux normes techniques, les normes juridiques diffèrent toujours selon les pays[1466]. Or, étant donné la dimension internationale de la cybercriminalité, on peut s'interroger sur la viabilité des approches nationales[1467]. La question se pose pour toutes les approches nationales et régionales mettant en œuvre une législation qui n'est pas conforme avec les normes internationales en vigueur. Étant donné qu'un manque d'harmonisation peut constituer un obstacle sérieux aux enquêtes internationales, il serait souhaitable que les approches nationales et régionales aillent au-delà des normes préconisées par les instruments internationaux[1468].

Deux raisons majeures expliquent le nombre croissant des approches régionales et nationales. La première tient à la lenteur des processus législatifs. Le Conseil de l'Europe ne peut pas forcer un de ses États membres à signer la Convention sur la cybercriminalité; de même ne peut-il pas forcer un État signataire à ratifier la convention. Le processus d'harmonisation est donc souvent jugé lent par rapport aux approches législatives nationales et régionales[1469]. Contrairement au Conseil de l'Europe, l'Union européenne a les moyens d'obliger ses États membres à mettre en œuvre les décisions-cadres et les directives-cadres. S'explique ainsi pourquoi plusieurs pays de l'Union européenne, qui ont signé la Convention sur la cybercriminalité (2001), mais ne l'ont pas encore ratifiée, ont cependant mis en œuvre la décision-cadre du Conseil de l'UE relative aux attaques visant les systèmes d'information (2005).

La seconde raison tient à des différences d'ordre national et régional. Au sein d'une même région, certaines infractions ne sont sanctionnées que dans certains pays. C'est notamment le cas des infractions à motivation religieuse[1470]. Alors qu'il est peu probable de parvenir à harmoniser au plan international les dispositions pénales relatives aux infractions contre les symboles religieux, une approche nationale en la matière permet de garantir que les normes juridiques du pays concerné sont maintenues.

5.5.3 Difficultés posées par les approches nationales

Les approches nationales présentent plusieurs difficultés. Certes, en ce qui concerne les infractions traditionnelles, les pays qui choisissent de sanctionner certains actes influent sur la capacité des délinquants à agir sur leur territoire. Mais, dans le cas des cyberdélits, la capacité d'un seul pays à influer sur le comportement des délinquants est beaucoup plus limitée, car ces derniers peuvent, en général, agir de l'extérieur du pays en se connectant au réseau[1471]. Ainsi, si le délinquant opère à partir d'un pays où l'acte en question n'est pas sanctionné, les enquêtes internationales et les demandes d'extradition échouent la plupart du temps. L'un des objectifs clés des approches juridiques internationales est donc d'empêcher la création de refuges pour cyberdélinquants en proposant et en appliquant des normes internationales[1472]. Pour être efficaces, les approches nationales doivent donc en général s'accompagner de mesures additionnelles[1473]. Les plus courantes sont la pénalisation de l'utilisateur de contenu illicite en plus du fournisseur, et la pénalisation des services utilisés dans la commission d'un délit.

La pénalisation de l'utilisateur de contenu illicite en plus du fournisseur

Une approche consiste à pénaliser l'utilisation de services illicites en plus de la seule pénalisation de la fourniture de ces services. La pénalisation des utilisateurs qui se trouvent à l'intérieur de la juridiction est une façon de compenser le manque d'influence sur les fournisseurs de services installés à l'étranger.

La pénalisation des services utilisés dans la commission d'un délit

Une seconde approche consiste à réglementer, voire à pénaliser, la fourniture, à l'intérieur de la juridiction, de certains services utilisés à des fins criminelles. Cette solution est plus ambitieuse que la première, car elle s'applique aux entreprises et organisations offrant des services neutres, qui sont utilisés pour des activités licites ou illicites. L'*Unlawful Internet Gambling Enforcement Act*, la loi d'application relative aux jeux illicites sur Internet, adoptée en 2006 aux États-Unis, est un exemple d'une telle approche[1474].

Autre mesure étroitement liée à la précédente, la mise en place d'obligations de filtrage de certains contenus en ligne[1475]. Cette approche, qui a fait l'objet de débats à l'occasion de la célèbre affaire Yahoo![1476], est actuellement examinée en Israël, où il est envisagé d'obliger les fournisseurs d'accès à limiter l'accès à certains sites proposant des contenus pour adultes. Les tentatives de contrôle du contenu en ligne ne se limitent d'ailleurs pas aux contenus pour adultes: certains pays utilisent les technologies de filtrage pour limiter l'accès aux sites traitant de sujets politiques. L'OpenNet Initiative[1477] recense une vingtaine de pays environ pratiquant la censure[1478].

[1047] This includes regional approaches.

[1048] The Group of Eight (G8) consisted of eight countries: Canada, France, Germany, Italy, Japan, United Kingdom, United States and the Russian Federation. The presidency of the group, which represents more than 60 per cent of the world economy (source: http://undp.org), rotates every year. In 2014 Russia was excluded and the group meets as G7.

[1049] The idea of the creation of five subgroups – among them, one on high-tech crimes – was to improve implementation of the 40 recommendations adopted by G8 Heads of State in 1996.

[1050] The establishment of the subgroup (also described as the subgroup to the "Lyon Group") continued the efforts of the G8 (at that time still G7) in the fight against organized crime, which started with the launch of the Senior Experts Group on Organized Crimes (the "Lyon Group") in 1995. At the Halifax summit in 1995, the G8 stated: "We recognize that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from drug trafficking and other serious crimes. To implement our commitments in the fight against transnational organized crime, we have established a group of senior experts with a temporary mandate to look at existing arrangements for cooperation both bilateral and multilateral, to identify significant gaps and options for improved coordination and to propose practical action to fill such gaps". See: Chairman's Statement, Halifax G7 Summit, June 17 1995. For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1051] Regarding the G8 activities in the fight against cybercrime, see also: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1052] "Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October 1999.

[1053] 14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in

consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes – including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions – so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.

[1054] The idea of a 24/7 network has been picked up by a number of international approaches in the fight against cybercrime. One example is Article 35 of the Convention on Cybercrime:

(1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) the preservation of data pursuant to Articles 29 and 30;

c) the collection of evidence, the provision of legal information, and locating of suspects. […]

[1055] *Jean-Pierre Chevenement*, the French Minister of the Interior, stated: "Now that the G8 has provided the impetus, it's vital that we formalize the new legal rules and procedures for cooperation in a legal instrument applying world-wide. For France, the negotiations under way in the Council of Europe on a Convention on Cyber-Crime are of fundamental importance for several reasons. The draft currently under discussion defines the offences which all States would have to recognize. It goes on to propose ways in which they could cooperate, taking up, for example, the idea of national contact points. It also proposes extradition procedures. In short, this agreement is an essential instrument, which France wants to see concluded within a reasonable period of time. The important thing about these negotiations is that the countries involved include some major countries outside the Council of Europe and that, once signed, this convention will be opened for signature by all States wishing to accede to it. The idea is in fact to get a convention which applies world-wide so that there can be no more "digital havens" or "Internet havens" in which anyone wanting to engage in shady activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must never lose sight of the fact that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate."

[1056] G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

[1057] The experts expressed their concerns regarding implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible"; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001.

[1058] G8 Justice and Home Affairs Communiqué, Washington DC, 11 May 2004.

[1059] G8 Justice and Home Affairs Communiqué Washington DC, 11 May 2004:10. "Continuing to Strengthen Domestic Laws: To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."

[1060] The participants expressed their intention to strengthen the instruments in the fight against cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of

high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors". See: www.g7.utoronto.ca/justice/justice2006.htm.

[1061] Regarding the topic of cyberterrorism, see above: § 2.9.1. In addition, see: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis,* Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeldt*, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

[1062] The summit declaration calls for measures in the fight against cyberterrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists". For more information, see: http://en.g8russia.ru/docs/17.html.

[1063] For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1064] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 6, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1065] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 7, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1066] G8 Summit 2010 Muskoka Declaration, 2010, available at: www.g7.utoronto.ca/summit/2010muskoka/communique.html.

[1067] See press release from 30.5.2011, available at: www.eg8forum.com/en/documents/news/Final_press_release_May_30th.pdf.

[1068] See G8 Declaration, Renewed Commitment for Freedom and Democracy, available at: www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html.

[1069] The United Nations (UN) is an international organization founded in 1945. It had 192 Member States in 2010.

[1070] A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.

[1071] A/RES/45/121, adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.

[1072] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at www.uncjin.org/Documents/EighthCongress.html.

[1073] See the preface to the Optional Protocol.

[1074] See Art. 2.

[1075] See especially the background paper: Crimes related to computer networks, A/CONF.187/10.

[1076] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1077] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 174, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1078] "The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks".

[1079] A/RES/55/63. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

[1080] A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

[1081] A/RES/57/239, on Creation of a global culture of cybersecurity; A/RES/58/199, on Creation of a global culture of cybersecurity and the protection of critical information infrastructure.

[1082] Measures to Combat Computer-related Crime, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, A/CONF.203/14.

[1083] Committee II Report, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19.

[1084] Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

[1085] 30(d): "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

[1086] Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

[1087] See in this context especially the background paper prepared by the secretariat.

[1088] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1089] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1090] „The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1091] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1092] *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

[1093] Regarding the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

[1094] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

[1095] Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[1096] Resolutions 55/63 and 56/121.

[1097] Resolutions 57/239 and 58/199.

[1098] Draft topics for consideration in a comprehensive study on the impact o fand response to cybercrime, 2010, UNODC, UNODC/CCPCJ/EG.4/2011/2.

[1099] Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive studay of the problem of cybercrime held in Vienna from 17 to 21 January 2011, UNODC/CCPCJ/EG.4/2011/3.

[1100] www.unodc.org/cybercrime-study/

[1101] UNODC Press Release (26.01.2012) available at: www.unodc.org/unodc/en/frontpage/2012/January/unodc-chief-announces-a-comprehensive-study-on-cybercrime.html

[1102] United Nations Commission on Crime Prevention and Criminal Justice.

[1103] www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[1104] Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, page X.

[1105] Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, S. XIX.

[1106] UNODC/CCPCJ/EG.4/2013/3.

[1107] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1108] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1109] Commission on Crime Prevention and Criminal Justice, Report on the twenty-thrid session (13 December 2013 and 12 to 16 May 2014), Economic and Social Council, Official Records,2014, Supplement No. 10

[1110] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1111] Development in the Field of Information and Telecommunications in the Context of International Security, 2013, available at: www.un.org/disarmament/topics/informationsecurity/

[1112] See: Development in the Field of Information and Telecommunications in the Context of International Security, 2013, page 1.

[1113] The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf.

[1114] Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

[1115] The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council.

[1116] CCPCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process in the development of the resolution and for an overview of different existing legal instruments, see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, see: www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

[1117] The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

[1118] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

[1119] For more information on the development process and the work of the intergovernmental expert group, see: Results of the second meeting of the Intergovernmental Expert Group to Prepare a study on Fraud and the Criminal Misuse and Falsification of Identity, Commission on Crime Prevention and Criminal Justice, 16th session, 2007, E/CN.15/2007/8, page 2.

[1120] ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

[1121] Regarding Internet-related ID-theft, see above: § 2.8.3, and below: § 6.2.16.

[1122] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.

[1123] ECOSOC Resolution 2004/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

[1124] Reports related to the activities of the working group are published. See: First meeting of the Core Group of Experts on Identity-Related Crime, Courmayeur Mont Blanc, Italy, 29-30 November 2007, available at: www.unodc.org/documents/organized-crime/Courmayeur_report.pdf (last visited: October 2008); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, available at: www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf (last visited: October 2008).

[1125] See for example: Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, 2009, E/CN.15/2009/CRP.13.

[1126] ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

[1127] For further information see: www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html.

[1128] The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. For more information, see: www.itu.int.

[1129] WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

[1130] WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

[1131] For more information on Action Line C5, see: http://www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, available at: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

[1132] For more information, see www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1133] www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1134] The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building, international cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1135] See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

[1136] www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; See: *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2009, Issue 7, page 533.

[1137] See, in this context: *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1, page 7 *et seq*.

[1138] Global Strategic Report, Chapter 1.6.

[1139] Global Strategic Report, Chapter 1.7.

[1140] Global Strategic Report, Chapter 1.10.

[1141] Global Strategic Report, Chapter 1.11.

[1142] 23-25 November 2009 (Santo Domingo, Dominican Republic): www.itu.int/ITU-D/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa; 15-18 July 2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP); 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP).

[1143] Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/

[1144] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

[1145] Information about the project are available at: www.itu.int/ITU-D/treg/projects/itu-ec/index.html

[1146] The adoption took place during the 3rd Ordinary General Assembly oft he West African Telecommunications Regulators Assembly.

[1147] www.itu.int/ITU-D/treg/projects/itu-ec/ECOWAS_MINISTERS_ADOPTS_GUIDELINES_FOR_TELECOMMUNICATION_MARKET_AT_ABUJA.pdf

[1148] http://news.ecowas.int/en/presseshow.php?nb=2&lang=en&annee=2007

[1149] Angla, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cap-Verde, Chad, Congo, Cote d'Ivoire, Eritrea, Gabon, Gambia, Ghana, Guinea, Guinea Equatorial, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Uganda, Central African Republic, Democratic Republic of Congo, Rwanda, Sao Tome-e-Principe, Senegal, Seychelles, Sierra Leone, South Africa, Swaziland, Tanzania, Togo, Zambia and Zimbabwe.

[1150] ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 5.

[1151] The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

[1152] CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

[1153] Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

[1154] Detailed information about requested support, activities and documents are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

[1155] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[1156] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

[1157] The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

[1158] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

[1159] The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD and UN. Source: *Nilsson* in *Sieber*, Information Technology Crime, page 577.

[1160] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf..

[1161] *Nilsson* in Sieber, Information Technology Crime, page 576.

[1162] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

[1163] Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

[1164] The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.

[1165] Decision CDPC/103/211196. CDPC explained its decision by pointing out the international dimension of computer crimes: "By connecting to communication and information services, users create a kind of common space, called

"cyber-space", which is used for legitimate purposes, but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."

[1166] Explanatory Report of the Convention on Cybercrime (185), No. 10.

[1167] The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

[1168] For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[1169] Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

[1170] Albania, Armenia, Australia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Malta, Mauritius, Moldova, Montenegro, Netherlands, Norway, Panama, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, United States.

[1171] The need for a ratification is laid down in Article 36 of the Convention on Cybercrime:

> *Article 36 – Signature and entry into force*
>
> *1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.*
>
> *2)This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.*

[1172] Australia, Dominican Republic, Mauritius and Philippines.

[1173] Argentina, Australia, Chile, Colombia, Costa Rica, Dominican Republic, Israel, Mauritius, Mecixo, Panama, Philippines, Senegal.

[1174] Argentina, Chile, Colombia, Costa Rica, Dominican Republic, Israel, Mexico, Morocco, Philippines, Senegal.

[1175] Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention on Cybercrime shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf; APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group,

Global Strategic Report, 2008, page 19, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[1176] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[1177] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention on Cybercrime."

[1178] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1179] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1180] See Art. 3 of the Fourth Draft Convention, PC-CY (98) Draft No. 4, 17.04.1998.

[1181] Albania, Andorra, Armenia, Austria, Belgium, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Spain, Sweden, Switzerland, South Africa, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine.

[1182] Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Finland, France, Germany, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine.

[1183] Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp. The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf.

[1184] For more information on the achievements and shortcomings see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

[1185] Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

[1186] Draft Electronic Crime Act 2006.

[1187] Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

[1188] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1189] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

[1190] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

[1191] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, page 18.

[1192] Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

[1193] Albania, Croatia,

[1194] Estonia, Hungary.

[1195] Lithuania, Romania, Slovenia, The former Yugoslav Republic of Macedonia.

[1196] Bulgaria, Cyprus, Denmark.

[1197] Armenia, Bosnia and Herzegovina, France, Netherlands, Norway, Ukraine, United States.

[1198] Finland, Iceland, Latvia.

[1199] Italy, Slovakia.

[1200] Germany, Moldova, Serbia.

[1201] Azerbaijan, Montenegro, Portugal, Spain.

[1202] United Kingdom, Switzerland.

[1203] Austria, Belgium, Georgia, Malta, Australia and Japan.

[1204] Czech Republic, Dominican Republic and Mauritius.

[1205] See Sec. 202a of the German Penal Code.

[1206] Country profiles can be downloaded at www.coe.int/cybercrime.

[1207] For details on the requirements, see: *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025, available at: www.fas.org/sgp/crs/misc/97-1025.pdf.

[1208] *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1209] See in this context, for example: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4,

[1210] See Art. 44 Convention on Cybercrime.

[1211] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1212] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1213] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1214] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1215] *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

[1216] Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1217] See *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009, page 127-150.

[1218] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007,

page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

[1219] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.8.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

[1220] Criticism about the lack of coverage of such topics in the existing instruments: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07, page 7.

[1221] See: Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, COM(2010) 517, page 6.

[1222] *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1223] See Art. 44 Convention on Cybercrime.

[1224] See Art. 37 Convention on Cybercrime.

[1225] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1226] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1227] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1228] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1229] See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[1230] See: Art. 41 Salvador Declaration on Comprehensive Strategies for Global Challenges, 2010. Available at: www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

[1231] See ITU Resolution 130 (Rev. Guadalajara, 2010).

[1232] San Marino did not even sign the Convention. Andorra, Monaco and Lichtenstein signed but never ratified the Convention.

[1233] See Explanatory Report to the Convention on Cybercrime, No. 298.

[1234] *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

[1235] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

[1236] ICB4PAC Workshop on Concepts and Techniques of Developing CyberCrime Policy and Legislation, Apia, Samoa 22-25 August 2011.

[1237] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, No. 47.

[1238] Model Law on Computer and Computer Related Crime, LMM(02)17. For more information about the Model Law see:

[1239] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1240] For further information and references on electronic evidence see blow: § 6.5.

[1241] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[1242] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1243] Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, Moldova,Monaco, Montegegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Sweden, The former Yugoslav Republic of Macedonia, Turkey, Ukraine and United Kingdom.

[1244] Albania, Andorra, Austria, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Greece, Ireland, Italy, Latvia, Luxemburg, Malta, Moldova, Montegegro, Netherlands, Portugal, Romania, Russia, San Marino, Serbia, Slovenia, Spain, Sweden, Sweden, The former Yugoslav Republic of Macedonia and Turkey.

[1245] For more details, see: *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

[1246] Cybercrime Convention Committee (T-CY)

[1247] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3.

[1248] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

[1249] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

[1250] EDRI, Transborder Data Access: Strong Criticsm on planst o extend CoE Cybercrime Treaty, 5.6.2013, available at: www.edri.org/edrigram/number11.11/transborder-data-access-cybercrime-treaty.

[1251] Report of the Transborder Group for 2013, Cybercrime Convention Committee, T-CY (2013) 30.

[1252] 1: transborder access with consent but without the limitation to data stored "in another Party"; 2: transborder access without consent but with lawfully obtained credentials; 3: transborder access without consent in good faith or in exigent or other circumstances; 4: extending a search from the original computer to connected systems without the limitation "in its territory"; 5: the power of disposal as connecting legal factor.

[1253] T-CY Guidance Note #3 Transborder Access to Data (Article 32), Cybercrime Convention Committee, T-CY (2013) 7E.

[1254] The European Union is a supranational and intergovernmental union with, as at today, 27 Member States from the European continent.

[1255] One example is the EU funded HIPCAR project on Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures. For more information, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1256] *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007, page 69 *et seq.*; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007, page 15 *et seq.*; *Ambos*, Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections, Maastricht Journal of European and Comparative Law, 2005, 173 *et seq.*

[1257] See: *Satzger*, International and European Criminal Law, 2005, page 84 for further reference.

[1258] itle VI, Treaty on European Union.

[1259] Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

[1260] Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03. See in this context: *Gercke.*

[1261] Communication from the Commission to the European Parliament and the Council on the implications of the Court's judgement of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

[1262] Decision of the Court of Justice of the European Communities, 23.10.2007, Case C-440/05; See in this context: *Eisele*, Anmerkung zum Urteil des EuGH C 440/05, JZ 2008, page 251 *et seq.*; *Fromm*, Anmerkung zum Urteil des EuGH C 440/05, ZIS 2008, page 168 *et seq.*

[1263] ABl. 2007 C 306, 1.

[1264] Regarding the impact of the reform on the harmonization of criminal law, see: *Peers*, EU criminal law and the Treaty of Lisbon, European law review 2008, page 507 *et seq.*; *Zeder*, EU-minimum rules in substantive penal law: What will be new with the Lisbon Treaty?, ERA Forum 2008, page 209 *et seq.*

[1265] Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009.

[1266] Regarding the Hague Programme, see: *Braum*, Das Haager-Programm der Europaeischen Union: falsche und richtige Schwerpunkte europaeischer Strafrechtsentwicklung in *Joerden/Szwarc*, Europaeisierung des Strafrechts in Deutschland und Polen, 2007, page 11 *et seq.*

[1267] See: Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009, No. 3.3.1.

[1268] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1269] See: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487, page 24.

[1270] Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1271] Communication of 8 December 1999 on a Commission initiative for The Lisbon Special European Council, 23 and 24 March 2000 – *e*Europe – An information society for all – COM 1999, 687. See in this regard also: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1272] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26.1.2001, COM(2000) 890.

[1273] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1274] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1275] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 31.

[1276] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 32.

[1277] Network and Information Security – A European Policy approach – adopted 6 June 2001.

[1278] For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

[1279] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1280] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1281] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[1282] See Directive 2000/31/EC, recital 1 *et seq.*

[1283] For more details, see below: § 6.

[1284] *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 *et seq.*

[1285] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1286] Decision No. 276/1999/EC of the **European** Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1287] Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA).

[1288] See Art. 4 of the Framework Decision.

[1289] This instrument was in the meantime substituted by the 2012 Directive (see below).

[1290] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

[1291] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1292] See the explanation of the Framework Decision in the Proposal For A Council Framework Decision on combating serious attacks against information systems, No. 1.6.

[1293] Council Framework Decision 2005/222/JHA of 24.02.2005 on attacks against information systems, recital 5.

[1294] Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

[1295] See below.

[1296] *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, page 286.

[1297] European Court of Justice, Case C-275/06.

[1298] See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

[1299] In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

[1300] Data Retention Directive, recital 6.

[1301] Data Retention Directive, recital 6.

[1302] Case C-301/06.

[1303] Judgement in Joined Cases C-293/12 and C-594/12.

[1304] Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[1305] "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

[1306] "Training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

[1307] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2010) 94.

[1308] Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[1309] See: Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, page 2.

[1310] ETS 201. For more information see: § 5.2.1

[1311] See Art. 5, No. 3, of the Draft Directive.

[1312] Regarding the challenges related to the use of encryption technology, see above: § 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

[1313] See Explanatory Report to the Convention on the Protection of Children, No. 140.

[1314] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180.

[1315] Regarding the underlying technology, see: *Austerberrry*, The Technology of Video & Audio Streaming, 2004, page 130 *et seq.*; *Wu/Hou/Zhu/Zhang/Peha*, Streaming Video over the Internet: Approaches and Directions, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 3, 2001, page 282 *et seq.*; *Garfia/Pau/Rico/Gerla*, P2P Streaming Systems: A Survey and Experiments, 2008.

[1316] Regarding filter obligations/approaches, see*: Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide.

[1317] See *Gercke*, The Role of Internet Service Providers in the Fight against Child Pornography, Computer Law Review International, 2009, page 69 *et seq.*

[1318] *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1319] *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1320] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55.

[1321] *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

[1322] *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009, page 131 *et seq.*; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page ix.

[1323] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

[1324] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Deciion 2005/222/JHA.

[1325] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1326] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, page 3.

[1327] 1999/364/JHA: Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the draft Convention on Cyber Crime held in the Council of Europe.

[1328] See Art. 1 of the Common Position.

[1329] See in this context: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1330] See *Gercke*, The Slow Awake of a Global Approach against Cybercrime, Computer Law Review International, page 145.

[1331] The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is based in Paris. For more information, see: www.oecd.org.

[1332] *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1333] OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

[1334] In 1992, the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information Systems. The 24 OECD member countries adopted the guidelines later.

[1335] Adopted by the OECD Council at its 1037th session on 25 July 2002. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

[1336] Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1337] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1338] The report is available at: www.legislationline.org/upload/lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

[1339] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1340] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, page 5, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1341] Computer Viruses and other malicious software: A threat to the internet economy, OECD, 2009.

[1342] The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties. It has 21 members.

[1343] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1344] The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

[1345] Australia, Brunei Darussalam, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Philippines, Singapore, Chinese Taipei, Thailand and United States.

[1346] See: Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

[1347] APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, on 26 October 2002. Regarding national legislation on cybercrime in the Asian-Pacific region, see: *Urbas*, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf. See also in this regard: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1348] APEC TEL-OECD Malware Workshop (2007); APEC TEL and ASEAN Workshop on Network Security (2007); Workshop on Cyber Security and Critical Information Infrastructure Protection (CIIP); APEC Symposium on Spam and Related Threats (2007); APEC Best Practices In International Investigations Training Sessions (2004); Conference on cybercrime for the APEC region (2005); Conference on cybercrime for the APEC region (2004); Conference on cybercrime for the APEC region (2003); Cybercrime legislation training workshops (several, 2003); Judge and Prosecutor Capacity Building Project.

[1349] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1350] Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar, APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

[1351] "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws."

[1352] The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1353] For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/som/mtg/2002/word.Par.0204.File.v1.1

[1354] See: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1355] Cybercrime Legislation & Enforcement Capacity Building Workshop, and Electronic Commerce Steering Group Meeting.

[1356] 2003/SOMIII/ECSG/O21..

[1357] *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.

[1358] See: Model Law on Computer and Computer Related Crime, LMM(02)17, Background information.

[1359] See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

[1360] Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1361] Draft Model Law on Electronic Evidence, LMM(02)12.

[1362] For more information see: www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf.

[1363] For more information see: African Union, Oliver Tambo Declaration, Johannesburg 2009, available at: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf.

[1364] The Draft Convention is available for download at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

[1365] See Part 1, Sec. II, Ch. II.

[1366] See Part 1, Sec. IV.

[1367] See Part 1, Sec. V.

[1368] See Part 2.

[1369] Art. III-1.

[1370] Part 3, Chaptr 1, Art. 1 and Art. 2.

[1371] Art. III-1-1 to Art. III-1-7

[1372] Art. III-1-8 to Art. III-1-12.

[1373] Art. III-2.

[1374] Art. III-3.

[1375] Art. III-4.

[1376] Art. III-5.

[1377] Art. III-6.

[1378] Art. III-7 1).

[1379] For more information see below: § 6.2.2.

[1380] Art. III-8.

[1381] Art. III-9.

[1382] Art. III-10.

[1383] Art. III-11.

[1384] Art. III-12.

[1385] Art. III-13.

[1386] Art. III-14.

[1387] Art. III-15.

[1388] Art. III-16.

[1389] Art. III-17.

[1390] Art. III-19.

[1391] Art. III-20.

[1392] Art. III-21.

[1393] Art. III-22.

[1394] Art. III-24.

[1395] Art. III-25.

[1396] Art. III-26.

[1397] Art. III-27.

[1398] Art. III-36.

[1399] Art. III-37.

[1400] Art. III-39.

[1401] Art. III-41.

[1402] Regarding reasons for this delay see for example: Gareth van Zyl, Adoption of flawed AU cybersecurity convention postponed, IT Web Africa, 21.01.2014, available at: www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed.

[1403] The League of Arab States is a regional organization, with currently 22 members.

[1404] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1405] Draft Electronic Crime Act 2006..

[1406] Draft Law on Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1407] Law No. 2 of 2006, enacted in February 2006.

[1408] Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1409] Decision of the Arab Justice Ministers Council, 19th session, 495-D19-8/10/2003..

[1410] Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE.

[1411] Non-official translation of the recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18 June 2007, Abu Dhabi:

1) Calling for the adoption of a treaty by the Gulf Cooperation Council (GCC) countries, inspired by the Council of Europe Cybercrime convention, to be expanded later to all Arab countries.

2) Calling all GCC countries to adopt laws combating cybercrime inspired by the model of the UAE cybercrime Law.

3) Calling for the adoption of laws in relation to procedural matters such as seizure, inspection and other investigation procedures for such special type of crimes.

5) Providing trainings to inspection and law enforcement officials on dealing with such crimes.

6) Providing sufficient number of experts highly qualified in new technologies and cybercrime particularly in regard to proof and collecting evidence.

7) Recourse to the Council of Europe's expertise in regard to combating cybercrime particularly in regard to studies and other services which would contribute in the elaboration and development of local countries legislation in GCC countries.

8) Harmonization of the legislations in Arab and particularly GCC countries in regard to basic principles in combating this type of crimes on both procedural and substantive level.

9) Increasing cooperation between public and private sectors in the intent of raising awareness and exchange of information in the cybercrime combating field.

1412 The Organization of American States is an international organization with 34 active Member States. For more information, see: www.oas.org/documents/eng/memberstates.asp.

1413 For more information, see: www.oas.org/juridico/english/cyber.htm, and the Final report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations, at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1414 The conclusions and recommendation of the meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas on Cyber Crime are available at: www.oas.org/juridico/english/cyber_meet.htm.

1415 The full list of recommendations from the 2000 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber. The full list of recommendations from the 2003 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1416 The OAS General Secretariat, through the Office of Legal Cooperation of the Department of International Legal Affairs, serves as the technical secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: www.oas.org/dil/department_office_legal_cooperation.htm.

1417 In addition, the Working Group of Governmental Experts on cybercrime recommended that training be provided in the management of electronic evidence and that a training programme be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G8 to help conduct cybercrime investigations. Pursuant to such recommendation, three OAS regional technical workshops were held during 2006 and 2007, the first being offered by Brazil and the United States, and the second and third by the United States. The list of technical workshops is available at: www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

1418 In the meantime, OAS has established joint collaboration with the Council of Europe and attended and participated in the 2007 Octopus Interface Conference on Cooperation against cybercrime. See: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

1419 Conclusions and Recommendations of REMJA-VII, 2008, are available at: www.oas.org/juridico/english/cybVII_CR.pdf.

1420 Conclusions and Recommendations of REMJA-VIII, 2010, are available at: www.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf.

1421 The seventh meeting of the working group on Cybercrime took place from 6-7 February 2012.

1422 Recommendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VII/doc.6/12rev.1.

1423 Recommendation of the Working Group: OEA/Ser.K/ XXXIV, CIBER-VII/doc.6/12rev.1.

1424 Recommendation of the Working Group: OEA/Ser.K/ XXXIV, CIBER-VII/doc.6/12rev.1.

1425 The eighth meeting oft he Working Group on Cyber-Crime took place from 27-28 February 2014.

1426 mendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VIII/doc.4/14rev.1.

1427 For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1428 The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

1429 CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

[1430] Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

[1431] The assessment report is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1432] The workshop was held in Saint Lucia on 8-12 March 2010. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1433] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[1434] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

[1435] More information about the event are available at: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/port_vila/port_vila.html.

[1436] The assessment report will be made available through the project website.

[1437] www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/samoa/samoa.html.

[1438] More information about the event are available at: www.spc.int/en/component/content/article/704-responding-to-cybercrime-threats-in-the-pacific.html.

[1439] An overview about the output of the conference is available at: and www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_tonga_apr_11/AGREED_Cybercrime_Workshop_Outcomes.pdf.

[1440] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[1441] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

[1442] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_cybercrime.pdf

[1443] *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

[1444] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf ; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. ABA International Guide to Combating Cybercrime, 2002, page 78.

[1445] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq*.

[1446] Regarding the application of Art. 23 *et seq.* with regard to traditional crimes, see: Explanatory Report to the Convention on Cybercrime, No. 243.

1447 *Schjolberg*, A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, twelfth UN Crime Congress, 2010, A/CONF.213, page 3, available at: www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf..

1448 *Schjolberg/Ghernaouti-Helie*, A Global Protocol on Cybersecurity and Cybercrime, 2009, available at: www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

1449 Available online: www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf.

1450 For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

1451 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations, No. 41 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations, No. 47 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations, No. 29 (page 7); "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations, No. 40 (page 10).

1452 Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/6_cybercrime/t%2Dcy/FINAL%20T-CY%20_2007_%2003%20-%20e%20-%20Report%20of%20the%20meeting1.pdf.

1453 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions, see *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon of phishing, see *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

1454 For an overview of the different legal approaches, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm. Regarding the economic impact, see for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

1455 There are two aspects that need to be taken into consideration in this context: To avoid redundancy, a new approach should focus on offences that are not intended to be covered within further amendments of the Convention on Cybercrime. The second aspect is related to the difficulties in finding a common position all countries can agree on. Based on the experiences with the negotiations of the Convention on cybercrime, it is likely that negotiations of criminalization that go beyond the standards of the Convention will run into difficulties.

1456 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1457 Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cybercrime, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 35 *et seq*., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cybercrime

and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 1 *et seq*., available at: http://media.hoover.org/documents/0817999825_1.pdf.

1458 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties which the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and surrender procedures between Member States (2002/584/JHA).

1459 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1460 See Convention on Cybercrime, Articles 23-35.

1461 See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq*.

1462 See above: § 2.6.7.

1463 See Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1464 See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1465 Regarding the network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1466 See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper, No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

1467 Regarding the international dimension, see above: § 3.2.6.

1468 With regard to the Convention on Cybercrime, see: Explanatory Report to the Convention on Cybercrime, No. 33.

1469 Regarding concerns related to the speed of the ratification process, see *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 144.

1470 See below: § 6.2.10.

1471 See above: §§ 3.2.6 and 3.2.7.

1472 The issue has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 stipulates: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 Ten-Point Action Plan highlights: "There must be no safe havens for those who abuse information technologies".

1473 For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq*.

1474 For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm. For more information, see below: § 6.2.11.

1475 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-

watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches,
see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf; *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq*.

1476 See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *www.juriscom.net/en/uni/doc/yahoo/poullet.htm*; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

1477 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

1478 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

6. Réponse juridique

Le présent chapitre est une vue d'ensemble de la réponse juridique au phénomène de cybercriminalité en expliquant les approches juridiques de la criminalisation de certains actes[1479]. Dans la mesure du possible, ces approches sont présentées dans un contexte international. Lorsque cela n'est pas possible, des exemples d'approches nationales ou régionales sont donnés.

6.1 Définitions

Bibliography (selected): *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.; *Macagno*, Definitions in Law, Bulletin Suisse de Linguistique Appliquée, Vol. 2, 2010, page 199 et seq, available at: http://ssrn.com/abstract=1742946.

6.1.1 La fonction des définitions

Les définitions sont un élément que l'on retrouve fréquemment dans divers cadres juridiques nationaux et régionaux. Cependant, il est important de faire la différence entre les différentes fonctions de ces définitions. En droit, il est en général possible de distinguer deux classes de définitions: les définitions descriptives et les définitions juridiques.[1480] Les définitions descriptives sont utilisées pour expliquer la signification de termes ambigus, alors que les définitions juridiques visent à désigner ceux qui sont soumis au droit en vertu d'une définition particulière d'un terme.[1481] L'aperçu suivant ne distingue pas ces deux types de définition.

Les cadres juridiques régionaux et les modèles de lois adoptent non seulement des concepts différents eu égard aux types de définitions, mais également s'agissant des aspects quantitatifs. Par exemple, la Convention sur la cybercriminalité ne contient que cinq définitions[1482] alors que le modèle de texte législatif du projet HIPCAR sur la cybercriminalité en contient vingt.

6.1.2 Fournisseur d'accès

Les fournisseurs d'accès jouent un rôle important, car ils permettent aux utilisateurs de se connecter à Internet. En droit sur la cybercriminalité, le terme fournisseur d'accès est utilisé tant pour régir la notion de responsabilité [1483] que l'implication dans les enquêtes – en particulier l'interception légale de communication.[1484] Le modèle de texte législatif du projet HIPCAR sur la cybercriminalité fournit une définition de ce terme.

> ***Définitions***
> ***3.*** *1) « Fournisseur d'accès » désigne toute personne physique ou morale qui fournit un service de transmission électronique de données en transmettant des informations fournies par ou à un utilisateur du service dans un réseau de communication, ou qui fournit un accès à un réseau de communication.*

[…]

La définition est large et couvre les fournisseurs commerciaux ainsi que les sociétés qui ne fournissent un accès qu'à leurs employés et les opérateurs de réseaux privés. Bien que cette disposition soit utile s'agissant d'une application large des règles de responsabilité, elle peut poser certains problèmes si la définition est également appliquée en droit procédural (ce qui n'était pas l'intention des rédacteurs du modèle de texte législatif du projet HIPCAR).

6.1.3 Fournisseur de cache

Les fournisseurs de mise en cache assurent un service important pour augmenter la rapidité d'accès aux contenus populaires. Eu égard à la nécessité de réglementer la responsabilité[1485] des fournisseurs de mise en cache, le modèle de texte législatif du projet HIPCAR a opté pour inclure une définition de ce terme.

> ***Définitions***
> ***3. […]***
> *2) « Fournisseur de cache » désigne toute personne physique ou morale fournissant un service de transmission électronique de données par stockage automatique, intermédiaire et temporaire des informations, dans le seul but de rendre plus efficace la transmission des informations aux autres utilisateurs du service à leur demande;*
> *[…]*

Tout comme dans leur définition du terme « fournisseur d'accès », les rédacteurs n'ont pas limité l'application de cette disposition aux opérations commerciales. Par conséquent, cette disposition couvre également les sociétés et les opérateurs de réseaux privés.

6.1.4 Enfant

Le terme enfant est particulièrement important s'agissant de la criminalisation de la pédopornographie.[1486] Il est également utilisé dans le contexte de certaines dispositions qui criminalisent la mise à la disposition de mineurs certains contenus (par exemple de la pornographie pour adulte).[1487] L'une des définitions les plus utilisées est fournie par la Convention des Nations Unies sur les droits de l'enfant de 1989.

> *Au sens de la présente Convention, un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable.*

Plusieurs cadres juridiques et modèles de lois propres à la cybercriminalité, tels que la Directive de l'UE sur la lutte contre la pédopornographie[1488], la Convention du Conseil de l'Europe de 2007 sur la protection des enfants[1489] et le modèle de texte législatif du projet HIPCAR de 2009 sur la cybercriminalité[1490] comportent des définitions similaires. La Convention du Conseil de l'Europe sur la cybercriminalité le défini pas le terme « enfant », mais uniquement le terme « pédopornographie ».

6.1.5 Pédopornographie

La pédopornographie est l'une des quelques infractions apparentées à la catégorie du contenu illégal pour laquelle la plupart des pays dans le monde ont adopté la criminalisation.[1491] Étant donné la difficulté de faire le tri entre les formes légales de contenu à caractère sexuel et la pédopornographie, certains cadres juridiques fournissent une définition de la pédopornographie.

L'un des principaux défis à relever pour les rédacteurs juridiques à cet égard est d'éviter les conflits entre les différentes catégories d'âge afin d'éviter une criminalisation non souhaitée dans des cas où l'âge du mariage ou du consentement sexuel et l'âge limite au sens de la définition de la pédopornographie diffèrent.[1492] Par exemple, si la pédopornographie est définie comme une description visuelle d'actes sexuels commis par une personne âgée de moins de 18 ans, et que par ailleurs l'âge du consentement sexuel et du mariage est fixé à 16 ans, deux enfants âgés de 17 ans peuvent se marier en toute légalité ou avoir des rapports sexuels, mais commettraient un délit sérieux (production de pédopornographie) s'ils photographiaient ou filmaient cet acte.[1493]

L'article 2 c) du Protocole optionnel à la Convention sur les droits de l'enfant, la vente d'enfants, la prostitution enfantine et la pédopornographie fournit une définition.

Article 2
Aux fins du présent Protocole:
[…]
(c) On entend par pédopornographie toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles.

La définition fournie dans le Protocole optionnel ne couvre pas explicitement les formes de pédopornographie fictionnelles, par exemple les images réalistes. Pour veiller à ce que ce genre de support soit également couvert par la définition, certains cadres juridiques comme la Convention du Conseil de l'Europe sur la cybercriminalité ont modifié la définition de la pédopornographie.

Article 9 *– Infractions se rapportant à la pornographie enfantine*
[…]
(2) Aux fins du paragraphe 1 ci-dessus, le terme « pornographie enfantine » comprend toute matière pornographique représentant de manière visuelle:
a) un mineur se livrant à un comportement sexuellement explicite;
b) une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;
c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.
(3) Aux fins du paragraphe 2 ci-dessus, le terme « mineur » désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.
[…]

L'article 9, paragraphe 2, fournit trois sous-sections d'objets représentant de manière visuelle de la pornographie enfantine: un mineur se livrant à un comportement sexuellement explicite, une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite et les images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

Bien qu'à cet égard la Convention sur la cybercriminalité élargisse la définition fournie par le Protocole optionnel à la Convention des Nations Unies, elle en réduit par ailleurs l'applicabilité dans deux aspects importants.

Bien que les rédacteurs de la Convention sur la cybercriminalité aient insisté sur l'importance d'une norme internationale uniforme concernant l'âge,[1494] la Convention sur la cybercriminalité autorise néanmoins les parties à fixer une limite d'âge différente dans la mesure où elle n'est pas inférieure à 16 ans.

La seconde différence majeure par rapport à la définition fournie par le Protocole optionnel réside dans le fait que la définition de la Convention du Conseil de l'Europe sur la cybercriminalité s'attache à la représentation visuelle. La pornographie enfantine n'est pas nécessairement distribuée sous forme d'images et de films, mais également sous forme de fichiers audio.[1495] Puisque la disposition décrite à l'article neuf se réfère à des « objets représentant de manière visuelle » un enfant, ces dispositions ne couvrent pas les fichiers audio.

Par conséquent, des approches plus récentes comme le texte législatif du projet HIPCAR [1496] sur la cybercriminalité[1497] adoptent le concept du Protocole optionnel à la Convention des Nations Unies plutôt que celui de la Convention du Conseil de l'Europe, et évitent ainsi d'utiliser le terme « de manière visuelle ».

Définitions
3.
[…] (4) « Pédopornographie » ou « pornographie enfantine » se réfère à tout matériel pornographique décrivant, présentant ou représentant:
a) un enfant se livrant à des comportements sexuellement explicites;
b) une personne qui paraît être un enfant se livrant à des comportements sexuellement explicites; ou
c) des images représentant un enfant se livrant à des comportements sexuellement explicites;
Cela inclut, sans s'y limiter, tout support pornographique audio, visuel ou écrit.
Un pays peut restreindre la criminalisation en ne mettant pas en œuvre (b) et (c).

La Directive de l'UE de 2011 sur la lutte contre la pornographie enfantine contient également une définition de la pédopornographie[1498], ainsi que la Convention du Conseil de l'Europe de 2007 sur la protection des enfants.[1499]

6.1.6 Données informatiques

L'utilisation croissante de la technologie informatique de même que la tendance à la numérisation des données ont augmenté la prévalence des données informatiques. Par conséquent, les données informatiques sont devenues une cible fréquente d'attaque allant de l'atteinte à l'intégrité des données[1500] à l'espionnage de données.[1501] Divers cadres juridiques régionaux proposent des définitions des données informatiques. C'est le cas de la section 3 de la loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique.

Définitions
3*. Dans la présente loi, sauf intention contraire manifeste :*
« Donnée informatique » s'entend de toute représentation de faits, d'information ou de concepts sous une forme adaptée à un traitement dans un système informatique, y compris un programme permettant d'ordonner à un système informatique d'exécuter une fonction;
[…]

La Convention du Conseil de l'Europe de 2001 sur la cybercriminalité[1502], la Décision-cadre du Conseil de l'UE de 2005 sur les attaques contre les systèmes d'information[1503], le projet de Directive ECOWAS de 2008 sur la lutte contre la cybercriminalité[1504], et le modèle de textes législatifs de 2009 sur la cybercriminalité du projet HIPCAR proposent des définitions similaires[1505].

6.1.7 Dispositif de stockage de données informatiques

Les dispositifs de stockage jouent un rôle important en matière de cybercriminalité — tant à l'égard d'atteinte éventuelle à l'intégrité des données qu'à l'égard de la saisie de preuve. La section 3 de la loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique est un exemple de cadre juridique régional proposant une telle définition.

Définitions
3.
[…]
« Support de stockage de données informatiques » s'entend de tout objet ou support (par exemple, un disque) à partir duquel l'information est susceptible d'être reproduite, avec ou sans l'aide d'un autre article ou dispositif;
[…]

Le modèle de textes législatifs du projet HIPCAR contient une définition similaire.[1506]

6.1.8 Système informatique

Dans les lois sur la cybercriminalité, le terme « système informatique » est utilisé en droit pénal matériel comme en droit procédural. Les systèmes informatiques peuvent être la cible d'attaques; ils peuvent être utilisés comme un outil pour commettre un délit et, enfin, ils peuvent être saisis comme une preuve. Par conséquent, la plupart des cadres juridiques régionaux et modèles de loi applicables contiennent une définition de ce terme. C'est le cas de la section 3 de la loi type du Commonwealth de 2002 relative à la criminalité informatique et liée à l'informatique.

Définitions
3.
[…]
« système informatique » s'entend d'un dispositif ou un groupe de dispositifs interconnectés ou apparentés, y compris l'Internet, dont un ou plusieurs d'entre eux, conformément à un programme, exécutent un traitement automatisé de données ou toute autre fonction;
[…]

Fait inhabituel, la définition mentionne le terme « l'Internet ». Internet est largement défini comme un système de réseaux interconnectés.[1507] D'un point de vue technique, l'Internet en lui-même n'est donc pas un système informatique, mais un réseau, et ne devrait donc pas être inclus dans la définition des systèmes informatiques, mais plutôt dans la définition des réseaux informatiques. Cependant, plusieurs rédacteurs de cadres juridiques ont suivi l'exemple du modèle de loi du Commonwealth et ont inclus l'Internet dans la définition des systèmes informatiques.

La Convention du conseil de l'Europe de 2001 sur la cybercriminalité[1508], la Décision-cadre du Conseil de l'UE de 2005 sur les attaques contre les systèmes d'information[1509], le projet de Directive ECOWAS de 2008 sur la lutte contre la cybercriminalité[1510], et le modèle de textes législatifs de 2009 sur la cybercriminalité du projet HIPCAR proposent des définitions similaires.[1511]

6.1.9 Infrastructure critique

Conséquence de l'utilisation croissante de l'informatique et des technologies de réseau dans l'exploitation d'infrastructures critiques, ce type d'infrastructures est devenu une cible potentielle d'attaque. [1512] Considérant l'impact potentiel de telles attaques, certains des cadres juridiques les plus récents incluent une criminalisation/aggravation de peine spécifique pour certaines attaques contre des infrastructures critiques, et en proposent donc également une définition. Un exemple avec le modèle de texte législatif de l'HIPCAR sur la cybercriminalité.

Définitions
3.
[…]
(8) « Infrastructures critiques » désigne les systèmes informatiques, les dispositifs, les réseaux, les programmes informatiques, les données informatiques qui sont tellement vitaux pour le pays que toute incapacité, destruction ou atteinte à l'intégrité de ces systèmes et actifs aurait un effet handicapant sur la sécurité, la sécurité nationale ou économique, la santé et la sûreté publiques nationales, ou toute combinaison de ces éléments;
[…]

6.1.10 Cryptologie

L'utilisation de technologies de chiffrement par les délinquants peut sérieusement compromettre l'accès aux preuves.[1513] Par conséquent, plusieurs pays ont mis en oeuvre une législation traitant de l'utilisation des technologies de chiffrement et des instruments d'enquête des services de répression dans ce domaine.[1514] Cependant, des différents cadres juridiques régionaux traitant de la cybercriminalité, seul le projet de convention de l'Union africaine sur la cybersécurité[1515] fournit une définition de la cryptologie dans son article I-1.

8) Cryptologie s'entend de la science de la protection et de la sécurisation de l'information, en particulier aux fins de garantir la confidentialité, l'authentification, l'intégrité et la non-répudiation;

6.1.11 Dispositif

Le terme dispositif est utilisé en particulier en lien avec la criminalisation des « dispositifs illégaux ».[1516] Eu égard aux risques potentiels de voir ces dispositifs largement répandus et utilisés pour commettre des délits, les rédacteurs de plusieurs cadres juridiques régionaux ont décidé d'inclure une disposition visant à criminaliser certaines activités ayant trait aux dispositifs légaux. Contrairement à la Convention du Conseil de l'Europe sur la cybercriminalité et au modèle de loi du Commonwealth, qui utilisent tous deux le terme dispositif, le modèle de loi de l'HIPCAR contient une définition de ce terme dans sa section 3.

Définitions
3.
[…]
(9) « Dispositifs » désigne, sans s'y limiter:
a) les composants de systèmes informatiques tels que les cartes graphiques, la mémoire et les puces;
b) les éléments de stockage, tels que les disques durs, les cartes mémoire, les disques compacts et les bandes;
c) les périphériques d'entrée, tels que les claviers, les souris, les pavés tactiles, les scanneurs et les appareils photo numériques;
d) les périphériques de sortie tels que les imprimantes et les écrans;
[…]

Il s'agit d'une définition descriptive typique, car la disposition indique explicitement que la définition du terme « dispositif » n'est pas limitée aux composants listés (« sans s'y limiter »). Ce terme inclut également les programmes informatiques par référence à la disposition sous-jacente[1517] qui criminalise les dispositifs illégaux.

6.1.12 Entrave

Dans les sociétés de l'information et les économies qui incluent le commerce électronique, le fonctionnement des systèmes informatiques est essentiel. Les attaques contre les systèmes informatiques qui empêchent le système d'exécuter des opérations peuvent sérieusement perturber la société et l'économie. Par conséquent, de nombreux cadres juridiques régionaux criminalisent l'entrave au fonctionnement d'un système informatique. [1518] Le modèle de texte législatif de l'HIPCAR sur la cybercriminalité contient une définition de ce terme propre à la cybercriminalité dans sa section 3.

Définitions
3.
[…]
(10) « Entraver » en relation avec un système informatique signifie, sans s'y limiter:
a) couper l'alimentation électrique d'un système informatique;
b) provoquer des interférences électromagnétiques sur un système informatique; et
c) corrompre un système informatique par quelque moyen que ce soit; et
d) introduire, transmettre, endommager, effacer, détériorer, altérer ou supprimer des données informatiques;
[…]

Cette définition souligne que, parmi les manipulations, figure l'entrave physique (par exemple la coupure de l'alimentation électrique) ainsi que les manipulations liées aux données (par exemple l'introduction de données informatiques).

6.1.13 Hébergeur

Les fournisseurs d'hébergement jouent un rôle crucial en matière de lutte contre la cybercriminalité, car leurs services sont, par exemple, utilisés pour stocker du contenu illégal. Par conséquent, plusieurs cadres

juridiques régionaux traitent des questions ayant trait à la responsabilité des FAI.[1519] Cependant, les principaux cadres juridiques régionaux ne fournissent aucune définition du fournisseur d'hébergement. Mais une définition de ce terme est incluse dans le modèle de texte législatif de l'HIPCAR sur la cybercriminalité.

> ***Définitions***
> ***3.***
> *[…]*
> *(11) « Hébergeur » désigne toute personne physique ou morale qui fournit un service de transmission électronique de données en stockant les informations fournies par l'utilisateur du service;*
> *[…]*

Cette définition ne limite pas l'application de la disposition aux fournisseurs commerciaux, mais inclut également les opérateurs privés. Par conséquent, même l'opérateur d'un site Internet privé qui permet à d'autres personnes de stocker les informations sur son site Internet peut être concerné par les dispositions relatives à la responsabilité.

6.1.14 Lien hypertexte

Alors que très souvent seuls les fournisseurs d'hébergement, les fournisseurs d'accès et les fournisseurs de mise en cache sont repris dans des sous-catégories des Fournisseurs d'accès Internet (FAI), plusieurs cadres juridiques fournissent une réglementation spécifique pour d'autres services tels que les moteurs de recherche[1520] et les liens hypertextes. À cet égard, le modèle de texte législatif de l'HIPCAR sur la cybercriminalité fournit une définition du terme « lien hypertexte ».

> ***Définitions***
> ***3.***
> *[…]*
> *(12) « Lien hypertexte » désigne une caractéristique ou une propriété d'un élément tel qu'un symbole, un mot, une phrase ou une image qui contient des informations sur une autre source et qui pointe vers et affiche un autre document lorsqu'elle est exécutée;*
> *[…]*

Cette définition est large et couvre divers types de liens hypertextes tels que les liens profonds.

6.1.15 Interception

Le terme interception est fréquemment utilisé en droit pénal matériel eu égard à la criminalisation de l'interception illégale et en droit pénal procédural[1521] eu égard à l'interception illégale de communication. Alors que des cadres régionaux comme la Convention du Conseil de l'Europe sur la cybercriminalité et le modèle de loi du Commonwealth incluent des dispositions ayant trait à l'interception légale et illégale, ces cadres ne fournissent aucune définition de l'interception. Toutefois, le modèle de texte législatif de l'HIPCAR sur la cybercriminalité en propose une.

> ***Définitions***
> ***3.***
> *[…]*
> *(13) « Interception » inclut, sans s'y limiter, l'acquisition, la visualisation et la capture de toute communication de données informatiques, que ce soit de manière câblée, sans fil, électronique, optique, magnétique, orale ou par tout autre moyen durant la transmission, à l'aide d'un dispositif technique;*
> *[…]*

6.1.16 Atteinte à l'intégrité

L'atteinte à l'intégrité est un terme générique utilisé dans plusieurs dispositions ayant trait à la cybercriminalité. L'atteinte à l'intégrité des données[1522] ainsi que l'atteinte à l'intégrité d'un système en sont des exemples.[1523] Toutefois, dans plusieurs instruments régionaux, le terme n'est utilisé que dans les titres de certaines dispositions, mais ne décrit pas un acte criminalisé en soi. Par conséquent, la plupart des cadres juridiques régionaux et modèles de loi ne fournissent aucune définition de ce terme.

6.1.17 Courriers électroniques multiples

Une grande part des courriels qui sont expédiés sont des spams. Par conséquent, un certain nombre de pays, de même que de récents modèles de loi, ont inclus des dispositions criminalisant les actes ayant trait à la distribution de spams.[1524] Le terme « courriers électroniques multiples » est un terme clé utilisé dans ces dispositions. Le modèle de texte législatif de l'HIPCAR sur la cybercriminalité contient une définition de ce terme.

Définitions
3.
[…]
(14) « Courriers électroniques multiples » désigne tout message électronique, notamment courriel et messagerie instantanée, envoyé à plus de mille destinataires;
[…]

6.1.18 Logiciel de criminalistique à distance

Certains cadres juridiques plus récents et avancés incluent des instruments de procédure qui, dans certains cas, autorisent les agences de répression à utiliser des outils de criminalistique sophistiqués – notamment les enregistreurs de frappe.[1525] Le modèle de texte législatif de l'HIPCAR sur la cybercriminalité contient une définition du terme « logiciel de criminalistique à distance ».

Définitions
3.
[…]
(15) « Logiciel de criminalistique à distance » désigne un logiciel d'enquête installé sur un système informatique et utilisé pour effectuer des tâches incluant, sans s'y limiter, l'enregistrement de frappes ou la transmission d'une adresse IP;
[…]

Dans le débat à propos de l'utilisation des normes HIPCAR, qui ont été élaborées pour les Caraïbes, il a été objecté, dans la région pacifique, que, pour couvrir intégralement le spectre des solutions de criminalistique, le terme « outil » (qui englobe également les solutions matérielles) est préférable au terme « logiciel ».

6.1.19 Saisir

En matière de criminalité traditionnelle, mais également de cybercriminalité, la saisie demeure l'un des instruments d'enquête les plus importants utilisés pour réunir des preuves. [1526] La loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique contient une définition de la saisie dans sa partie III (Pouvoirs procéduraux, section 11).

Définitions pour la présente partie
[…]
II. Dans la présente partie :
[…]

Le terme « saisi » inclut:

(a) faire et conserver une copie de données informatiques, y compris en utilisant l'équipement sur site; et

(b) rendre inaccessible, ou supprimer, les données informatiques dans le système informatique accédé; et

(c) sortir sur imprimante les données informatiques.

Cette définition qui contient trois sous-sections a fait l'objet de modifications ultérieures dans le cadre de l'élaboration du modèle de texte législatif de l'HIPCAR sur la cybercriminalité. Une définition est proposée à la section 3 (16).

Définitions

3.

[…]

(16) « Saisir » signifie:

a. activer tout système informatique et moyen de stockage des données informatiques sur site;

b. faire et conserver une copie des données informatiques, en utilisant notamment l'équipement sur site;

c. maintenir l'intégrité de ces données informatiques stockées;

d. rendre inaccessible ou retirer les données informatiques du système informatique accédé;

e. sortir sur imprimante les données informatiques; ou

f. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un moyen de stockage des données informatiques;

[…]

La Convention du Conseil de l'Europe sur la cybercriminalité a adopté une approche différente et a inclus les différents éléments de la saisie dans la disposition elle-même.[1527]

6.1.20 Fournisseur de services

Le terme « fournisseur de services » désigne une catégorie utilisée pour décrire les différents types de prestataires offrant des services Internet. Comme cela a été souligné précédemment, différents cadres juridiques régionaux intègrent des dispositions relatives aux fournisseurs de services (notamment des dispositions ayant trait à la responsabilité des différents types de fournisseurs de services, ou aux instruments qui requièrent l'assistance d'un fournisseur de services aux services de répression). Ces instruments ne font pas tous la distinction entre les différents types de fournisseurs. Par conséquent, les cadres de juridiques régionaux, en particulier ceux qui ne font pas cette distinction, incluent une définition de ce terme. C'est le cas, par exemple, de la Convention du Conseil de l'Europe sur la cybercriminalité.

Article 1 - Définitions

[…]

c) l'expression « fournisseur de services » désigne:

i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs;

[…]

La loi type du Commonwealth de 2002 relative à la criminalité informatique et liée à l'informatique [1528], et le modèle de textes législatifs de 2009 du projet HIPCAR sur la cybercriminalité[1529] contiennent également des définitions similaires.

6.1.21 Données relatives au trafic

Les données relatives au trafic désignent une catégorie de données pour lesquelles certains cadres juridiques régionaux et modèles de loi fournissent des instruments d'enquête spécifiques. [1530] Par conséquent, ces cadres juridiques régionaux et modèles de loi fournissent également souvent une définition de ce terme. C'est le cas de la section 3 de la loi type du Commonwealth de 2002 relative à la criminalité informatique et liée à l'informatique.

> ***Définitions***
> ***3.***
> *[…]*
> *« Données relatives au trafic » désigne les données informatiques:*
> *(a) ayant trait à une communication passant par un système informatique; et*
> *(b) générées par un système informatique en tant qu'éléments de la chaîne de communication; et*
> *(c) indiquant l'origine, la destination, l'itinéraire, l'heure, la taille et la durée de la communication ou le type de services sous-jacents.*

La Convention du Conseil de l'Europe sur la cybercriminalité de 2001[1531], et le modèle de texte législatif de 2009 du projet HIPCAR sur la cybercriminalité proposent également des définitions similaires.[1532]

6.2 Droit pénal substantiel

Bibliography (selected): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002; *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke/Tropina*, from Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, Cybercrime Training for Judges, 2009; *Gercke*, How Terrorist Use the Internet in Pieth/Thelesklaf/Ivory, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf; Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.*, available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf; *Lavalle*, A Politicized and Poorly Conceived Notion Crying Out for Clarification: The Alleged Need for Universally Agreed Definition of Terrorism, Zeitschrift fuer auslaendisches oeffentliches Recht und Voelkerrecht, 2006, page 89 *et seq.*;

Levesque, Sexual Abuse of Children: A Human Rights Perspective, 1999; *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11; *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact and Prevention, Youth & Society, Vol. 34, 2003; *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; *Parsonage*, Web Browser Session Restore Forensics, A valuable record of a user's internet activity for computer forensic examinations, 2010, available at: http://computerforensics.parsonage.co.uk/downloads/WebBrowserSessionRestoreForensics.pdf; Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement Act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII; *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, 2001; *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP/e-RIAPL, 2008, C-07; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33; *Walden*, Computer Crimes and Digital Investigations, 2006; *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2; *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729; *Wolak/ Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

6.2.1 Accès illégal (Hacking)

Depuis le développement des réseaux informatiques et de leur capacité à relier des ordinateurs entre eux et à offrir aux utilisateurs l'accès à d'autres systèmes informatiques, les ordinateurs sont utilisés par les hackers à des fins criminelles[1533]. Les motivations des hackers sont très diverses[1534]. Il leur est inutile d'être présents sur le lieu du délit[1535]; il leur suffit de contourner tous les dispositifs qui protègent les réseaux[1536]. Dans de nombreux cas d'accès illégal, les systèmes de sécurité qui protègent l'emplacement physique des équipements de réseau sont plus complexes que ceux qui protègent les informations sensibles circulant sur les réseaux, même à l'intérieur d'un même bâtiment[1537].

L'accès illégal aux systèmes informatiques empêche les opérateurs de diriger, d'exploiter et de contrôler leurs systèmes en toute tranquillité[1538]. L'objectif des dispositifs de protection est de maintenir l'intégrité des systèmes informatiques[1539]. Il est essentiel de faire la distinction entre l'accès illégal et les infractions ultérieures à cet accès, comme l'espionnage de données[1540], car les dispositions juridiques ont une vue différente de la protection dans ces deux cas. Dans la plupart des cas, l'accès illégal (le droit cherche à protéger l'intégrité du système informatique proprement dit) n'est pas l'objectif ultime, mais plutôt une première étape vers d'autres infractions, comme la modification ou l'obtention de données en mémoire (le droit cherche à protéger l'intégrité et la confidentialité des données)[1541].

La question est de savoir si l'accès illégal doit être criminalisé, en plus des infractions ultérieures[1542]. L'analyse des diverses approches nationales de la criminalisation de l'accès illégal à des systèmes informatiques montre que les dispositions en vigueur créent parfois la confusion entre l'accès illégal et les infractions ultérieures, ou bien cherchent à limiter la criminalisation de l'accès illégal aux graves violations seulement[1543]. Certains pays criminalisent simplement l'accès alors que d'autres limitent la criminalisation aux infractions seulement lorsque le système violé est protégé par des mesures de sécurité ou lorsque l'auteur a l'intention de nuire ou encore lorsque des données ont été obtenues, modifiées ou endommagées[1544]. Pour d'autres pays, le droit ne criminalise pas l'accès proprement dit, mais seulement les infractions ultérieures[1545]. Ceux qui s'opposent à la criminalisation de l'accès illégal se réfèrent à des situations où la simple intrusion n'a pas causé de danger ou lorsque des actes de « hacking » ont conduit à la détection de failles et de points faibles dans la sécurité des systèmes informatiques visés[1546].

Convention du Conseil de l'Europe sur la cybercriminalité

La Convention du Conseil de l'Europe sur la cybercriminalité comporte une disposition relative à l'accès illégal, qui protège l'intégrité des systèmes informatiques en criminalisant l'accès non autorisé à un système. Remarquant qu'il existait des incohérences au plan national[1547], la Convention offre la possibilité de limiter, au moins dans la plupart des cas, qui permet aux pays sans législation de retenir des législations plus libérales concernant l'accès illégal[1548]. Cette disposition vise à protéger l'intégrité des systèmes informatiques.

Disposition

> ***Article 2 – Accès illégal***
> *Chaque Partie adopte des mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.*

Les actes couverts

Le terme « accès » ne désigne pas un certain moyen de communication, mais est indéfini et ouvert à d'autres développements techniques[1549]. Il englobe tous les moyens de pénétrer un autre système informatique, y compris les attaques Internet[1550], ainsi que l'accès illégal à des réseaux sans fil. Cette disposition couvre même l'accès non autorisé à des ordinateurs qui ne sont pas connectés à un réseau (par exemple, en contournant une protection par mot de passe)[1551]. Cette définition large signifie que l'accès illégal couvre non seulement de futurs développements techniques, mais aussi des données secrètes auxquelles ont accès des personnes internes et des membres du personnel[1552]. La deuxième phrase de l'article 2 offre la possibilité de limiter la criminalisation de l'accès illégal à l'accès par un réseau[1553].

Les actes illégaux et les systèmes protégés sont donc définis de façon à rester ouverts pour tenir compte de futurs développements. Le Rapport explicatif dresse une liste des matériels, composants, données stockées, répertoires, données liées au trafic et au contenu comme exemples de parties de systèmes informatiques auxquelles on peut avoir accès[1554].

Élément moral

Comme toutes les autres infractions définies dans la Convention sur la cybercriminalité, l'article 2 repose sur le fait que l'auteur commette les infractions intentionnellement[1555]. La Convention ne donne pas de définition du terme « intentionnellement ». Dans le rapport explicatif, les rédacteurs soulignent que la définition du mot « intentionnellement » devrait être donnée à un niveau national[1556].

Sans droit

L'accès à un ordinateur ne peut faire l'objet de poursuites, au titre de l'article 2 de la Convention, que s'il est commis « sans droit »[1557]. L'accès à un système autorisant l'accès libre et public ou l'accès à un système

avec l'autorisation du propriétaire ou autre détenteur de droit ne peut être qualifié de sans droit[1558]. Outre la question du libre accès, la légitimité des procédures de test de sécurité est également étudiée[1559]. Les administrateurs de réseaux et les entreprises de sécurité qui testent la protection de systèmes informatiques afin de repérer les lacunes éventuelles dans les mesures de sécurité craignaient que leurs interventions soient assimilées à un accès illégal[1560]. Bien que ces professionnels travaillent généralement avec l'autorisation du propriétaire et agissent donc légalement, les rédacteurs de la Convention ont souligné le fait que « les tests ou la protection de la sécurité d'un système informatique autorisés par le propriétaire ou l'exploitant, […] se font avec droit »[1561].

Le fait que la victime du délit ait communiqué un mot de passe ou un code d'accès similaire à l'auteur ne signifie pas nécessairement que l'auteur a agi ensuite avec droit lorsqu'il a accédé au système informatique de la victime. Si l'auteur a persuadé la victime de lui divulguer un mot de passe ou un code d'accès à la suite d'une approche de type « ingénierie sociale »[1562], il faut alors vérifier si l'autorisation donnée par la victime couvre l'acte commis par l'auteur[1563]. En général, ce n'est pas le cas et l'auteur a donc agi sans droit.

Restrictions et réserves

La Convention propose une alternative à cette approche large en offrant la possibilité de restreindre la criminalisation au moyen d'éléments additionnels énumérés dans la deuxième phrase[1564]. La procédure relative à la façon d'utiliser ces réserves est exposée à l'article 42 de la Convention[1565]. Ces réserves peuvent concerner des mesures de sécurité[1566], l'intention spéciale d'obtenir des données informatiques[1567], d'autres intentions malhonnêtes qui justifient la culpabilité pénale ou des exigences que l'infraction soit commise contre un système informatique à travers un réseau[1568]. On peut trouver une approche similaire dans la Décision-cadre du Conseil de l'UE [1569] relative aux attaques visant les systèmes d'information.[1570]

Loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique

On trouve une approche similaire à la section 5 de la loi type du Commonwealth de 2002[1571]. Comme dans la Convention du Conseil de l'Europe sur la cybercriminalité, cette disposition protège l'intégrité des systèmes informatiques.

> ***Accès illégal 5.***
> *Toute personne qui intentionnellement, sans justification ou excuse légitimes, accède à l'ensemble ou à une partie d'un système informatique commet une infraction passible, après déclaration de culpabilité, d'une peine de prison d'une durée d'une durée maximale de [durée de la peine], ou d'une amende d'une durée maximale de [montant de l'amende], ou des deux.*

La section 5 adopte une approche semblable à l'article 5 de la Convention du Conseil de l'Europe sur la cybercriminalité. La différence principale avec la Convention sur la cybercriminalité est le fait que la loi type du Commonwealth ne contient pas d'options pour faire des réserves.

Directive de l'Union européenne relative aux attaques contre les systèmes d'information

La directive de l'Union européenne de 2013 relative aux attaques contre les systèmes d'information[1572] contient une disposition qui criminalise l'accès illicite aux systèmes d'information dans son article 3.

> ***Article 3*** *– Accès illicite à des systèmes d'information*
> *1. Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'accès sans droit, lorsqu'il est intentionnel, à tout ou partie d'un système d'information, lorsque l'acte est commis en violation d'une mesure de sécurité, au moins lorsqu'il ne s'agit pas de cas mineurs.*
> *2. Les Etats membres peuvent décider que le comportement visé au paragraphe 1 ne soit érigé en infraction pénale qu'en cas d'infraction à une mesure de sécurité.*

Cette disposition a été rédigée conformément aux normes définies par la Convention du Conseil de l'Europe sur la cybercriminalité.[1573] La première grande différence avec la Convention sur la cybercriminalité est le

fait que les Etats membres peuvent restreindre la criminalisation aux cas où les faits ne sont pas sans gravité. Dans ce contexte, la décision-cadre souligne explicitement que les cas sans gravité ne doivent pas être concernés par cet instrument.[1574] La deuxième grande différence tient au fait que l'article 3 énonce que cette disposition ne peut être appliquée que lorsqu'il y a eu violation d'une mesure de sécurité en place, alors que cette restriction est seulement facultative dans le cas de la Convention sur la cybercriminalité.

Projet de Convention internationale de Stanford

Le projet informel de Convention de Stanford de 1999 [1575] reconnaît que l'accès illégal figure parmi les infractions que les États signataires devraient criminaliser.

Disposition

> ***Art. 3*** *– Infractions*
> *1. Au titre de la présente Convention, une infraction est commise si une personne s'engage illégalement et intentionnellement dans l'une des actions suivantes sans autorité, autorisation ou consentement reconnu juridiquement:*
> *[...]*
> *(c) pénètre dans un système cybernétique dont l'accès est restreint, de manière ostensible et non ambiguë;*
> *[...]*

Les actes couverts

Ce projet de disposition fait apparaître un certain nombre de similitudes avec l'article 2 de la Convention du Conseil de l'Europe sur la cybercriminalité. Ces deux textes imposent qu'un acte intentionnel soit commis sans droit/sans autorité. Dans ce contexte, l'exigence du projet de disposition (« *sans autorité, autorisation ou consentement reconnus juridiquement* ») est plus précise que l'expression « sans droit »[1576] utilisée dans la Convention sur la cybercriminalité, et vise explicitement à intégrer le concept d'autoprotection[1577]. Une autre différence avec l'approche régionale de la Convention sur la cybercriminalité réside dans le fait que le projet de disposition utilise l'expression « système cybernétique ». Le système cybernétique est défini à l'article 1, paragraphe 3 du projet de Convention. Il couvre tout ordinateur ou réseau d'ordinateurs utilisés pour relayer, transmettre, coordonner ou contrôler la transmission de données ou de programmes. Cette définition offre de nombreuses similitudes avec la définition de l'expression « système informatique » donnée par l'article 1 a) de la Convention sur la cybercriminalité[1578]. Bien que le projet de Convention se réfère à des actes liés à l'échange de données et mette donc l'accent, pour l'essentiel, sur les systèmes informatiques basés sur des réseaux, ces deux définitions couvrent aussi bien les ordinateurs interconnectés que les ordinateurs autonomes[1579].

6.2.2 Présence illégale

L'intégrité des systèmes informatiques peut être violée non seulement en pénétrant illégalement dans un système informatique, mais également en continuant d'utiliser un système informatique au-delà de l'autorisation d'utilisation. Puisque dans ces cas le système informatique n'a pas été accédé illégalement, l'application des dispositions qui criminalisent l'accès illicite aux systèmes informatiques peut poser problème.

Conseil de l'Europe

La Convention du Conseil de l'Europe sur la cybercriminalité criminalise l'accès illicite à un système informatique, mais pas la présence illégale dans un système informatique. Néanmoins, la présence illégale a fait l'objet d'un débat pendant la négociation de la Convention. En 1998, lorsque la quatrième ébauche de la Convention sur la cybercriminalité a été finalisée, elle contenait toujours cet élément.

***Art. 2** – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques*
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants [Lorsqu'ils sont commis intentionnellement]:
[…]
1bis: le manquement intentionnel à quitter un système informatique, auquel a accédé entièrement ou partiellement une personne sans autorisation, dès qu'elle a eu connaissance de cette situation [anormale].
[…]

Toutefois, cette disposition a été supprimée de la version finale de la Convention sur la cybercriminalité ouverte à la signature en 2001.

Exemple

Certaines approches récentes comme le texte législatif sur la cybercriminalité de l'HIPCAR [1580] [1581] comportent des dispositions spécifiques pour traiter cette question. La section 5 criminalise la présence illégale dans un système informatique. Comme dans le cas de la criminalisation de l'accès illégal, l'intérêt légal protégé est l'intégrité des systèmes informatiques.

Présence illégale
***5.** (1) Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, reste intentionnellement connectée à l'ensemble ou une partie d'un système informatique, ou qui continue d'utiliser un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.*
(2) Un pays peut décider de ne pas criminaliser la connexion non autorisée si d'autres recours efficaces existent. Un pays peut également imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.

Cette disposition, présentée sous cette forme dans aucune autre approche régionale, reflète le fait que l'intégrité d'un système informatique peut être violée non seulement par l'introduction sans autorisation dans un système informatique, mais également par la présence maintenue à l'intérieur d'un système informatique après l'expiration de l'autorisation. Le terme « présence » suppose que le délinquant ait toujours accès au système informatique. Cela peut être le cas, par exemple, si le délinquant/la délinquante demeure connecté(e) ou continue d'exécuter des opérations. Le fait qu'il/elle dispose de la possibilité théorique de se connecter au système informatique n'est pas suffisant. La section 54 précise que le délinquant/la délinquante doit commettre l'infraction intentionnellement. Les actes assimilables à de l'imprudence ne sont pas concernés. Par ailleurs, la section 54 ne criminalise que les actes qui sont commis « sans motif ou justification légitimes ».

6.2.3 Espionnage de données

La Convention sur la cybercriminalité, le Modèle de loi du Commonwealth et le Projet de Convention de Stanford proposent des solutions juridiques aux seuls problèmes d'interception illégale[1582]. On peut se demander si l'article 3 de la Convention sur la cybercriminalité est applicable à d'autres cas que ceux où des infractions sont commises sous la forme d'interception de processus de transferts de données. Comme il est indiqué ci-après[1583], la question de savoir si l'accès illégal à des informations stockées sur un disque dur est couvert par la Convention a fait l'objet d'un débat d'un grand intérêt[1584]. Vu qu'un processus de transfert est nécessaire, il est vraisemblable que l'article 3 de la Convention sur la cybercriminalité ne couvre pas des formes d'espionnage de données autres que l'interception de processus de transferts[1585]. C'est intéressant dans la mesure où le 9e projet de la convention sur la cybercriminalité mentionnait la pertinence de pénaliser l'espionnage de données.

À ce propos, on pose souvent la question de savoir si la criminalisation de l'accès illégal rend inutile la criminalisation de l'espionnage de données. Lorsque l'auteur a un accès légitime à un système informatique (par exemple, parce qu'il/elle a reçu l'ordre de le réparer) et si à cette occasion (en violation de la légitimation limitée) il/elle copie des fichiers du système, cet acte n'est en général pas couvert par les dispositions relatives à la criminalisation de l'accès illégal[1586].

Vu qu'un important volume de données vitales est aujourd'hui stocké dans des systèmes informatiques, il est essentiel de savoir si les mécanismes de protection de données existants sont adéquats ou si d'autres dispositions juridiques pénales sont nécessaires pour protéger l'utilisateur contre l'espionnage de données[1587]. Aujourd'hui, les utilisateurs d'ordinateurs peuvent recourir à divers dispositifs matériels et outils logiciels pour protéger les informations secrètes. Ils peuvent installer des pare-feux, des systèmes de contrôle d'accès ou chiffrer des informations stockées et ainsi diminuer le risque d'espionnage de données[1588]. Bien qu'il existe des dispositifs conviviaux qui ne demandent que des connaissances limitées de la part des utilisateurs, une protection véritablement efficace des données sur un système informatique exige souvent des connaissances que peu d'utilisateurs possèdent[1589]. Les données stockées sur des systèmes informatiques privés ne sont souvent pas suffisamment protégées contre l'espionnage de données. Des dispositions juridiques criminelles peuvent donc offrir une protection additionnelle.

Quelques pays ont décidé d'élargir la protection qui est disponible par des mesures techniques visant à criminaliser l'espionnage de données. On distingue deux approches principales: certains pays suivent une voie étroite et criminalisent l'espionnage de données uniquement lorsque l'on obtient des informations secrètes spécifiques; on citera comme exemple le paragraphe 1831 du titre 18 du Code des Etats-Unis, qui criminalise l'espionnage économique. Cette disposition ne couvre pas uniquement l'espionnage de données, mais aussi d'autres moyens d'obtenir des informations secrètes.

Code des Etats-Unis

§ 1831 *– Espionnage économique*
a) En général — quiconque, ayant l'intention ou sachant que l'infraction profite à un gouvernement étranger, un intermédiaire étranger, ou un agent étranger, en toute connaissance de cause—

(1) vole, ou, sans autorisation, s'approprie, prend, emporte, ou cache, ou frauduleusement, ou de façon factice, ou par supercherie, obtient un secret commercial;
(2) sans autorisation, copie, duplique, illustre, dessine, photographie, télécharge, modifie, détruit, photocopie, reproduit, transmet, livre, envoie, adresse par courrier, communique ou cède un secret commercial;
(3) reçoit, achète, ou possède un secret commercial, sachant que ce dernier a été volé ou approprié, obtenu ou transformé sans autorisation;
(4) tente de commettre une infraction décrite à l'un des paragraphes 1) à 3); ou
(5) conspire avec une ou plusieurs personnes en vue de commettre une infraction décrite à l'un des paragraphes 1) à 3) et qu'une ou plusieurs de ces personnes agissent de façon à obtenir l'objet de la conspiration; devra, sauf comme il est prévu à l'alinéa b), payer une amende d'une durée maximale de $ 500 000 ou être puni d'une peine de prison d'une durée d'une durée maximale de 15 ans, ou des deux.

b) Organisation — Toute organisation qui commet une infraction décrite à l'alinéa a) devra payer une amende d'une durée maximale de $ 10 000 000.

Ce paragraphe 1831 a été introduit par la Loi sur l'espionnage économique de 1996.[1590] Avant 1996, l'espionnage économique n'était criminalisé qu'en vertu de lois fédérales largement incohérentes.[1591] La Loi sur l'espionnage économique criminalise deux types de détournement de secret commercial dans son titre 18 — vol d'un secret commercial au bénéfice d'un gouvernement, d'un instigateur ou d'un agent étranger; et vol de secrets commerciaux commis en vue d'en tirer un avantage économique, qu'il profite ou non un gouvernement, un instigateur ou un agent étranger.[1592] Bien que cette disposition s'attache à la protection de contenus (secrets commerciaux) et ne désigne aucun format spécifique (données informatiques), elle ne s'applique pas uniquement aux délits conventionnels, mais également aux infractions liées à l'informatique.[1593] En général, le paragraphe 1830 a) 2) du titre 18 du Code des Etats-Unis

est également applicable à ce genre de cas.[1594] Eu égard aux cas liés à l'informatique, ces actes sont couverts par le paragraphe 1830 a) 2) à 5).

Texte législatif sur la cybercriminalité de l'HIPCAR

La section 8 du texte législatif sur la cybercriminalité de l'HIPCAR[1595] est un autre exemple.[1596]

> ***Espionnage des données***
> ***8.*** *(1) Une personne qui, sans motif ou justification légitimes, ou en se prévalant à tort d'un motif ou d'une justification légitime, obtient intentionnellement, pour elle-même ou un tiers, des données informatiques qui ne lui sont pas destinées et qui sont spécialement protégées contre l'accès non autorisé, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.*
> *(2) Un pays peut limiter la criminalisation à certaines catégories de données informatiques.*

La section huit protège le secret des données informatiques stockées et protégées. Cette protection spéciale suppose que l'hébergeur des informations ait mis en oeuvre des mesures de protection qui compliquent significativement l'accès aux données sans autorisation. À titre d'exemple, on peut citer la protection par mot de passe et le chiffrement. Les notes explicatives du texte législatif soulignent qu'il est nécessaire que ces mesures de protection aillent au-delà des mesures de protection standard appliquées aux données ainsi qu'aux autres propriétés, par exemple les restrictions d'accès à certaines parties des bâtiments gouvernementaux.[1597]

Code pénal allemand

On trouve une approche similaire à la Section 202a du Code pénal allemand, dans sa version en vigueur jusqu'à 2007[1598].

> ***Section 202a.*** *– Espionnage de données:*
> *(1) Toute personne qui obtient, sans autorisation, pour lui-même ou pour une autre personne, des données qui ne lui sont pas destinées et qui sont spécifiquement protégées contre tout accès non autorisé, est passible d'une peine de prison d'une durée d'une durée maximale de trois ans ou d'une amende.*
> *(2) Le terme "données" au sens de la sous-section 1 désigne uniquement les données stockées ou transmises par des moyens électroniques ou magnétiques ou sous toute autre forme qui n'est pas visible directement.*

Cette disposition couvre non seulement les secrets économiques, mais aussi les données informatiques stockées en général[1599]. En termes d'objets de protection, cette approche est plus large que celle du paragraphe 1831 (Espionnage économique) du Code des Etats-Unis, mais l'application de cette disposition est limitée puisque l'obtention de données n'est criminalisée que lorsque ces données sont spécialement protégées contre l'accès non autorisé[1600]. La protection de données informatiques stockées, au titre du droit criminel allemand, est donc limitée aux personnes ou entreprises qui ont pris des mesures pour éviter d'être victimes de telles infractions[1601].

Pertinence d'une telle disposition

La mise en œuvre d'une telle disposition est particulièrement pertinente lorsque l'auteur a été autorisé à accéder à un système informatique (par exemple, parce qu'il/elle avait reçu l'ordre de remédier à un problème informatique) et a ensuite abusé de cette autorisation pour obtenir de manière illégale des informations stockées dans le système informatique[1602]. Eu égard au fait que l'autorisation couvre l'accès au système informatique, il n'est généralement pas possible de le couvrir par des dispositions criminalisant l'accès illégal**.**

Sans droit

L'application de dispositions relatives à l'espionnage de données exige en général que les données soient obtenues sans le consentement de la victime. Les attaques par hameçonnage[1603] sont la preuve évidente

du succès des escroqueries basées sur la manipulation des utilisateurs[1604]. Du fait du consentement des victimes, les auteurs qui réussissent à manipuler des utilisateurs pour qu'ils divulguent des informations secrètes ne peuvent être poursuivis sur la base des dispositions mentionnées ci-dessus.

6.2.4 Interception illégale

Le recours aux TIC s'accompagne de plusieurs risques liés à la sécurité du transfert de l'information[1605]. Contrairement aux opérations classiques de vente par correspondance à l'intérieur d'un pays, les opérations de transferts de données par l'Internet font intervenir de nombreux fournisseurs et différents points où ces opérations peuvent être interceptées[1606]. Le maillon le plus faible pour l'interception demeure l'utilisateur, en particulier lorsqu'il utilise un ordinateur personnel, qui est souvent mal protégé contre les attaques venues de l'extérieur. Les auteurs visant toujours le maillon le plus faible, le risque d'attaques contre les utilisateurs privés est important surtout si l'on tient compte des éléments suivants:

- le développement de technologies vulnérables; et
- l'intérêt croissant des informations personnelles pour les auteurs d'infractions.

Les nouvelles technologies de réseau (comme le « LAN sans fil ») offrent plusieurs avantages pour l'accès à l'Internet[1607]. La mise en place d'un réseau sans fil chez un particulier, par exemple, permet aux familles de se connecter à Internet depuis n'importe quel point situé dans un rayon d'action donné, sans qu'il soit nécessaire de passer par une connexion câblée. Mais la popularité de cette technologie et le confort qui en résulte s'accompagnent de risques graves pour la sécurité du réseau. Si un réseau sans fil non protégé est disponible, les auteurs d'infractions peuvent s'y connecter et l'utiliser à des fins criminelles sans avoir à pénétrer dans un bâtiment. Il leur suffit de se trouver à portée du réseau sans fil pour lancer une attaque. Des essais sur le terrain laissent à penser que dans certaines zones, on peut compter jusqu'à 50 pour cent des réseaux sans fil privés qui ne sont pas protégés contre les interceptions ou accès non autorisés[1608]. Dans la plupart des cas, l'absence de protection est due à une méconnaissance des mesures de protection à mettre en place[1609].

Dans le passé, les auteurs d'infractions se concentraient principalement sur les réseaux d'entreprises pour pratiquer des interceptions illégales[1610]. L'interception de communications d'entreprises avait davantage de chances de rapporter des informations plus utiles que celles obtenues sur les réseaux privés. Le nombre croissant de vols d'identité à partir de données personnelles privées suggère que les délinquants ont peut-être changé de cible[1611]. Ils portent désormais un grand intérêt aux données privées comme les numéros de carte de crédit, les numéros de sécurité sociale[1612], les mots de passe et les informations sur les comptes bancaires.[1613]

La Convention du Conseil de l'Europe sur la cybercriminalité

La Convention sur la cybercriminalité inclut une disposition qui protège l'intégrité des transmissions non publiques en criminalisant leurs interceptions non autorisées. Cette disposition vise à aligner la protection des transferts électroniques sur la protection des conversations contre les écoutes illégales et (ou) enregistrements qui déjà existent dans la plupart des systèmes juridiques[1614].

Disposition

Article 3 *– Interception illégale*
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Les actes couverts

L'applicabilité de l'article 3 est limitée à l'interception de transmissions réalisées par des mesures techniques[1615]. Les interceptions liées aux données électroniques peuvent être définies comme tout acte d'acquisition de données pendant une opération de transfert[1616].

Comme cela a été évoqué auparavant, la question de savoir si l'accès illégal à des informations stockées sur un disque dur est couvert par cette disposition fait l'objet d'une controverse[1617]. Généralement, cette disposition ne s'applique qu'à l'interception de transmissions et l'accès à des informations stockées n'est pas considéré comme l'interception d'une transmission[1618]. Le fait que l'application de cette disposition fasse l'objet d'un débat même lorsque l'auteur accède physiquement à un système informatique autonome est dû, en partie, au fait que la Convention sur la cybercriminalité ne prévoit pas de dispositions concernant l'espionnage de données[1619]; le Rapport explicatif de la Convention contient deux explications quelque peu imprécises concernant l'application de l'article 3:

Tout d'abord, le Rapport explicatif fait remarquer que cette disposition couvre les processus de communication qui se déroulent au sein d'un système informatique[1620]. Toutefois, il ne répond toujours pas à la question de savoir si cette disposition ne devrait s'appliquer que dans les cas où les victimes envoient des données qui sont ensuite interceptées par les auteurs ou si elle devrait également s'appliquer lorsque les auteurs utilisent l'ordinateur. Le second point a trait à la criminalisation de l'acquisition illégale de données informatiques.

Le rapport souligne que l'interception peut être commise soit indirectement par l'utilisateur de dispositifs d'écoute, soit « par l'accès et l'utilisation du système informatique »[1621]. Si des auteurs d'infractions parviennent à accéder à un système informatique et l'utilisent pour faire des copies non autorisées de données sur un disque dur externe, lorsque cet acte conduit à un transfert de données (envoi des données entre le disque dur interne et le disque dur externe), ce processus n'est pas *intercepté*, mais plutôt *déclenché*, par les auteurs. L'élément manquant de l'interception technique est un argument fort contre l'application de la disposition en cas d'accès illégal à des informations stockées[1622].

Le terme « transmission » couvre tous les transferts de données, par téléphone, télécopie, courriel ou transferts de fichiers[1623]. L'infraction établie au titre de l'article 3 ne s'applique qu'aux transmissions non publiques[1624]. Une transmission est dite « non publique » si le processus utilisé est confidentiel[1625]. L'élément vital utilisé pour faire la différence entre les transmissions publiques et non publiques n'est pas la nature des données transmises, mais la nature du processus de transmission lui-même. Même le transfert d'informations accessibles au public peut être considéré comme une infraction si les Parties impliquées dans le transfert ont l'intention de garder secret le contenu de leurs communications. L'utilisation de réseaux publics n'exclut pas les communications « non publiques ».

Élément moral

Comme toutes les autres infractions définies par la Convention sur la cybercriminalité, l'article 3 impose que l'auteur commette les infractions intentionnellement[1626]. La Convention ne contient pas de définition du terme « intentionnellement ». Dans le Rapport explicatif, les rédacteurs soulignent que la définition du terme « intentionnellement » devrait être donnée au niveau national[1627].

Sans droit

L'interception de communications ne peut faire l'objet de poursuites au titre de l'article 3 de la Convention que si elle est effectuée « sans droit »[1628]. Les rédacteurs de la Convention ont donné une série d'exemples d'interceptions qui ne sont pas effectuées sans droit, parmi lesquels: acte sur ordre ou avec l'autorisation des participants à la transmission[1629]; activités autorisées de contrôle ou de protection approuvées par les participants[1630]; interception légitime sur la base de dispositions du droit criminel ou dans l'intérêt de la sécurité nationale[1631].

Lors des négociations relatives à la rédaction de la Convention, on s'est également posé la question de savoir si l'utilisation de cookies conduisait à des sanctions pénales basées sur l'article 3[1632]. Les rédacteurs ont souligné que les pratiques commerciales courantes (comme les cookies) n'étaient pas considérées comme des interceptions sans droit[1633].

Restrictions et réserves

L'article 3 offre la possibilité de limiter la criminalisation en demandant des éléments additionnels énumérés dans la deuxième phrase, y compris une « intention délictueuse » ou en relation avec un système informatique connecté à un autre système informatique.

Directive de l'Union européenne relative aux attaques contre les systèmes d'information

La directive de l'UE de 2013 relative aux attaques contre les systèmes d'information[1634] contient une disposition qui érige en infraction l'interception illégale (article 6).

> ***Article 6*** *– Interception illégale*
> *Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'interception, effectuée par des moyens techniques, de transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques, lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.*

Cette disposition est rédigée conformément aux normes définies dans la Convention du Conseil de l'Europe sur la cybercriminalité[1635], la principale différence tenant à la possibilité de restreindre ce principe aux cas non mineurs. Loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique. On trouve une approche similaire à la section 8 de la loi type du Commonwealth de 2002[1636].

> ***Interception illégale de données***
> ***8.*** *Une personne qui, intentionnellement, sans excuse ou justification légitimes, intercepte par des moyens techniques:*
> *(a) toute transmission non publique vers un système informatique, en provenance de ce dernier ou à l'intérieur de ce dernier; ou*
> *(b) des émissions électromagnétiques provenant d'un système informatique, qui transportent des données informatiques; commet une infraction passible, après déclaration de culpabilité, d'une peine de prison d'une durée d'une durée maximale [durée de la peine], ou d'une amende d'une durée maximale de [montant de l'amende], ou des deux.*

La Section 8 adopte une approche semblable à l'article 3 de la Convention du Conseil de l'Europe sur la cybercriminalité. Tout comme la Convention sur la cybercriminalité, cette disposition protège les données lors de processus de transmission non publics.

Projet de Convention internationale de Stanford

Le projet informel de Convention de Stanford de 1999 [1637] (le « Projet Stanford ») ne criminalise pas de manière explicite l'interception de données informatiques.

6.2.5 Atteinte à l'intégrité des données

La protection d'objets tangibles ou physiques contre l'endommagement intentionnel est un élément classique des législations pénales nationales. Avec la généralisation de la numérisation, davantage d'informations commerciales critiques sont stockées sous forme de données [1638]. Les attaques ou la tentative d'obtention de ces informations peuvent entraîner des pertes financières [1639]. Outre la suppression, l'altération de telles informations peut également avoir des conséquences majeures[1640]. Dans certains cas, les législations précédentes n'ont pas complètement aligné la protection des données sur la protection des objets tangibles. Cela permettait aux auteurs d'infractions de concevoir des escroqueries qui ne conduisent pas à des sanctions criminelles[1641].

Convention du Conseil de l'Europe sur la cybercriminalité

À l'article 4, la Convention sur la cybercriminalité inclut une disposition qui protège l'intégrité des données contre les brouillages non autorisés[1642]. L'objectif de cette disposition est de combler une lacune dans certaines lois pénales nationales et de fournir aux données informatiques et aux programmes informatiques les protections similaires à celles dont bénéficient les objets tangibles contre les dommages intentionnels[1643].

Disposition

Article 4 – Atteinte à l'intégrité des données
(1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.
(2) Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Les actes couverts

L'article 4 criminalise cinq types d'actes différents. Les termes « endommagement » et « détérioration » désignent tout acte lié à l'altération négative de l'intégrité du contenu informatif de données et de programmes[1644]. Le terme « effacement » désigne les actes par lesquels l'information est supprimée du support de stockage et sont jugés comparables à la destruction d'un objet tangible. Tout en proposant une définition, les rédacteurs de la Convention n'ont pas fait la différence entre les diverses méthodes de suppression de données[1645]. Jeter un fichier dans la poubelle virtuelle n'efface pas ce fichier du disque dur[1646]. Même lorsque l'on « vide » la poubelle, on n'efface pas nécessairement le fichier[1647]. Il n'est donc pas certain que la possibilité de récupérer un fichier effacé empêche l'application de cette disposition[1648]. Le terme « suppression » de données informatiques désigne une action qui affecte la disponibilité des données pour la personne ayant accès au support où l'information est stockée[1649]. L'application de ces dispositions fait particulièrement débat en ce qui concerne les attaques par déni de service[1650] [1651]. Pendant ce type d'attaques, les données fournies sur le système informatique visé ne sont plus disponibles pour l'utilisateur potentiel ni pour le propriétaire du système informatique[1652]. Le terme « altération » désigne la modification de données existantes, sans nécessairement diminuer leur disponibilité[1653]. Cet acte couvre notamment l'introduction de logiciels malveillants comme les logiciels espions, les virus ou les publiciels sur l'ordinateur de la victime[1654].

Élément moral

Comme toutes les autres infractions définies par la Convention sur la cybercriminalité, l'article 4 impose que l'auteur commette les infractions intentionnellement[1655]. La Convention ne contient pas de définition du terme « intentionnellement ». Dans le Rapport explicatif, les rédacteurs soulignent que la définition du terme « intentionnellement » devrait être donnée au niveau national[1656].

Sans droit

De même que pour les dispositions examinées ci-dessus, les actes doivent être commis « sans droit »[1657]. Le droit d'altérer des données a été examiné, en particulier dans le contexte du « remailer »[1658]. Les remailers sont utilisés pour modifier certaines données afin de faciliter l'anonymat des communications[1659]. Le Rapport explicatif mentionne qu'en principe ces actes sont considérés comme une protection légitime de la vie privée, et donc comme étant exécutés avec autorisation[1660].

Restrictions et réserves

L'article 4 donne la possibilité de limiter la criminalisation aux cas où un danger grave survient; c'est une approche similaire à la Décision-cadre du Conseil de l'UE sur les attaques contre des systèmes d'information[1661] qui permet aux États membres de limiter l'application de la disposition de fond de la législation pénale aux « cas qui ne sont pas mineurs »[1662].

Directive de l'Union européenne relative aux attaques contre les systèmes d'information

La directive de l'UE de 2013 relative aux attaques contre les systèmes d'information[1663] contient une disposition qui érige en infraction l'atteinte illégale à l'intégrité des données (article 5).

> ***Article 5*** *– Atteinte illégale à l'intégrité des données*
> *Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable le fait d'effacer, d'endommager, de détériorer, d'altérer, de supprimer ou de rendre inaccessibles des données informatiques d'un système d'information lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.*

Cette disposition est rédigée conformément aux normes définies dans la Convention du Conseil de l'Europe sur la cybercriminalité[1664], la principale différence tenant à la possibilité de restreindre ce principe aux cas non mineurs.

Loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique

On peut trouver une approche en accord avec l'article. 4 de la Convention sur la cybercriminalité à la section 8 de la loi type du Commonwealth de 2002[1665].

Disposition

> ***Atteinte à l'intégrité des données***
> ***6.***
> *(1) Toute personne qui, intentionnellement ou avec témérité, sans justification ou excuse légitime commet l'un des actes suivants:*
> *(a) détruit ou altère des données; ou*
> *(b) rend des données dénuées de sens, inutiles ou sans effet; ou*
> *(c) obstrue, interrompt ou interfère avec l'utilisation légitime de données; ou*
> *(d) obstrue, interrompt ou interfère avec toute personne dans l'utilisation légitime de données; ou*
> *(e) refuse l'accès à des données à des personnes habilitées à y accéder;*
> *commet une infraction passible, après déclaration de culpabilité, d'une peine de prison d'une durée maximale de [durée de la peine], ou une amende d'une durée maximale de [montant de l'amende], ou des deux.*
> *(2) La sous-section (1) est applicable, que l'infraction ait un effet temporaire ou permanent.*

La première différence essentielle entre la section 6 et la disposition correspondante de la Convention sur la cybercriminalité réside dans le fait que cette disposition du modèle de loi du Commonwealth criminalise, en plus des actes intentionnels, les actes commis par inadvertance. Contrairement à la section 6, trois autres dispositions du modèle de loi[1666], tout comme la Convention sur la cybercriminalité, limitent la

criminalisation aux actes intentionnels. La prise en compte de l'inadvertance élargit de manière significative cette approche, puisque même la suppression involontaire de fichiers sur un système informatique ou les dommages involontaires à un dispositif de stockage entraîneront des sanctions pénales.

La seconde différence réside dans le fait que les actes couverts par la section 6 diffèrent sensiblement par rapport à la disposition correspondante de la Convention sur la cybercriminalité. Enfin, cette disposition contient une clarification dans la sous-section 2 qui précise que les actes concernés ne doivent pas nécessairement produire un effet permanent, et que les effets temporaires sont également couverts.

Projet de Convention internationale de Stanford

Le projet informel de Convention de Stanford de 1999[1667] (le « Projet Stanford ») contient deux dispositions qui criminalisent les actes liés au brouillage de données informatiques.

Disposition

Art. 3
1. Les infractions au titre cette Convention sont commises si une personne s'engage de manière illégitime et intentionnelle dans l'une des actions suivantes sans autorisation, permission ou consentement reconnus légalement:

(a) crée, stocke, altère, efface, transmet, détourne, achemine incorrectement, manipule ou interfère avec des données ou des programmes dans un système cybernétique avec l'intention de perturber, ou sachant que de telles activités le feront, le fonctionnement prévu dudit système cybernétique ou d'un autre système cybernétique, ou d'exécuter des fonctions ou des activités non prévues par son propriétaire et jugées illégales au titre de cette Convention;

(b) crée, stocke, altère, efface, transmet, détourne, achemine incorrectement, manipule ou interfère avec des données dans un système cybernétique avec pour objet et effet de fournir de fausses informations afin de provoquer des dommages substantiels à des personnes ou des biens.

Les actes couverts

La différence principale entre la Convention sur la cybercriminalité, la loi type du Commonwealth d'une part, et l'approche du projet de Convention de Stanford d'autre part, réside dans le fait que ce dernier ne criminalise que des brouillages avec les données et si cela interfère avec le fonctionnement d'un système informatique (article 3, paragraphe 1a) ou si l'acte est commis dans le but de fournir de fausses informations afin de causer des dommages à des personnes ou à des biens (article 3, paragraphe 1b). Aussi, le projet de Convention de Stanford ne criminalise pas l'effacement d'un document de texte normal d'un dispositif de stockage de données lorsque cela n'a pas d'influence sur le fonctionnement d'un ordinateur ni ne fournit de fausses informations. La Convention sur la cybercriminalité et la loi type du Commonwealth suivent toutes deux une voie plus large en protégeant l'intégrité des données informatiques sans qu'il y ait obligatoirement d'autres effets.

6.2.6 Atteinte à l'intégrité du système

Les personnes ou les entreprises offrant des services basés sur les TIC dépendent du bon fonctionnement de leurs systèmes informatiques[1668]. Le manque de disponibilité de pages Internet qui sont victimes d'attaques par déni de service (DOS) [1669] démontre combien est sérieuse la menace de ces attaques[1670]. Des attaques de ce type peuvent entraîner de graves pertes financières et toucher les systèmes les plus puissants[1671]. Les entreprises ne sont pas les seules cibles. Dans le monde entier des experts discutent actuellement des scénarios possibles de cyberterrorisme qui prennent en compte des attaques contre des infrastructures critiques comme l'alimentation en énergie et les télécommunications[1672].

Convention du Conseil de l'Europe sur la cybercriminalité

Pour protéger l'accès des opérateurs et des utilisateurs aux TIC, la Convention sur la cybercriminalité inclut une disposition dans son article 5 qui criminalise l'entrave intentionnelle à l'utilisation légitime d'un système informatique[1673].

Disposition

> ***Article 5*** *– Atteinte à l'intégrité du système*
> *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration ou la suppression de données informatiques.*

Les actes couverts

L'application de cette disposition implique que le fonctionnement d'un système informatique ait été entravé[1674]. Le terme « entrave » se rapporte à des actions qui portent atteinte au bon fonctionnement du système informatique[1675]. L'application de cette disposition est limitée au cas où l'entrave est le résultat de l'une des actions mentionnées. En outre, la disposition prévoit que l'entrave doit être « sérieuse ». Il incombe aux parties concernées de déterminer les critères à remplir pour que l'entrave soit qualifiée de sérieuse[1676]. Des restrictions possibles en vertu du droit national peuvent inclure un niveau de dommage minimum, ainsi qu'une limitation de la criminalisation aux attaques contre des systèmes informatiques importants[1677].

La liste des actions par lesquelles le fonctionnement du système informatique a été influencé de manière négative est péremptoire[1678].

Le terme « introduction » n'est défini ni par la Convention elle-même ni par les rédacteurs de la Convention. Eu égard au fait que la transmission est mentionnée comme action additionnelle à l'article 5, le terme « introduction » pourrait être défini comme toute action liée à l'utilisation d'interfaces d'entrée physiques permettant le transfert d'informations vers un système informatique alors que le terme « transmission » couvre les actions associées à l'entrée à distance de données[1679].

«L'endommagement» et la «détérioration», en tant qu'actes se chevauchant, sont définis par les rédacteurs de la Convention sur la cybercriminalité dans le Rapport explicatif pour ce qui est de l'article 4. Ils concernent l'altération négative de l'intégrité ou du contenu informatif de données et de programmes.[1680]

Le terme « effacement » a également été défini par les rédacteurs de la Convention et du Rapport explicatif concernant l'article 4 comme une action où l'information est retirée du support de stockage[1681].

Le terme « altération » désigne la modification de données existantes, sans nécessairement diminuer la disponibilité des données[1682].

Le terme « suppression » de données informatiques désigne une action qui affecte de manière négative la disponibilité des données pour la personne qui a accès au support où l'information est stockée[1683].

Application de la disposition en ce qui concerne le spam

On s'est posé la question de savoir si le problème des spams[1684] pouvait être traité au titre de l'article 5, sachant que les spams peuvent surcharger les systèmes informatiques[1685]. Les rédacteurs ont affirmé que les spams ne conduisaient pas nécessairement à des entraves « sérieuses » et que « de tels comportements ne devraient être criminalisés que dans le cas d'une entrave intentionnelle et grave à la communication »[1686]. Les rédacteurs ont également noté que les parties peuvent avoir une conception différente de l'entrave dans leur droit interne[1687], par exemple, en faisant de certains actes d'ingérence, des infractions administratives ou en les rendant passibles d'une sanction[1688].

Élément moral

Comme toutes les autres infractions définies par le Convention sur la cybercriminalité, l'article 5 exige que l'auteur commette une infraction de façon intentionnelle[1689]. Cela inclut l'intention de commettre l'une des actions énumérées ainsi que l'intention d'entraver gravement le fonctionnement d'un système informatique.

La Convention ne contient pas de définition du terme « intentionnellement ». Dans le Rapport explicatif, les rédacteurs ont souligné que la définition du terme « intentionnellement » devait être laissée aux droits internes[1690].

Sans droit

L'action doit être exécutée « sans droit »[1691]. Comme cela a déjà été évoqué, les administrateurs de réseaux et les entreprises spécialisées dans la sécurité et chargées de tester la protection des systèmes informatiques se sont inquiétés de la criminalisation possible de leurs travaux[1692]. Ces professionnels travaillent avec l'autorisation du propriétaire et agissent donc dans la légalité. De plus, les rédacteurs de la Convention ont indiqué explicitement que les tests de sécurité d'un système informatique pratiqués avec l'autorisation du propriétaire ne se font pas sans droit[1693].

Restrictions et réserves

Contrairement aux articles 2 à 4, l'article 5 ne contient pas de possibilité explicite de restreindre l'application de cette disposition à la mise en œuvre dans le droit interne. Néanmoins, la responsabilité qu'ont les parties de définir la gravité de l'infraction leur donne la possibilité de restreindre son application. On peut trouver une approche similaire dans la Décision-cadre[1694] de l'Union européenne sur les attaques contre les systèmes d'information[1695].

Loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique

On peut trouver une approche en accord avec l'article 5 de la Convention sur la cybercriminalité à la section 7 de la loi type du Commonwealth de 2002.[1696]

Disposition

Atteinte à l'intégrité d'un système informatique
7.
(1) Toute personne qui intentionnellement ou avec témérité, sans justification ou excuse légitime:
(a) entrave ou interfère avec le fonctionnement d'un système informatique; ou
(b) entrave ou interfère avec une personne qui utilise ou fait fonctionner légitimement un système informatique;
commet une infraction passible, après déclaration de culpabilité, d'une peine de prison d'une durée maximale de [durée de la peine], ou d'une amende d'une durée maximale de [montant de l'amende], ou des deux.
A la sous-section (1), le terme "entrave", en relation avec un système informatique, inclut, mais sans s'y limiter les actes suivants:
(a) couper l'alimentation électrique d'un système informatique; et
(b) provoquer des brouillages électromagnétiques sur un système informatique; et
(c) altérer un système informatique par quelque moyen que ce soit; et
(d) introduire, effacer ou altérer des données informatiques;

La principale différence avec la disposition équivalente de la Convention du Conseil de l'Europe réside dans le fait que, sur la base de la section 7 de la loi type du Commonwealth, même les actions exécutées avec témérité sont criminalisées. Même une coupure involontaire de la fourniture d'électricité pendant les travaux de construction peu, par conséquent, aboutir à des sanctions pénales. En suivant cette voie, la loi type va même au-delà des exigences de la Convention sur la cybercriminalité. Une autre différence réside

dans le fait que la définition du terme « entrave » à la section 7 de la loi type du Commonwealth recouvre davantage d'actions par rapport à l'article 5 de la Convention sur la cybercriminalité.

Directive de l'Union européenne relative aux attaques contre les systèmes d'information

La directive de l'UE de 2013 relative aux attaques contre les systèmes d'information[1697] contient une disposition qui érige en infraction l'atteinte illégale à l'intégrité d'un système (article 4).

> ***Article 4 – Atteinte illégale à l'intégrité d'un système***
> *Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable le fait de provoquer une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, en transmettant, en endommageant, en effaçant, en détériorant, en altérant, en supprimant ou en rendant inaccessibles des données informatiques lorsque l'acte est commis de manière intentionnelle et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.*

Cette disposition est rédigée conformément aux normes définies dans la Convention du Conseil de l'Europe sur la cybercriminalité, la principale différence tenant à la possibilité de restreindre ce principe aux cas non mineurs. Cette approche est basée sur la Convention du Conseil de l'Europe sur la cybercriminalité. La première différence essentielle est que, outre les actes couverts par la Convention sur la cybercriminalité (introduction, transmission, endommagement, effacement, détérioration, altération et suppression), l'article 4 criminalise également l'entrave au fonctionnement d'un système d'information en rendant les données informatiques inaccessibles. Les données sont rendues inaccessibles si, en commettant cet acte, le délinquant empêche une personne d'accéder à ces données. Malgré la liste plus complexe des actes repris à l'article 4, il n'y a là encore aucune différence avec l'article correspondant de la Convention du Conseil de l'Europe sur la cybercriminalité dans la mesure où le fait de rendre des données inaccessibles est couvert par l'acte de suppression de données informatiques. La note explicative de la 19e ébauche de la Convention sur la cybercriminalité souligne que le groupe d'experts qui a rédigé la Convention est tombé d'accord sur la double signification du terme « suppression »: l'effacement de données qui, ainsi, n'existent plus physiquement, et le fait de rendre des données inaccessibles.[1698]

Projet de Convention internationale de Stanford

Le projet informel de Convention de Stanford de 1999[1699] (le « Projet Stanford ») contient deux dispositions qui criminalisent les actes liés aux brouillages de systèmes informatiques.

Disposition

> ***Art.3***
> *1. Des infractions au titre cette Convention sont commises si une personne s'engage de manière illégitime et intentionnelle dans l'une des actions suivantes sans autorisation, permission ou consentement reconnus légalement:*
>
> > *(a) crée, stocke, altère, efface, transmet, détourne, achemine incorrectement, manipule ou interfère avec des données ou des programmes dans un système cybernétique avec l'intention de perturber, ou sachant que de telles activités le feront, le fonctionnement prévu dudit système cybernétique ou d'un autre système cybernétique, ou d'exécuter des fonctions ou des activités non prévues par son propriétaire et jugées illégales au titre de cette Convention;*

Les actes couverts

La différence principale entre la Convention sur la cybercriminalité, la loi type du Commonwealth et l'approche du projet Stanford réside dans le fait que ce dernier couvre toutes les manipulations de systèmes informatiques alors que la Convention sur la cybercriminalité et la loi type du Commonwealth limitent la criminalisation à l'entrave au bon fonctionnement d'un système informatique.

6.2.7 Contenus érotiques ou pornographiques

La criminalisation et la gravité de la criminalisation de contenus illégaux et de contenus explicites sur le plan sexuel varient d'un pays à l'autre[1700]. Les Parties qui ont négocié la Convention sur la cybercriminalité se sont concentrées sur l'harmonisation des législations concernant la pédopornographie et ont exclu la criminalisation, au sens plus large, de contenus érotiques et pornographiques. Quelques pays ont traité ce problème en mettant en œuvre des dispositions qui criminalisent l'échange de contenus pornographiques par des systèmes informatiques. Toutefois, le manque de définition standard fait qu'il est difficile pour les agents chargés de faire appliquer la loi d'enquêter sur ces délits si les auteurs agissent à partir de pays qui n'ont pas criminalisé l'échange de contenus sexuels.[1701]

Exemples

La section 184 du Code pénal allemand est un exemple de criminalisation de l'échange de contenus pornographiques.

Section 184 Dissémination d'écrits pornographiques
(1) Quiconque, en relation avec des écrits pornographiques (Section 11 sous-section (3)):
1. offre, donne ou les rend accessible à une personne de moins de 18 ans;
2. affiche, adresse, présente ou par toute autre forme d'intervention les rend accessibles à des personnes de moins de 18 ans ou dans lequel elles peuvent les voir;
3. offre ou les donne à une autre personne dans le commerce de détail hors des locaux commerciaux, dans des kiosques ou autres points de vente dans lequel le client ne pénètre généralement pas, par l'intermédiaire d'une entreprise de vente par correspondance ou dans des bibliothèques de prêts commerciales ou des cercles de lecture;
3a. offre ou les donne à une autre personne par le biais d'une location commerciale ou d'une société d'abonnement commerciale comparable, à l'exception de magasins dont l'entrée est interdite aux personnes de moins de 18 ans et dans lesquels elles ne peuvent voir ces contenus;
4. entreprend de les importer par le biais d'une entreprise de vente par correspondance;
5. les offre, les annonce ou les recommande de manière publique dans un lieu dont l'entrée est autorisée aux personnes de moins de 18 ans ou dans lequel ils peuvent les voir ou par la diffusion d'écrits en dehors des transactions commerciales passant par les canaux normaux;
6. permet à une autre personne de les obtenir sans que cette dernière lui ait demandé;
7. les montre lors de projections publiques de films à titre de compensation demandée complètement ou de façon prédominante pour cette projection;
8. les produit, les obtient, les fournit, les stocke ou entreprend de les importer afin de les utiliser ou d'utiliser des copies réalisées à partir de ces contenus au sens des alinéas 1 à 7 ou de permettre cette utilisation par une autre personne; ou
9. s'engage à les exporter afin de les diffuser ou de diffuser des copies réalisées à partir de ces contenus à l'étranger en violation des dispositions pénales applicables dans ces pays ou de les rendre accessibles publiquement ou de permettre cette utilisation, sera puni d'une peine de prison d'une durée d'une durée maximale d'un an ou d'une amende.

Cette disposition repose sur le concept selon lequel le commerce et l'échange d'écrits pornographiques ne doivent pas être criminalisés si des mineurs ne sont pas impliqués[1702]. Sur cette base, la législation vise à protéger le développement harmonieux des mineurs[1703]. L'impact négatif éventuel de l'accès à la pornographie sur le développement des mineurs fait l'objet d'une controverse[1704]. L'échange d'écrits pornographiques entre adultes n'est pas pénalisé par la section 184. Le terme « écrits » couvre non seulement les écrits classiques, mais aussi les stockages numériques[1705]. De même, l'expression « les rendre accessibles » s'applique non seulement à des actions au-delà de l'Internet, mais couvre également des cas où les auteurs d'infractions déposent des contenus pornographiques sur des sites web où ils sont disponibles[1706].

Aux Philippines, la Section 4.C.1 du projet de loi N° 3777 de 2007 est un exemple d'une approche qui va au-delà et qui criminalise tout contenu sexuel[1707].

Section 4.C1.: *Infractions liées au cybersexe – Sans préjuger des poursuites au titre de la Loi de la République N° 9208 et de la Loi de la République N° 7710, quiconque qui d'une façon quelconque fait la publicité, encourage ou facilite le cybersexe par l'utilisation de technologies de l'information et de la communication comme les ordinateurs, les réseaux informatiques, la télévision, le satellite, le téléphone mobile, […], etc.*
Section 3i.: *Cybersexe ou sexe virtuel – ces expressions désignent toute forme d'activité ou d'éveil sexuels au moyen d'ordinateurs ou de réseaux de télécommunications.*

Cette disposition se conforme à une approche très large, car elle criminalise toute forme de publicité sexuelle ou d'encouragement à des activités sexuelles par l'Internet. Conformément au principe de la double incrimination[1708], les enquêtes internationales concernant de telles approches sont difficiles[1709].

6.2.8 Pédopornographie

L'Internet devient le principal instrument de commerce et d'échange de matériel contenant de la pédopornographie[1710]. Les principales raisons de ce développement sont la vitesse et l'efficacité de l'Internet en matière de transfert de fichiers, ses faibles coûts de production et de distribution et son anonymat ressenti[1711]. Dans le monde entier, des millions d'utilisateurs ont accès et peuvent télécharger les images postées sur une page Internet[1712]. L'une des raisons les plus importantes du succès des pages web offrant de la pornographie ou même de la pédopornographie tient au fait que les internautes se sentent moins observés lorsqu'ils sont assis chez eux et téléchargent du matériel à partir de l'Internet. À moins que les internautes utilisent des moyens de communication anonymes, leur impression de manque de traçabilité est fausse[1713]. Dans la plupart des cas, ils ne sont tout simplement pas conscients du sillage électronique qu'ils laissent derrière eux alors qu'ils naviguent sur l'Internet[1714].

Les dispositions visant à criminaliser la pornographie enfantine sont généralement conçues pour protéger des intérêts juridiques différents. La criminalisation de la production de pornographie enfantine vise à protéger l'enfant contre les abus sexuels.[1715] En ce qui concerne la prohibition des actes ayant trait à l'échange (offre, distribution) et la possession de pornographie enfantine, la criminalisation vise à détruire le marché, dans la mesure où la demande soutenue pour de nouveaux produits peut motiver les délinquants à continuer d'abuser des enfants.[1716] Par ailleurs, l'interdiction de l'échange vise à rendre l'accès à ces supports plus difficile et ainsi prévenir un effet déclencheur de l'abus sexuel d'enfants. Enfin, la criminalisation de la possession vise à empêcher les délinquants d'utiliser la pornographie enfantine pour séduire les enfants en vue de les entraîner dans des relations sexuelles.[1717]

Convention sur la cybercriminalité du Conseil de l'Europe

Afin d'améliorer et d'harmoniser la protection des enfants contre l'exploitation sexuelle[1718], cette Convention inclut un article qui traite de la pédopornographie.

Disposition

Article 9 *– Infractions se rapportant à la pédopornographie*
(1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a) la production de pédopornographie en vue de sa diffusion par le biais d'un système informatique;
b) l'offre ou la mise à disposition de pédopornographie par le biais d'un système informatique;
c) la diffusion ou la transmission de pédopornographie par le biais d'un système informatique;
d) le fait de se procurer ou de procurer à autrui de la pédopornographie par le biais d'un système informatique;
e) La possession de pédopornographie dans un système informatique ou un moyen de stockage de données informatiques.

(2) Aux fins du paragraphe 1 ci-dessus le terme "pédopornographie" comprend toute matière pornographique représentant de manière visuelle:

a) un mineur se livrant à un comportement sexuellement explicite;
b) une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;
c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.
(3) Aux fins du paragraphe 2 ci-dessus, le terme "mineur" désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.
(4) Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

La plupart des pays criminalisent déjà les abus envers les enfants ainsi que les méthodes classiques de distribution de matériels pédopornographiques[1719]. La Convention sur la cybercriminalité ne se limite donc pas à combler les lacunes des législations pénales nationales[1720] – elle cherche également à harmoniser les diverses règlementations[1721].

Les actes couverts

« Production » décrit tout processus de création de contenu pédopornographique. L'interprétation de ce terme fait l'objet d'un débat. Au Royaume-Uni, le téléchargement d'images de pornographie enfantine est considéré comme de la production (« fabrication ») de pornographie enfantine.[1722] La distinction entre « se procurer » et « produire » faite à l'article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité indique que le rédacteur de la Convention n'assimile pas le simple téléchargement de pornographie enfantine à de la production. Même sur la base de la distinction faite dans la Convention sur la cybercriminalité, cependant, une différentiation supplémentaire est nécessaire. Un délinquant/une délinquante qui prend des photos d'un enfant en train d'être abusé sexuellement produit de la pornographie enfantine; mais il/elle n'est pas sûr(e) qu'une personne qui utilise des images de pornographie enfantine pour les combiner dans une animation visuelle soit également productrice de pornographie enfantine. Bien que cette personne soit effectivement productrice de l'animation, l'applicabilité du terme « production » dans la Convention du Conseil de l'Europe sur la cybercriminalité, s'il s'agit de la documentation d'un cas réel d'abus sexuel d'enfants, reste incertaine. Le fait que la Convention sur la cybercriminalité vise à criminaliser la production de pornographie enfantine fictive — qui ne requiert pas l'abus sexuel réel d'un enfant — est un argument en faveur d'une interprétation large du terme « production ». D'autre part, le rapport explicatif de la Convention sur la cybercriminalité indique que la criminalisation de la production est nécessaire pour combattre le danger « à la source ».[1723] Bien que la Convention du Conseil de l'Europe sur la cybercriminalité ne précise pas cette intention des rédacteurs, le rapport explicatif de la Convention du Conseil de l'Europe sur la protection de l'enfant[1724] fournit une explication plus spécifique de la motivation des rédacteurs eu égard à une disposition similaire.[1725] Les rédacteurs de la Convention sur les droits de l'enfant ont souligné que la criminalisation de la production de pornographie enfantine est « nécessaire pour combattre les actes d'abus sexuels et l'exploitation à la source ». Cela peut être considéré comme un argument en faveur d'une approche plus restrictive.

Il est nécessaire que la production de pornographie enfantine soit réalisée en vue d'être distribuée par le biais d'un système informatique. Si le délinquant produit le contenu pour son usage personnel, ou envisage de le distribuer sous forme non électronique, l'article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité ne s'applique pas. L'auto description est un autre problème débattu dans le contexte de la production.[1726] Si le délinquant, à distance, convainc un enfant de prendre des photos pornographiques de lui-même/elle-même, cela peut, suivant la législation nationale, aboutir à criminaliser la victime (l'enfant) et non le délinquant.

« Offrir » couvre l'acte de solliciter d'autres personnes pour obtenir de la pornographie enfantine. Il n'est pas nécessaire que le support soit offert commercialement, mais cela implique que le délinquant qui offre le support soit capable de fournir.[1727] « Mettre à disposition » désigne un acte qui permet à d'autres utilisateurs d'accéder à de la pornographie enfantine. Cet acte peut être commis en hébergeant de la pornographie enfantine sur des sites Internet ou en se connectant à des systèmes de partage de fichiers et en permettant à d'autres personnes d'accéder à ces supports depuis des capacités de stockage ou des dossiers non verrouillés.

« Distribution » désigne la transmission active de pornographie enfantine à d'autres personnes. « Transmission » désigna toute communication par voie de signaux transmis. « Se procurer » pour soi-même ou pour d'autres couvre tous les actes visant à obtenir activement de la pornographie enfantine.

Enfin, l'article 9 criminalise la « possession » de pornographie enfantine. La criminalisation de la possession de pornographie enfantine diffère également suivant les systèmes juridiques nationaux.[1728] La demande de ces produits peut générer leur production en continu.[1729] Ainsi, la possession de ce genre de contenu peut encourager les abus sexuels sur les enfants. Les rédacteurs suggèrent donc que de rendre illégale la possession de contenu de pornographie enfantine est un moyen d'efficace de freiner la production.[1730] Cependant, la Convention permet aux parties, dans son paragraphe 4, d'exclure la criminalisation de la simple possession en limitant la responsabilité criminelle à la production, l'offre et la distribution de pornographie enfantine seulement.[1731] La possession implique le contrôle d'une personne qui s'adonne intentionnellement à la pornographie enfantine. Cela suppose que le délinquant/la délinquante dispose d'un contrôle, ce qui est le cas eu égard non seulement aux dispositifs de stockage locaux, mais également aux dispositifs de stockage accessibles et contrôlables par lui/elle. Par ailleurs, la possession en général suppose l'existence d'un élément moral comme indiqué dans la définition ci-dessus.

Pornographie enfantine

L'article 9, paragraphe 2, répartit en trois catégories les matières représentant des faits de pornographie enfantine de manière visuelle: un mineur se livrant à un comportement sexuellement explicite; une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite; et des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite. L'exigence d'une représentation visuelle exclut les fichiers sonores.

Bien que les rédacteurs se soient efforcés d'améliorer la protection des enfants contre l'exploitation sexuelle, les intérêts juridiques concernés par le paragraphe 2 sont plus larges. Le paragraphe 2.a, met directement l'accent sur la protection contre l'abus d'enfants. Les paragraphes 2.b et 2.c, ont trait aux images produites sans enfreindre les droits de l'enfant, ou en d'autres termes, créées au moyen de logiciels de modélisation en trois dimensions.[1732] La pornographie enfantine fictive est ainsi pénalisée parce que ces images peuvent, sans nécessairement nuire à un « enfant réel », être utilisées pour persuader des enfants de participer à des actes de ce type.[1733]

L'une des principales difficultés liées à cette définition tient à ce qu'elle s'articule autour de la représentation visuelle. Or, la pornographie enfantine n'est pas nécessairement diffusée sous forme d'images ou de séquences filmées, mais aussi sous forme de fichiers sonores.[1734] Étant donné que la formulation de l'article 9 désigne une « matière représentant de manière visuelle » un enfant, cette disposition ne s'applique pas aux fichiers sonores. En conséquence, les approches plus récentes telles que le texte législatif sur la cybercriminalité[1735] du projet HIPCAR[1736] adoptent une autre approche et évitent de mentionner la forme « visuelle ».

Définitions
3.
[…]
(4) On entend par pornographie enfantine toute matière pornographique qui décrit, présente ou représente:
(a) un enfant se livrant à un comportement sexuellement explicite;
(b) une personne qui apparaît comme un enfant se livrant à un comportement sexuellement explicite; ou
(c) des images représentant un enfant se livrant à un comportement sexuellement explicite;
y compris, sans limitation, toute matière pornographique sonore, visuelle ou textuelle.
Un pays ne peut limiter la pénalisation en n'appliquant pas les points (b) et (c).

Une autre définition plus large figure à l'article 2, paragraphe (c), du Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants.

Article 2
Aux fins du présent Protocole,
[…]
(c) On entend par pornographie mettant en scène des enfants toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles.

L'une des principales différences entre les législations nationales tient à l'âge de la personne impliquée. Certains pays définissent la notion de « mineur » dans leur droit national sur la pornographie enfantine comme toute personne de moins de 18 ans, conformément à la définition d'un « enfant » donnée à l'article 1 de la Convention des droits de l'enfant des Nations unies[1737]. D'autres définissent un mineur comme une personne de moins de 14 ans.[1738] Une approche similaire peut être observée dans la Décision-cadre du Conseil européen de 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie[1739] et dans la Convention du Conseil de l'Europe de 2007 sur la protection des enfants contre l'exploitation et les abus sexuels.[1740] Insistant sur l'importance d'une norme d'âge internationale uniforme, la Convention sur la cybercriminalité définit le terme « mineur » sur la base de la Convention des Nations unies.[1741] Eu égard toutefois aux écarts substantiels qui existent entre les différentes législations nationales, la Convention sur la cybercriminalité autorise les parties à exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans. Un problème qui soulève de plus en plus souvent la controverse a trait à la pénalisation potentiellement non souhaitée lorsque l'âge requis pour consentir à des relations sexuelles diffère de la limite d'âge de la définition.[1742] Si par exemple la pornographie enfantine est définie comme la représentation visuelle d'une activité sexuelle d'une personne de moins de 18 ans, et qu'en même temps, la majorité sexuelle est fixée à 16 ans, deux mineurs de 17 ans ont légalement le droit d'avoir une relation sexuelle, mais ils se rendent coupables d'une infraction grave (production de pornographie enfantine) s'ils photographient ou s'ils filment cet acte.[1743]

Élément moral

Comme pour toutes les autres infractions définies par la Convention du Conseil de l'Europe sur la cybercriminalité, l'article 9 exige que l'auteur commette intentionnellement les comportements concernés.[1744] Dans le Rapport explicatif, les rédacteurs ont expressément souligné que la Convention sur la cybercriminalité ne s'applique pas aux actes se rapportant à la pornographie enfantine survenus de façon non intentionnelle. L'absence d'intention peut spécialement être pertinente si le délinquant/la délinquante a ouvert fortuitement une page Internet contenant des images de pornographie enfantine et que certaines images ont été enregistrées dans des dossiers temporaires ou des fichiers du cache de son ordinateur bien qu'il/elle ait fermé immédiatement le site.

Sans droit

Les actes relevant de la pornographie enfantine peuvent uniquement être poursuivis au titre de l'article 9 de la Convention sur la cybercriminalité s'ils sont commis « sans droit ».[1745] Les rédacteurs de la Convention sur la cybercriminalité n'ont pas précisé plus en détail les circonstances dans lesquelles un utilisateur agit sans autorisation. D'une manière générale, un acte n'est pas commis « sans droit » seulement si un membre d'une institution de répression agit dans le cadre d'une enquête.

Convention du Conseil de l'Europe sur la protection des enfants

Une autre approche pour ériger en infraction pénale les actes se rapportant à la pornographie enfantine est exprimée à l'article 20 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.[1746]

Disposition

Article 20 *– Infractions se rapportant à la pédopornographie*
(1) Chaque Partie prend les mesures législatives ou autres nécessaires pour ériger en infraction pénale les comportements intentionnels suivants, lorsqu'ils sont commis sans droit:
a) la production de pédopornographie;
b) l'offre ou la mise à disposition de pédopornographie;
c) la diffusion ou la transmission de pédopornographie;
d) le fait de se procurer ou de procurer à autrui de la pédopornographie;
e) la possession de pédopornographie;
f) le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pédopornographie.
(2) Aux fins du présent article, l'expression "pédopornographie" désigne tout matériel représentant de manière visuelle un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles.
(3) Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1.a et e. à la production et à la possession:
– de matériel pornographique constitué exclusivement de représentations simulées ou d'images réalistes d'un enfant qui n'existe pas;
– de matériel pornographique impliquant des enfants ayant atteint l'âge fixé en application de l'Article 18, paragraphe 2, lorsque ces images sont produites et détenues par ceux-ci, avec leur accord et uniquement pour leur usage privé.
(4) Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1.f).

Actes couverts

La disposition s'appuie sur l'article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité, et par conséquent, elle est largement comparable à cette disposition.[1747] La principale différence tient à ce que la Convention sur la cybercriminalité met l'accent sur la pénalisation des actes liés aux services d'information et de communication (« la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique »), tandis que la Convention sur la protection des enfants adopte principalement une approche plus large (« la production de pornographie enfantine ») et inclut même les actes qui ne sont pas liés à un réseau informatique.

Nonobstant les similitudes dans les actes couverts, l'article 20 de la Convention sur la protection des enfants désigne un acte qui n'est pas visé dans la Convention sur la cybercriminalité. Aux termes de l'article 20, paragraphe 1.f, de la Convention sur la protection des enfants, le fait d'accéder à de la pornographie par le biais d'un ordinateur doit constituer une infraction pénale. L'accès inclut tout acte consistant à déclencher le processus d'affichage d'informations rendues disponibles par le biais des TIC. C'est le cas, par exemple, si le délinquant saisit le nom de domaine d'un site Internet dont il sait qu'il contient de la pornographie enfantine et qu'il déclenche le processus de réception des informations de la première page qui implique un processus obligatoire de téléchargement automatique. Les institutions de répression peuvent ainsi poursuivre un délinquant si elles peuvent prouver qu'il a ouvert des sites contenant de la pornographie enfantine même si elles ne peuvent pas prouver qu'il a téléchargé du matériel. De telles difficultés se posent pour réunir des preuves, par exemple, si le délinquant utilise une technologie de codage pour protéger les fichiers téléchargés sur son support d'enregistrement.[1748] Le Rapport explicatif sur la Convention sur la protection des enfants fait remarquer que la disposition doit également pouvoir s'appliquer aux cas dans lesquels le délinquant se contente de regarder des images de pornographie enfantine sans les télécharger.[1749] En général, l'ouverture d'un site web déclenche automatiquement un processus de téléchargement – souvent, sans même que l'utilisateur le sache.[1750] Le cas cité dans le Rapport explicatif n'est donc pertinent que lorsqu'un téléchargement n'est pas exécuté en arrière-plan. Il s'applique toutefois également lorsque la consommation de pornographie enfantine peut être réalisée sans télécharger de matériel. Cela peut se produire, par exemple, si le site web permet la lecture de vidéos en continu, et qu'en raison de la configuration technique du processus de lecture, il ne met pas les informations reçues en

tampon mais les élimine immédiatement après la transmission (p. ex. si le délinquant utilise la lecture de vidéo en continu).

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique

Une approche similaire à l'article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité est inscrite à la section 10 de la Loi-type de 2002 du Commonwealth.[1751]

Pédopornographie

10*(1) Toute personne qui commet intentionnellement l'un quelconque des actes suivants:*

(a) publier de la pornographie enfantine par le biais d'un système informatique; ou

(b) produire de la pornographie enfantine aux fins de sa publication par le biais d'un système informatique; ou

(c) détenir de la pornographie enfantine dans un système informatique ou sur un support d'enregistrement de données informatique; si elle est jugée coupable, est passible d'une peine de prison d'une durée maximale de [durée de la peine] ou d'une amende maximale de [montant] ou des deux.[1752]

(2) Une justification peut être apportée à une accusation relative à une infraction au sens du paragraphe (1), point (a) ou (c) si la personne concernée apporte la preuve que la pornographie enfantine était destinée à une finalité scientifique, de recherche, médicale ou de répression de bonne foi.[1753]

(3) Au sens de la présente section:

On entend par « pornographie enfantine » toute matière qui représente de manière visuelle:

(a) un mineur se livrant à un comportement sexuellement explicite; ou

(b) une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite; ou

(c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

On entend par « mineur » une personne de moins de [x] ans.

L'acte de « publier » inclut:

(a) le fait de distribuer, transmettre, diffuser, faire circuler, fournir, exhiber, prêter pour en obtenir un bénéfice, échanger, troquer, vendre ou proposer à la vente, louer ou proposer à la location, donner de toute autre manière ou rendre accessible de quelque manière que ce soit; ou

(b) le fait d'avoir en sa possession, sous sa garde ou sous son contrôle aux fins de réaliser un acte visé au point (a); ou

(c) le fait d'imprimer, photographier, copier ou fabriquer de toute autre manière (d'une espèce ou d'une nature similaire ou différente) aux fins de réaliser un acte visé au point (a).

La principale différence avec la Convention du Conseil de l'Europe sur la cybercriminalité tient à ce que la Loi-type du Commonwealth ne définit pas strictement le terme « mineur » et laisse le soin aux États membres d'établir la limite d'âge. À l'instar de la Convention du Conseil de l'Europe sur la cybercriminalité, la Loi-type du Commonwealth ne prévoit pas la pénalisation de l'accès à de la pornographie enfantine par le biais des technologies de l'information.

Protocole facultatif à la Convention des Nations unies relative aux droits de l'enfant

Une approche neutre en termes technologiques est utilisée à l'article 3 du Protocole facultatif concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants.

Article 3

1. Chaque État Partie veille à ce que, au minimum, les actes et activités suivants soient pleinement couverts par son droit pénal, que ces infractions soient commises au plan interne ou transnational, par un individu ou de façon organisée:

[...]

(c) Le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de vendre ou de détenir aux fins susmentionnées, des matériels pornographiques mettant en scène des enfants, tels que définis à l'article 2.

[...]

Bien que le Protocole facultatif ne mentionne pas expressément le rôle de l'internet dans la diffusion de ces matériels[1754], il pénalise les actes ayant trait à la pornographie enfantine dans une formulation neutre sur le plan des technologies employées. La pornographie mettant en scène des enfants est définie comme étant toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles.[1755] Les actes visés sont comparables à ceux faisant l'objet de la Convention sur la cybercriminalité, excepté que l'article 3 a été rédigé dans un souci de neutralité technologique.

Projet de convention internationale de Stanford

Le Projet informel[1756] de Convention internationale de Stanford de 1999 (ci-après le « Projet de Stanford ») ne contient pas de dispositions pénalisant l'échange de pornographie enfantine par le biais de systèmes informatiques. Ses rédacteurs ont affirmé qu'en règle générale, aucun type de discours ou de publication ne doit faire l'objet d'un traitement pénal aux termes du Projet de Stanford.[1757] Ayant constaté que différentes approches nationales se côtoyaient, les rédacteurs du Projet de Stanford ont attribué aux États le pouvoir de décider de cet aspect de la pénalisation.[1758]

6.2.9 Sollicitation d'enfants

L'internet permet de communiquer avec d'autres personnes sans divulguer son âge ou son sexe. Un délinquant peut abuser de cette possibilité pour solliciter des enfants.[1759] Ce phénomène est appelé couramment la « prédation ».[1760] Certains ordres juridiques régionaux comprennent des dispositions qui pénalisent une telle prise de contact.

Convention du Conseil de l'Europe sur la protection des enfants

Un exemple réside à l'article 23 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.[1761]

> ***Article 23*** *– Sollicitation d'enfants à des fins sexuelles*
> *Chaque Partie prend les mesures législatives ou autres nécessaires pour ériger en infraction pénale le fait pour un adulte de proposer intentionnellement, par le biais des technologies de l'information et de la communication, une rencontre à un enfant n'ayant pas atteint l'âge fixé en application de l'article 18, paragraphe 2, dans le but de commettre à son encontre une infraction établie conformément aux articles 18, paragraphe 1.a, ou 20, paragraphe 1.a, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre.*

La sollicitation d'un enfant dans le but d'abuser sexuellement de cet enfant ne tombe généralement pas dans le champ d'application des dispositions pénalisant l'abus sexuel des enfants dans la mesure où la sollicitation est assimilée à un acte préparatoire. Eu égard au débat croissant sur la prédation en ligne, les rédacteurs de la Convention ont décidé d'ajouter l'article 23 afin qu'un acte préparatoire soit déjà constitutif d'une infraction pénale.[1762] Afin d'éviter une pénalisation excessive, ils ont néanmoins précisé qu'une simple conversation d'ordre sexuel avec un enfant ne doit pas être jugée suffisante pour la commission de l'acte de sollicitation, bien qu'elle puisse faire partie de la préparation d'un abus sexuel.[1763]

Cette approche entraîne deux problèmes principaux. Premièrement, la disposition porte uniquement sur la sollicitation par le biais des TIC, excluant de fait toute autre forme de sollicitation. Les rédacteurs ont affirmé qu'il était justifié de mettre l'accent sur ces technologies car elles sont difficiles à contrôler.[1764] Aucune donnée fiable en termes scientifiques n'a toutefois été fournie pour démontrer que la sollicitation d'enfants se résume à un problème en ligne. Il existe en outre de bonnes raisons non seulement pour éviter une situation dans laquelle un acte qui est illégal lorsqu'il est commis dans le monde réel est légal lorsqu'il est commis en ligne, mais aussi, à l'inverse, pour veiller à ne pas pénaliser un comportement en ligne lorsqu'il est légal dans le monde réel. La Déclaration conjointe de 2001 sur les défis de la liberté d'expression à l'ère nouvelle, par exemple, indique que les États ne devraient pas adopter de règles distinctes limitant le contenu sur l'internet.[1765]

Un autre problème inhérent à la pénalisation de cet acte préparatoire tient à ce qu'elle pourrait donner lieu à des conflits dans le système du droit pénal dans la mesure où la préparation d'actes encore plus graves n'est pas une infraction. L'ordre des valeurs d'un pays serait remis en question si la préparation de l'abus sexuel d'un enfant était érigée en infraction pénale alors que la préparation du meurtre d'un enfant ne l'est pas. Une approche de ce type doit donc être formulée sur la base d'un examen approfondi des avantages et des risques liés à la pénalisation d'un acte préparatoire.

6.2.10 Discours haineux et racisme

Le degré de pénalisation d'un discours haineux atteste de profondes disparités.[1766] Dans les pays dotés d'une forte protection constitutionnelle de la liberté d'expression[1767], en particulier, un discours haineux n'est généralement pas une infraction pénale. Une interdiction peut spécialement être observée en Afrique et en Europe.[1768]

Convention du Conseil de l'Europe sur la cybercriminalité (protocole additionnel)

Le Conseil de l'Europe joue un rôle actif dans la lutte contre le racisme, et à l'issue de Sommet de Vienne de 1993, il a adopté une Déclaration et un Plan d'action sur la lutte contre le racisme, la xénophobie, l'antisémitisme et l'intolérance.[1769] En 1995, le Conseil de l'Europe a ensuite adopté des recommandations sur la lutte contre le racisme.[1770] Au cours des négociations relatives à la Convention du Conseil de l'Europe sur la cybercriminalité, la pénalisation des discours haineux en ligne a été abordée. Étant donné que les parties négociatrices n'ont pas réussi à s'accorder[1771] sur une position commune sur la pénalisation du discours haineux et du matériel xénophobe, les dispositions concernant ces infractions ont été intégrées dans un premier Protocole à la Convention.[1772] L'une des principales difficultés des dispositions érigeant le matériel xénophobe en infraction pénale consiste à trouver un équilibre entre la protection de la liberté d'expression[1773], d'une part, et la prévention de l'atteinte aux droits de personnes ou de groupes, d'autre part. Sans s'attarder sur les détails, les difficultés rencontrées lors de la négociation de la Convention du Conseil de l'Europe sur la cybercriminalité[1774] et l'état d'avancement des signatures/des ratifications du Protocole additionnel [1775] démontrent bien que la portée différente de la protection de la liberté d'expression entrave le processus d'harmonisation. [1776] En ce qui concerne en particulier le principe commun de la double incrimination[1777], l'absence d'harmonisation entraîne des difficultés de répression dans les affaires ayant une dimension internationale.[1778]

Disposition

Article 3 – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe.
2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles.
3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.
Article 4 – Menace avec une motivation raciste et xénophobe
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant:

La menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 5 – Insulte avec une motivation raciste et xénophobe

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant:

l'insulte en public, par le biais d'un système informatique, (i) d'une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques.

2. Une Partie peut:

a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule;

b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

Article 6 – Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité

1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants:

la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale ou définitive du Tribunal militaire international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.

2. Une Partie peut:

a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments;

b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

Actes couverts

L'article 3 pénalise la diffusion et la mise à disposition au public intentionnelles de matériel xénophobe par le biais d'un système informatique.[1779] En conséquence, les modes de diffusion traditionnels qui n'impliquent pas de système informatique (comme les livres et les périodiques) ne sont pas couverts. D'après la définition énoncée à l'article 2, un matériel raciste et xénophobe désigne tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes. La « diffusion » désigne la diffusion active de matériel.[1780] La « mise à disposition au public » signifie l'acte de mettre un matériel en ligne[1781] et nécessite que des utilisateurs puissent accéder à ce matériel. Cet acte peut être commis en publiant le matériel sur un site web ou en se connectant à un système de partage de fichiers et en permettant à d'autres personnes d'accéder au matériel dans des instruments ou des dossiers d'enregistrement non bloqués. Le Rapport explicatif souligne que la création ou la compilation d'hyperliens doit également être englobée.[1782] Étant donné qu'un hyperlien sert uniquement à faciliter l'accès à un matériel, une telle interprétation dépasse le texte de la disposition. La diffusion inclut toute action consistant à transmettre un matériel raciste ou xénophobe à d'autres personnes. L'incrimination nécessite

en outre que la diffusion et la mise à disposition comprennent une interaction avec le public, excluant ainsi la communication privée.[1783]

L'article 6 utilise une approche similaire à l'article 3, en incriminant la diffusion ou la mise à disposition du public, par le biais d'un système informatique,[1784] de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.

L'article 4 incrimine la menace, par le biais d'un système informatique, de commettre une infraction pénale grave envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou par la religion, ou envers un groupe de personnes qui se distingue par une de ces caractéristiques. Il se réfère à une menace qui provoque la crainte chez la personne envers laquelle elle est dirigée qu'elle risque d'être victime d'une infraction pénale grave.[1785] À la différence de l'article 3, la notion de « menace » ne nécessite pas d'interaction avec le public et englobe donc également l'envoi de messages électroniques à la victime.

L'article 5 adopte une approche similaire à l'article 4, en incriminant l'insulte d'une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion si cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou d'un groupe de personnes qui se distingue par une de ces caractéristiques. L'« insulte » se réfère à toute expression outrageante ou invective qui porte atteinte à la dignité d'une personne et qui est directement liée à l'appartenance à un groupe de la personne insultée. Afin d'éviter un conflit avec la liberté d'expression[1786], une définition stricte doit être donnée à l'acte d'insulte. La principale différence entre les articles 4 et 5 tient à ce que cette disposition s'applique uniquement à l'insulte publique et exclut donc les communications privées (comme le courrier électronique).[1787]

Projet de convention internationale de Stanford

Le Projet informel[1788] de Convention internationale de Stanford de 1999 (ci-après le « Projet de Stanford ») ne comprend pas de disposition incriminant le discours haineux. Ses rédacteurs ont affirmé qu'en règle générale, aucun type de discours ou de publication ne doit faire l'objet d'un traitement pénal aux termes du Projet de Stanford.[1789] Ayant constaté que différentes approches nationales se côtoyaient, les rédacteurs du Projet de Stanford ont attribué aux États le pouvoir de décider de cet aspect de la pénalisation.[1790]

6.2.11 Infractions religieuses

Le degré de protection des religions et de leurs symboles fluctue d'un pays à l'autre.[1791] Plusieurs préoccupations sont exprimées à propos de l'incrimination des infractions de ce type. Le Rapporteur spécial des Nations unies pour la liberté d'opinion et d'expression, le Représentant de l'OSCE pour la liberté des médias et le Rapporteur spécial de l'OEA pour la liberté d'expression ont affirmé dans leur Déclaration conjointe de 2006 que « dans de nombreux pays, les autorités font un usage abusif des règles excessives adoptées en la matière pour limiter les prises de position non traditionnelles, discordantes, critiques ou minoritaires ou étouffer les débats sur les défis sociaux difficiles ».[1792] Dans leur Déclaration conjointe de 2008, ils ont en outre souligné que les organisations internationales, y compris l'Assemblée générale des Nations unies et le Conseil des droits de l'homme, devaient s'abstenir d'adopter de nouvelles déclarations soutenant l'idée d'ériger en infraction pénale la diffamation d'une religion.

Convention du Conseil de l'Europe sur la cybercriminalité (protocole additionnel)

Les négociations sur ce sujet parmi les parties à la Convention sur la cybercriminalité se sont heurtées aux mêmes difficultés qu'au sujet du matériel xénophobe.[1793] Les pays qui ont négocié le texte du Premier protocole additionnel à la Convention sur la cybercriminalité se sont néanmoins accordés pour ajouter la religion parmi les éléments de la protection dans deux dispositions.

Dispositions

Article 4 – Menace avec une motivation raciste et xénophobe
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant:
La menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques.
Article 5 – Insulte avec une motivation raciste et xénophobe
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant: l'insulte en public, par le biais d'un système informatique, (i) d'une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques.
[…]

Bien que ces deux dispositions traitent la religion comme une caractéristique, elles ne protègent pas la religion ou les symboles religieux par le biais d'une incrimination, mais elles érigent en infraction pénale les menaces et les insultes envers une personne en raison de son appartenance à un groupe.

Exemples de législations nationales

Certains pays dépassent cette approche et pénalisent également les actes se rapportant à des aspects religieux. Les sections 295B et 295C du Code pénal pakistanais peuvent être citées à titre d'exemples.

***295-B**. Profanation, etc. du Saint Coran: quiconque profane, endommage ou désacralise intentionnellement un exemplaire du Saint Coran ou un extrait ou l'utilise de manière à le discréditer ou dans un autre but illicite sera passible d'une peine de prison à perpétuité.*
***295-C**. L'usage de remarques visant à discréditer, etc. le Prophète: quiconque, au moyen de mots verbaux ou écrits, ou au moyen d'une représentation visible ou d'une imputation, innuendo, ou d'une insinuation, directe ou indirecte, profane le nom sacré du Prophète Mahomet (que la paix soit avec lui) sera condamné à la peine de mort ou à une peine de prison à perpétuité et sera également passible d'une amende.*

Eu égard aux incertitudes qui entouraient l'application de ces dispositions, le projet de loi de 2006 du Pakistan sur la criminalité électronique comprenait deux dispositions consacrées aux infractions liées à l'internet,[1794] mais ces dispositions ont été supprimées lorsque le projet a été déposé une nouvelle fois, en 2007, sous la forme de la loi sur la prévention de la criminalité électronique,[1795] qui a été proclamée en décembre 2007.[1796]

***20. Profanation, etc. d'un exemplaire du Saint Coran** – Quiconque, utilisant un système électronique ou un dispositif électronique profane, endommage ou désacralise intentionnellement un exemplaire du Saint Coran ou un extrait ou l'utilise de manière à le discréditer ou pour tout objectif illicite sera passible d'une peine de prison à perpétuité.*
***21. Utilisation de remarques visant à discréditer, etc. concernant le Saint Prophète** – Quiconque, utilisant un système électronique ou un dispositif électronique, au moyen de mots, verbaux ou écrits, ou au moyen d'une représentation visible ou d'une imputation, innuendo, ou d'une insinuation, directe ou indirecte, profane le nom sacré du Prophète Mahomet (que la paix soit avec lui) sera condamné à la peine de mort ou à une peine de prison à perpétuité et sera également passible d'une amende.*

S'agissant des dispositions incriminant la diffusion de matériel xénophobe sur l'internet, l'une des principales difficultés des approches globales incriminant les infractions religieuses a trait au principe de la liberté d'expression.[1797] Ainsi que cela a été évoqué plus haut, les degrés divers de protection de la liberté d'expression constituent un obstacle au processus d'harmonisation.[1798] En ce qui concerne en particulier le principe commun de la double incrimination[1799], l'absence d'harmonisation entraîne des difficultés de répression dans les affaires ayant une dimension internationale.[1800]

6.2.12 Jeux de hasard illégaux

Le nombre croissant de sites web proposant des jeux de hasard illégaux suscite l'inquiétude[1801] car ces sites peuvent être utilisés pour contourner l'interdiction des jeux de hasard qui prévaut dans certains pays.[1802] Si ces sites sont gérés depuis un endroit où les jeux de hasard en ligne ne sont pas interdits, il est difficile pour les pays réprimant l'exploitation de jeux de hasard sur l'internet d'empêcher leurs citoyens d'utiliser ces services.[1803]

Exemple de législation nationale

La Convention du Conseil de l'Europe sur la cybercriminalité ne contient pas d'interdiction des jeux de hasard en ligne. Un exemple d'approche nationale à ce sujet réside dans la section 284 du Code pénal allemand:

Exemple

Section 284 Organisation non autorisée d'un jeu de hasard
(1) Quiconque, sans la permission d'une autorité publique, organise publiquement ou propose un jeu de hasard ou met à disposition l'équipement nécessaire, est passible d'une peine de prison d'une durée maximale de deux ans ou d'une amende.
(2) Les jeux de hasard, en club ou en réunion privée dans lesquels les jeux de hasard sont régulièrement organisés, sont qualifiés de jeux organisés publiquement.
(3) Quiconque, dans les cas mentionnés à la sous-section (1) agit:
1. professionnellement; ou
2. en tant que membre d'un groupe qui s'est constitué pour commettre en permanence de tels actes, sera passible d'une peine de prison de trois mois à cinq ans.
(4) Quiconque recrute pour un jeu de hasard public (sous-section (1) et (2)), sera passible d'une peine d'une durée maximale d'un an ou d'une amende.

Cette disposition est destinée à limiter les risques d'addiction[1804] aux jeux de hasard en définissant des procédures applicables à l'organisation de tels jeux.[1805] Elle ne met pas expressément l'accent sur les jeux de hasard sur l'internet, mais elle les inclut également.[1806] Elle pénalise ainsi l'exploitation de jeux de hasard illégaux sans l'autorisation des pouvoirs publics compétents. De plus, elle pénalise toute personne qui met (intentionnellement) à disposition un équipement qui est ensuite utilisé pour pratiquer des jeux de hasard.[1807] Cette pénalisation excède les conséquences de l'aide et de l'incitation dès lors que les délinquants sont passibles de peines plus lourdes.[1808]

Afin d'éviter une enquête pénale, l'exploitant de sites web de jeux de hasard illégaux peut déplacer physiquement ses activités[1809] dans un pays qui ne réprime pas les jeux de hasard illégaux.[1810] Une telle délocalisation pose un problème aux institutions de répression car le fait qu'un serveur soit installé en dehors du territoire d'un pays[1811] n'affecte généralement pas les possibilités d'y accéder pour les utilisateurs situés dans le pays.[1812] Afin d'améliorer la capacité des institutions de répression à lutter contre les jeux de hasard illégaux, le législateur allemand a donc étendu la pénalisation aux utilisateurs.[1813] Aux termes de la section 285, les institutions de répression peuvent ainsi poursuivre les utilisateurs qui participent à des jeux de hasard illégaux et diligenter une enquête même si les exploitants de jeux de hasard ne peuvent être traduits en justice s'ils sont installés en dehors de l'Allemagne.

Section 285 Participation à un jeu de hasard non autorisé
Quiconque participe à un jeu de hasard public (Section 284) est passible d'une peine de prison d'une durée maximale de six mois ou d'une amende ne dépassant pas 180 montants quotidiens.

Si des délinquants utilisent des sites de jeux de hasard à des fins de blanchiment de capitaux, il est souvent difficile de les identifier.[1814] Un exemple d'approche[1815] appliquée pour prévenir les jeux de hasard illégaux et le blanchiment de capitaux réside dans la Loi de 2005 des États-Unis sanctionnant les jeux de hasard illégaux sur l'internet.[1816]

§ 5363. Interdiction de l'acceptation de tout instrument financier en vue de jeux illégaux sur Internet
Quiconque est engagé dans une activité de pari ou de spéculation ne peut accepter en toute connaissance de cause ce qui suit, en rapport avec la participation d'une autre personne à des jeux illégaux sur Internet
(1) crédits, ou produits de crédit, au profit ou pour le compte de telle autre personne (y compris le crédit élargi par l'utilisation d'une carte de crédit);
(2) transfert de fonds électroniques, ou fonds transmis par ou à travers une activité de transfert d'argent, ou les produits d'un transfert de fonds électronique ou d'un service de transfert d'argent, de ou pour le compte de ladite autre personne;
(3) tout chèque, traite ou instrument similaire tiré par ou pour le compte de ladite autre personne et qui est tiré sur ou payable ou à travers une institution financière quelconque; ou
(4) produits de toute autre forme de transaction financière, comme le Secrétaire peut le prescrire par réglementation, qui implique une institution financière en tant que débiteur ou intermédiaire financier pour le compte de ou pour le bénéfice de ladite autre personne.
§ 5364. Politiques et procédures visant à identifier et à empêcher les transactions restreintes
a) Avant la fin de période de 270 jours commençant à la date de la mise en vigueur de ce sous-chapitre, le Secrétaire, en consultation avec le Conseil des gouverneurs de la réserve fédérale et l'Avocat général, prescrira des règlementations demandant à chaque système de paiement désigné, et à tous les participants à l'intérieur de ce système, d'identifier et d'empêcher les transactions restreintes par l'établissement de politiques et de procédures raisonnablement conçues pour identifier et empêcher les transactions restreintes de la façon suivante:
1) Elaboration de politiques et de procédures qui:
a) autorisent le système de paiement où toute personne impliquée dans le système de paiement à identifier les transactions restreintes au moyen de codes dans des messages d'autorisation ou par d'autres moyens;
b) bloquent les transactions restreintes identifiées à la suite des politiques et procédures élaborées conformément au sous-paragraphe (a).
2) Etablissement de politiques et procédures visant à empêcher l'acceptation des produits ou des services du système de paiement en rapport avec une transaction restreinte.
b) en prescrivant des règlementations au titre de la sous-section (a) le Secrétaire:
1) définira les types de politiques et procédures, y compris des exemples non exclusifs, qui seraient jugés applicables, élaborés de manière raisonnable de façon à identifier, bloquer ou empêcher l'acceptation de produits ou services par rapport à chaque type de transaction restreinte;
2) dans la mesure où cela est pratique, autoriser tout participant à un système de paiement de choisir entre d'autres moyens d'identification et de blocage ou empêcher par un autre moyen l'acceptation de produits ou de services du système de paiement ou du participant en ce qui concerne les transactions restreintes; et
3) envisager d'exempter les transactions réduites de toutes exigences imposées au titre de telles règlementations, si le Secrétaire estime qu'il n'est ni pratique ni raisonnable d'identifier et de bloquer ou de toute autre façon empêcher de telles transactions.
c) Un fournisseur de transactions financières sera considéré comme étant en conformité avec les règlementations prescrites au titre de la sous-section (a), si
1) cette personne s'appuie et se conforme aux politiques et procédures d'un système de paiement désigné dont il est membre ou participant pour
a) identifier et bloquer les transactions restreintes; ou

b) d'une autre manière, empêcher l'acceptation des produits ou services du système de paiement, de membres, ou de participants en rapport avec des transactions restreintes; et

2) de telles politiques et procédures du système de paiement désigné sont conformes aux exigences des règlementations prescrites au titre de la sous-section (a).

d) Quiconque est soumis à une réglementation prescrite ou un ordre lancé au titre de ce sous-chapitre et qui bloque, ou refuse d'honorer une transaction

1) qui est une transaction restreinte;

2) qu'une telle personne estime de manière raisonnable être une transaction restreinte; ou

3) en tant que membre d'un système de paiement désigné en accord avec les politiques et procédures du système de paiement, dans un effort visant à se conformer aux règlementations prescrites au titre de la sous-section (a) ne sera pas responsable auprès d'une Partie quelconque pour une telle action.

e) Les exigences de cette section seront applicables exclusivement par les régulateurs fonctionnels fédéraux et par la Commission commerciale fédérale, comme il est prévu à la section 505(a) de la loi Gramm-Leach-Bliley.

5366. Sanctions pénales

a) Quiconque viole la section 5363 est passible d'une amende conformément au titre 18, ou d'une peine de prison d'une durée maximale de cinq ans, ou les deux.

b) Après condamnation d'une personne au titre de cette section, le tribunal peut adresser une injonction permanente prohibitive pour telle personne de placer, recevoir ou autrement de faire des paris et des spéculations ou d'envoyer, recevoir ou inviter des informations l'aidant à placer les paris ou spéculations.

Cette loi a pour objectif d'aborder les enjeux et les risques des jeux de hasard (transfrontaliers) sur l'internet.[1817] Elle se compose de deux principes importants. Premièrement, elle interdit l'acceptation de tout instrument financier en vue de jeux de hasard illégaux sur l'internet par toute personne engagée dans une activité de pari ou de spéculation. Cette disposition ne régit pas les actes réalisés par les utilisateurs de sites de jeux de hasard sur l'internet ou les institutions financières.[1818] Une infraction à cette disposition peut donner lieu à une sanction pénale.[1819] Deuxièmement, elle demande au Secrétaire du Trésor et au Conseil des gouverneurs de la Réserve fédérale de prescrire des réglementations imposant aux participants à un système de paiement d'identifier et d'empêcher les transactions restreintes se rapportant à des jeux de hasard illégaux sur l'internet par le biais de politiques et de procédures raisonnables. Cette deuxième disposition ne s'applique pas seulement aux personnes engagées dans une activité de pari ou de spéculation, mais à l'ensemble des institutions financières. À la différence des personnes engagées dans une activité de pari ou de spéculation qui acceptent des instruments financiers à des fins de jeux de hasard illégaux sur l'internet, les institutions financières n'assument généralement pas de responsabilité pénale. S'agissant de l'effet international de cette loi, les conflits potentiels avec l'Accord général sur le commerce des services (GATS)[1820] font actuellement l'objet d'un examen.[1821]

6.2.13 Calomnie et diffamation

La calomnie et la publication de fausses informations ne sont pas des actes commis uniquement sur les réseaux informatiques. Ainsi que cela a déjà été évoqué, toutefois, la possibilité de communication anonyme [1822] et les difficultés logistiques liées à l'immense quantité d'informations disponibles sur l'internet[1823] constituent des facteurs abstraits qui facilitent ces actes. La question de savoir si la diffamation doit être érigée en infraction pénale est sujette à la controverse.[1824] Les préoccupations relatives à la pénalisation de la diffamation se rapportent principalement au conflit potentiel avec le principe de la liberté d'expression. Plusieurs organisations ont donc appelé au remplacement des lois pénales sur la diffamation.[1825] Le Rapporteur spécial des Nations unies pour la liberté d'opinion et d'expression et le Représentant de l'OSCE pour la liberté des médias ont déclaré: "La diffamation pénale n'est pas une restriction justifiable sur la liberté d'expression; toutes les lois pénales sur la diffamation devraient être abolies et remplacées, lorsque cela est nécessaire, par des lois civiles appropriées sur la diffamation".

Malgré ces préoccupations, certains pays [1826] se sont dotés de dispositions de droit pénal qui répriment la calomnie ainsi que la publication de fausses informations. Il importe de souligner que même dans les pays

qui pénalisent la diffamation, le nombre d'affaires traitées connaît de larges fluctuations. Alors qu'au Royaume-Uni, aucun dossier n'a été ouvert en 2004 et un seul suspect a été accusé de calomnie en 2005,[1827] les statistiques allemandes ont enregistré 187 527 infractions à l'interdiction de diffamation en 2006.[1828] La Convention du Conseil de l'Europe sur la cybercriminalité, la Loi-type du Commonwealth et le Projet de Stanford ne contiennent pas de dispositions traitant directement des actes de ce type.

Exemple de législation nationale

Un exemple de disposition pénale concernant la calomnie figure à la section 365 du Code pénal du Queensland (Australie). Le Queensland a rétabli la responsabilité pénale en cas de diffamation au travers de la Loi pénale modificatrice de 2002 sur la diffamation.[1829]

Disposition

365 Diffamation pénale[1830]
(1) Toute personne qui, sans excuse légitime, publie du matériel diffamatoire concernant une autre personne vivante (la personne pertinente) —
a) sachant que le matériel est faux ou sans se préoccuper de savoir si le matériel est vrai ou faux; et
b) ayant l'intention de nuire gravement à la personne pertinente ou à toute autre personne ou sans se soucier de savoir si cela cause un préjudice grave pour la personne pertinente ou toute autre personne; commet un méfait. Peine maximale —3 ans de prison.
(2) Dans le cas d'une procédure relative à une infraction définie dans cette section, la personne accusée a une excuse légitime pour la publication de matériel diffamatoire à propos de la personne pertinente si, et uniquement dans ce cas, la sous-section (3) est applicable. […]

Un autre exemple de pénalisation de la calomnie se trouve à la section 185 du Code pénal allemand:

Disposition

Section 185 Insulte
L'insulte est punie d'une peine de prison d'une durée maximale d'un an ou d'une amende et si l'insulte est accompagnée de violence, elle est passible d'une peine de prison d'une durée maximale de deux ans ou d'une amende.

Dans les deux cas, ces dispositions n'ont pas été conçues pour cibler uniquement les actes commis sur l'internet. Leur application n'est pas limitée à des moyens de communication spécifiques, de sorte qu'ils peuvent réprimer aussi bien les actes commis sur un réseau que les actes commis dans un autre cadre.

6.2.14 Spam

Sachant que pas moins de 75 %[1831] de l'ensemble des messages électroniques seraient des messages indésirables[1832], un débat intense s'est tenu sur la nécessité de sanctionner pénalement les messages indésirables.[1833] Les solutions législatives nationales en matière de spam diffèrent.[1834] L'une des principales raisons pour lesquelles le spam reste problématique tient à ce que la technologie de filtrage ne parvient pas encore à reconnaître et à bloquer tous les messages indésirables.[1835] Les mesures de protection ne mettent que partiellement les utilisateurs à l'abri des messages non sollicités.

En 2005, l'OCDE a publié un rapport analysant l'incidence du spam sur les pays en développement,[1836] d'après lequel les représentants des pays en développement expriment fréquemment l'opinion que les internautes de leur pays souffrent beaucoup plus des effets du spam et des abus sur l'internet. L'analyse des résultats de ce rapport montre que l'impression de ces représentants est juste. Eu égard à la plus grande rareté et au coût supérieur des ressources, le spam se révèle un problème nettement plus grave dans les pays en développement que dans les pays occidentaux.[1837]

Les problèmes ne s'arrêtent toutefois pas à l'identification des messages électroniques indésirables. La distinction entre les messages qui ne sont pas souhaités par les destinataires, mais envoyés légalement, et les messages qui sont envoyés illégalement est complexe. La tendance actuelle à l'envoi informatisé (y compris par courrier électronique et VoIP) met en exergue l'importance de protéger les communications contre les attaques. Si le spam dépasse un certain niveau, les messages concernés peuvent gravement perturber l'utilisation des TIC et réduire la productivité des utilisateurs.

Convention du Conseil de l'Europe sur la cybercriminalité

La Convention du Conseil de l'Europe sur la cybercriminalité n'érige pas expressément le spam en infraction pénale.[1838] Ses rédacteurs ont estimé que la criminalisation d'actes de ce type doit se limiter aux cas d'entrave grave et intentionnelle à la communication.[1839] Cette approche met l'accent sur les effets sur un système ou un réseau informatique, et non sur les messages non sollicités eux-mêmes. En vertu de l'approche juridique adoptée dans la Convention du Conseil de l'Europe sur la cybercriminalité, la lutte contre le spam peut uniquement s'appuyer sur l'entrave illégale aux réseaux et aux systèmes informatiques:

> ***Article 5 – Atteinte à l'intégrité du système***
> *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.*

Projet de convention internationale de Stanford

Le Projet informel[1840] de Convention de Stanford de 1999 ne comprend pas de disposition criminalisant le spam. À l'instar de la Convention du Conseil de l'Europe sur la cybercriminalité, le Projet de Stanford criminalise uniquement le spam si les messages non sollicités entraînent une perturbation intentionnelle du système.

Texte législatif sur la cybercriminalité du projet HIPCAR

Une approche spécifique peut être observée, par exemple, à la section 15 du texte législatif sur la cybercriminalité[1841] du projet HIPCAR[1842]:

> ***Spam***
> ***15. (1)*** *Toute personne qui, intentionnellement et sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime:*
> *a. déclenche la transmission de messages de courrier électronique multiples à partir ou par l'intermédiaire d'un tel système informatique; ou*
> *b. utilise un système informatique protégé pour relayer ou retransmettre des messages de courrier électronique multiples dans le but de tromper ou d'induire en erreur les utilisateurs ou tout fournisseur de service de courrier électronique ou d'accès à l'internet quant à l'origine de ces messages; ou*
> *c. falsifie gravement les informations d'en-tête dans des messages de courrier électronique multiples et déclenche intentionnellement la transmission de ces messages; si elle est jugée coupable, est passible d'une peine de prison d'une durée maximale de [durée de la peine] ou d'une amende maximale de [montant] ou des deux.*
> *(2) Un pays peut limiter la criminalisation de la transmission de messages électroniques multiples dans le cadre des relations d'une entreprise avec ses clients ou d'autres entreprises. Un pays peut décider de ne pas criminaliser les actes visés à la section 15, paragraphe (1), point (a), s'il existe d'autres moyens de recours efficaces.*

Cette disposition inclut trois actes distincts. La section 15, paragraphe (1), point (a), a trait à l'opération consistant à déclencher la transmission de messages électroniques multiples. La section 3, paragraphe (14), définit les messages de courrier électronique multiples comme les messages électroniques, y compris les

courriels et les messages instantanés, adressés à plus de 1 000 destinataires. Dans ce contexte, la Note explicative souligne que la limitation de la criminalisation aux actes réalisés sans justification ou excuse légitime joue un rôle important pour distinguer les envois en masse légitimes (p. ex. lettres d'information) et le spam illégal.[1843] La section 15, paragraphe (1), point (b), criminalise le fait de contourner une technologie anti-spam en utilisant abusivement des systèmes informatiques pour relayer ou transmettre des messages électroniques. La section 15, paragraphe (1), point (c), couvre le fait de contourner une technologie anti-spam en falsifiant les informations d'en-tête. La Note explicative met en exergue que la section 15 exige que le délinquant commette les infractions intentionnellement et sans justification ou excuse légitime.[1844]

Code des États-Unis (USC)

La criminalisation du spam est limitée aux cas dans lesquels la quantité de messages indésirables produit une incidence grave sur la puissance de traitement des systèmes informatiques. Les messages indésirables qui nuisent à l'efficacité du commerce, mais pas nécessairement du système informatique, ne peuvent faire l'objet de poursuites. Un certain nombre de pays utilisent donc une approche différente. Un exemple réside dans la législation des États-Unis, et notamment la section 18 de l'USC, § 1037.[1845]

§ 1037. Fraude et activités connexes en rapport avec le courrier électronique
(a) En général – quiconque affecte le commerce entre Etats ou le commerce international, en toute connaissance de cause –
(1) accède à un ordinateur protégé sans autorisation et déclenche intentionnellement la transmission de messages électroniques commerciaux multiples à partir ou à travers ledit ordinateur,
(2) utilise un ordinateur protégé pour relayer ou retransmettre des messages électroniques commerciaux multiples avec l'intention de tromper ou d'induire en erreur les destinataires ou tout autre service d'accès à l'Internet, en ce qui concerne l'origine de tels messages,
(3) falsifie matériellement les informations se trouvant dans les en-têtes de messages électroniques commerciaux multiples et déclenche intentionnellement la transmission de tels messages,
(4) enregistre, en utilisant des informations qui falsifient matériellement l'identité du véritable inscrit, pour cinq comptes de courriers électroniques ou plus ou des comptes d'utilisateurs en ligne ou deux noms de domaines ou plus et déclenche intentionnellement la transmission de messages électroniques commerciaux multiples à partir de toute combinaison de tels comptes ou noms de domaines, ou
(5) se présente faussement comme étant l'inscrit ou le successeur légitime dans l'intérêt de l'inscrit de cinq adresses de protocoles Internet ou plus et déclenche intentionnellement la transmission de messages électroniques commerciaux multiples à partir de telles adresses,
ou conspire pour le faire, sera puni comme il est prévu à la sous-section (b).
(b) Peines – La peine pour une infraction au titre de la sous-section (a) est–
(1) une amende à ce titre, une peine de prison maximale de 5 ans ou les deux, si–
(A) l'infraction est commise subséquemment à tout acte délictueux grave conformément aux législations des Etats-Unis ou d'un de ses Etats; ou
(B) le défendeur a précédemment été condamné au titre de cette section ou de la section 1030, ou au titre de la législation d'un état pour conduite impliquant la transmission de messages électroniques commerciaux multiples ou l'accès non autorisé à un système informatique;

Cette disposition a été mise en œuvre par la loi CAN-SPAM de 2003.[1846] La finalité de cette loi était d'instaurer une norme nationale unique destinée à contrôler le courrier électronique commercial.[1847] Elle s'applique aux messages électroniques commerciaux, mais pas aux messages relatifs aux transactions et aux relations commerciales existantes. L'approche réglementaire exige que les messages électroniques commerciaux comprennent une indication sur la sollicitation, y compris des instructions pour ne plus recevoir ce type de messages et l'adresse physique de l'expéditeur.[1848] La section 18 de l'USC, § 1037, criminalise spécialement les expéditeurs de messages électroniques indésirables s'ils falsifient les informations d'en-tête des messages pour contourner les technologies de filtrage.[1849] De plus, la disposition

criminalise l'accès non autorisé à un ordinateur protégé et le déclenchement de la transmission de messages électroniques commerciaux multiples.

6.2.15 Abus de dispositifs

Un autre problème grave a trait à l'existence d'outils logiciels et matériels destinés à commettre des infractions.[1850] En marge de la prolifération de « dispositifs de piratage », l'échange de mots de passe permettant à des utilisateurs non autorisés d'accéder à des systèmes informatiques soulève un défi de taille.[1851] Eu égard à l'existence de tels dispositifs et à la menace potentielle qu'ils impliquent, il est difficile de focaliser la criminalisation sur l'utilisation de ces outils aux seules fins de commettre des infractions. La plupart des systèmes pénaux nationaux contiennent des dispositions réprimant l'élaboration et la production de tels outils, en complément à la « tentative d'infraction ». Une méthode permettant de lutter contre la diffusion de dispositifs de ce type consiste en effet à criminaliser leur production. En général, cette criminalisation, qui s'accompagne généralement d'un transfert substantiel de la responsabilité pénale, se limite aux infractions les plus graves. Dans la législation de l'UE, en particulier, on constate une tendance à étendre la criminalisation des actes préparatoires à des infractions moins graves. [1852]

Convention du Conseil de l'Europe sur la cybercriminalité

Considérant les autres initiatives du Conseil de l'Europe, les rédacteurs de la Convention sur la cybercriminalité ont établi une infraction pénale distincte pour certains actes légaux ayant trait à des dispositifs déterminés ou l'accès à des données pouvant être utilisées abusivement afin de commettre une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de systèmes ou de données:[1853]

Disposition

Article 6 *– Abus de dispositifs*

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a) la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i) d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii) d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b) la possession d'un élément visé aux paragraphes a)i) ou ii) ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2) Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3) Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Objets couverts

Le paragraphe 1a) cite à la fois les dispositifs[1854] conçus pour commettre et encourager des actes de cybercriminalité et les mots de passe permettant d'accéder à un système informatique. Le terme « dispositifs » inclut à la fois les solutions utilisant du matériel et des logiciels pour commettre l'une des

infractions mentionnées. Le Rapport explicatif cite par exemple les logiciels tels que des programmes-virus, ou bien des programmes conçus ou adaptés pour accéder à des systèmes informatiques.[1855] À la différence des dispositifs, « un mot de passe, un code d'accès ou des données informatiques similaires » n'exécutent pas d'opérations, mais constituent des codes d'accès. Une question débattue à cet égard consiste à déterminer si la publication de failles d'un système tombe dans le champ d'application de la disposition.[1856] Contrairement à un code d'accès ordinaire, la divulgation d'une faille du système ne permet pas nécessairement d'accéder immédiatement à un système informatique, mais elle permet à un délinquant d'exploiter cette faille pour attaquer un système informatique avec fruit.

Actes couverts

La Convention sur la cybercriminalité incrimine une large gamme d'actes. Outre la production, elle sanctionne également la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition de dispositifs et de mots de passe. Une approche similaire (limitée aux dispositifs destinés à contourner des mesures techniques) figure dans la législation de l'UE sur l'harmonisation des droits d'auteur,[1857] et plusieurs pays ont intégré des dispositions similaires dans leur droit pénal.[1858] La « diffusion » désigne l'action consistant à transmettre des dispositifs ou des mots de passe à autrui.[1859] Aux fins de l'article 6, la « vente » fait référence à toute activité consistant à vendre des dispositifs et des mots de passe en échange d'une somme d'argent ou d'une autre rétribution. L'« obtention pour utilisation » se réfère à l'action d'obtenir des mots de passe et des dispositifs.[1860] Le fait que l'acte d'obtention soit associé à l'utilisation d'outils de ce type requiert généralement une intention dans le chef du délinquant de se procurer ces outils pour un usage qui dépasse la finalité « normale », à savoir « dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ». L'« importation » désigne l'action d'obtenir des dispositifs et des codes d'accès à partir d'autres pays.[1861] En conséquence, un délinquant qui importe de tels outils pour les vendre peut être poursuivi avant même de les proposer à la vente. Sachant que l'obtention d'outils de ce type est uniquement criminalisée si elle peut être associée à l'utilisation, on peut se demander si la seule importation de tels outils, sans l'intention de les vendre ou de les utiliser, tombe sous le coup de l'article 6 de la Convention du Conseil de l'Europe sur la cybercriminalité. La « mise à disposition » désigne toute action permettant à d'autres utilisateurs d'accéder aux outils en cause.[1862] Le Rapport explicatif ajoute que cette expression doit également englober la création ou la compilation d'hyperliens visant à faciliter l'accès à ces dispositifs.[1863]

Outils à double usage

À la différence de l'approche choisie par l'Union européenne pour l'harmonisation des droits d'auteur,[1864] cette disposition ne s'applique pas uniquement aux dispositifs qui sont exclusivement conçus pour faciliter la commission d'actes de cybercriminalité, mais la Convention sur la cybercriminalité inclut également les dispositifs qui sont généralement utilisés à des fins légales lorsque le délinquant a spécialement l'intention de commettre un acte de cybercriminalité. Dans le Rapport explicatif, les rédacteurs affirment que la limitation aux dispositifs conçus exclusivement pour commettre des crimes est trop restrictive et risquerait de créer des difficultés insurmontables pour l'établissement de la preuve dans les procédures pénales, ce qui rendrait la disposition pratiquement inapplicable ou applicable uniquement dans de rares cas.[1865]

Afin d'assurer une protection appropriée des systèmes informatiques, les experts possèdent et utilisent divers outils logiciels qui pourraient les exposer à des mesures de répression. La Convention sur la cybercriminalité aborde ces préoccupations de trois manières[1866]: elle permet aux parties, à l'article 6, paragraphe 1, sous-paragraphe b, d'instaurer des réserves en ce qui concerne la détention d'un nombre minimal des éléments concernés pour que la responsabilité pénale soit engagée. D'autre part, la criminalisation de la possession de ces dispositifs est limitée par le critère de l'intention de les utiliser pour commettre une infraction telle qu'énoncée aux articles 2 à 5 de la Convention sur la cybercriminalité.[1867] Le Rapport explicatif précise que cette intention spécifique a été incluse « afin d'éviter le risque de la surpénalisation lorsque des dispositifs sont fabriqués et commercialisés à des fins légitimes, par exemple pour contrer des atteintes aux systèmes informatiques ».[1868] Enfin, les rédacteurs de la Convention sur la cybercriminalité ont clairement établi au paragraphe 2 que les outils créés pour l'essai autorisé ou la protection d'un système informatique ne sont pas visés par la disposition, puisqu'elle porte uniquement sur les actes non autorisés.

Criminalisation de la possession

Le paragraphe 1, sous-paragraphe b, pousse la disposition du paragraphe 1, sous-paragraphe a, à un degré supérieur en criminalisant la possession de dispositifs ou de mots de passe s'ils sont associés à l'intention de commettre un acte de cybercriminalité. La criminalisation de la possession d'outils prête à controverse.[1869] L'article 6 ne se limite pas aux outils qui sont conçus exclusivement pour commettre des infractions, et les détracteurs de la criminalisation craignent que la criminalisation de la possession de tels dispositifs ne crée des risques inacceptables pour les administrateurs de systèmes et les spécialistes de la sécurité de réseaux.[1870] La Convention sur la cybercriminalité permet aux parties d'exiger qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

Élément moral

Comme pour toutes les autres infractions définies par la Convention sur la cybercriminalité du Conseil de l'Europe, l'article 6 exige que l'auteur commette intentionnellement les comportements concernés.[1871] En complément à l'intention normale concernant les comportements désignés, l'article 6 de la Convention sur la cybercriminalité exige une intention spécifique supplémentaire d'utiliser le dispositif en cause afin de commettre l'une des infractions citées aux articles 2 à 5 de la Convention.[1872]

Sans droit

D'une manière similaire aux dispositions décrites précédemment, les actes concernés doivent être commis « sans droit ».[1873] En réponse aux craintes que la disposition puisse servir à criminaliser l'utilisation légitime d'outils logiciels dans le cadre de mesures de protection individuelle, les rédacteurs de la Convention sur la cybercriminalité ont précisé que de tels actes ne sont pas réputés commis « sans droit ».[1874]

Restrictions et réserves

En raison du débat sur la nécessité de criminaliser la possession de dispositifs, la Convention sur la cybercriminalité inclut à l'article 6, paragraphe 3, la possibilité d'une réserve complexe (en complément au paragraphe 1, sous-paragraphe b, 2e phrase). Si une partie opte pour cette réserve, elle peut exclure la criminalisation de la possession d'outils et une série d'actes illégaux au titre du paragraphe 1, sous-paragraphe a, par exemple, la production de tels dispositifs.[1875]

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique

Une approche similaire à l'article 6 de la Convention du Conseil de l'Europe sur la cybercriminalité est inscrite à la section 10 de la Loi-type de 2002 du Commonwealth.[1876]

Dispositifs illégaux
9.
(1) Une personne qui commet une infraction si elle:
(a) produit, vend, obtient pour utilisation, importe, exporte, distribue ou met à disposition, intentionnellement ou avec témérité, sans justification ou excuse légitime:
(i) un dispositif, incluant un programme informatique, qui est conçu ou adapté dans le but de commettre une infraction visée aux sections 5, 6, 7 ou 8; ou
(ii) un mot de passe d'ordinateur, un code d'accès ou des données similaires permettant d'accéder à tout ou partie d'un système informatique;
avec l'intention qu'il peut être utilisé par quiconque voulant commettre une infraction visée aux sections 5, 6, 7 ou 8; ou
(b) a en sa possession un dispositif mentionné dans les sous-paragraphes (i) ou (ii) avec l'intention qu'il soit utilisé par quiconque voulant commettre une infraction visée aux sections 5, 6, 7 ou 8.
(2) Une personne jugée coupable d'une infraction contre cette section est passible d'une peine de prison d'une durée maximale de [durée de la peine] ou d'une amende maximale de [montant] ou des deux.

Bien que les dispositifs et les actes énoncés dans la disposition soient les mêmes, une différence essentielle par rapport à la Convention du Conseil de l'Europe sur la cybercriminalité tient à ce que la Loi-type du Commonwealth criminalise, outre les actes intentionnels, les actes téméraires, alors que la Convention sur la cybercriminalité requiert une intention dans tous les cas. Au cours des négociations sur la Loi-type du Commonwealth, d'autres modifications de la disposition pénalisant la possession de tels dispositifs ont été débattues. Le groupe d'experts a proposé de criminaliser les délinquants possédant plus d'un seul élément.[1877] Le Canada a proposé une approche similaire, sans déterminer au préalable le nombre d'éléments qui engagerait la responsabilité pénale.[1878]

Projet de convention internationale de Stanford

Le Projet informel[1879] de Convention internationale de Stanford de 1999 (ci-après le "Projet de Stanford ») comprend une disposition criminalisant les actes se rapportant à certains dispositifs illégaux.

> ***Article 3*** *– Infractions*
> *1. Les infractions au titre de cette Convention sont commises si une personne s'engage illégalement et intentionnellement dans l'une des actions suivantes sans l'autorité, l'autorisation ou le consentement reconnu légitimement:*
> *[...]*
> *(e) fabrique, vend, utilise, envoie ou distribue de quelconque autre façon tout dispositif ou programme ayant pour objectif de commettre une action quelconque interdite par les Art. 3 et 4 de la présente Convention;*

Ses rédacteurs ont affirmé qu'en règle générale, aucun type de discours ou de publication ne doit faire l'objet d'un traitement pénal aux termes du Projet de Stanford.[1880] L'unique exception qu'ils ont concédée porte sur les dispositifs illégaux.[1881] Dans ce contexte, les rédacteurs ont souligné que la criminalisation doit se limiter aux actes désignés, et par exemple, ne pas englober les discussions sur les failles d'un système.[1882]

Texte législatif sur la cybercriminalité du projet HIPCAR

Une approche intéressante peut être observée dans le texte législatif élaboré par les pays bénéficiaires dans le cadre de l'initiative HIPCAR.[1883]

> ***Dispositifs illégaux***
> ***10****.*
> *[…]*
> *(3) Un pays peut décider de ne pas ériger en infraction pénale le simple accès non autorisé s'il existe d'autres recours efficaces. De plus, un pays peut décider de limiter la criminalisation aux dispositifs énumérés dans une Annexe.*

Afin d'éviter une criminalisation excessive, les rédacteurs ont décidé de donner la possibilité de limiter la criminalisation à une liste noire. Dans ce cas, seuls les dispositifs répertoriés dans cette liste sont couverts par la disposition. Cette approche réduit les risques de criminaliser des actes qui sont souhaitables dans un but de sécurité informatique. La tenue d'une telle liste nécessiterait toutefois plus que probablement des ressources substantielles.

6.2.16 Falsification informatique

Les procédures pénales relatives à une falsification informatique tendaient par le passé à être rares car la plupart des documents juridiques étaient établis sur papier. À la faveur de la numérisation, cette situation est aujourd'hui en train de changer.[1884] La multiplication des documents numériques est favorisée par l'instauration d'un cadre juridique pour leur utilisation, par exemple, avec la reconnaissance juridique des signatures numériques. De plus, les dispositions contre la falsification informatique jouent un rôle important dans la lutte contre le « phishing ».[1885]

Convention du Conseil de l'Europe sur la cybercriminalité

La plupart des systèmes de droit pénal répriment la falsification de documents sur papier.[1886] Les rédacteurs de la Convention sur la cybercriminalité ont remarqué que les structures dogmatiques des législations nationales diffèrent.[1887] Certains concepts reposent sur l'authenticité de l'auteur d'un document, tandis que d'autres sont fondés sur l'authenticité de son contenu. Les rédacteurs ont décidé de définir des normes minimales et de protéger la sécurité et la fiabilité des données électroniques en créant une infraction qui soit le pendant de la falsification traditionnelle de documents sur papier afin de combler les lacunes du droit pénal, qui pourrait ne pas s'appliquer aux données enregistrées sur support électronique.[1888]

Disposition

> ***Article 7 – Falsification informatique***
> *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnelles et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement visibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.*

Objet couvert

La cible d'une falsification informatique réside dans les données, sans distinction qu'elles soient directement lisibles et/ou intelligibles ou non. Les données informatiques sont définies dans la Convention sur la cybercriminalité[1889] comme étant « toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ». La disposition ne fait pas seulement référence à des données informatiques, qui doivent faire l'objet de l'un des actes mentionnés, mais il faut également que ces actes engendrent des données non authentiques.

À tout le moins en ce qui concerne l'élément moral, l'article 7 exige que les données soient équivalentes à un document public ou privé. En d'autres termes, les données doivent être légalement pertinentes:[1890] la falsification de données qui ne peuvent pas être utilisées à des fins légales n'est pas couverte par la disposition.

Actes couverts

L'« introduction » de données[1891] doit correspondre à la production d'un document sur papier falsifié.[1892] Le terme « altération » se réfère à la modification de données existantes.[1893] Le Rapport explicatif précise spécialement les modifications et les changements partiels.[1894] La notion de « suppression » de données informatiques décrit une action qui affecte l'accessibilité des données.[1895] Dans le Rapport explicatif, les rédacteurs mentionnent spécialement le fait de retenir ou de cacher des données.[1896] L'acte peut être réalisé, par exemple, en bloquant certaines informations provenant d'une base de données lors de la création automatique d'un document électronique. Le terme « effacement » correspond à la définition donnée à ce terme à l'article 4 sur les actes par lesquels des informations sont éliminées.[1897] Le Rapport explicatif ne fait référence qu'au fait de sortir des données figurant sur un support,[1898] mais la portée de la disposition plaide fortement en faveur d'une définition plus large de la notion d'« effacement ». Sur la base d'une définition plus large, cet acte peut ainsi être réalisé en supprimant un fichier complet ou en effaçant partiellement des informations d'un fichier.[1899]

Élément moral

Comme pour toutes les autres infractions définies par la Convention du Conseil de l'Europe sur la cybercriminalité, l'article 3 exige que le délinquant commette intentionnellement les infractions concernées. [1900] La Convention sur la cybercriminalité ne contient pas de définition du terme « intentionnellement ». Dans le Rapport explicatif, les rédacteurs ont noté que le terme « intentionnellement » doit être défini au niveau national.[1901]

Sans droit

Un acte de falsification ne peut être poursuivi en vertu de l'article 7 de la Convention sur la cybercriminalité que s'il est commis « sans droit ».[1902]

Restrictions et réserves

L'article 7 offre également la possibilité d'adopter une réserve limitant la criminalisation, en exigeant des éléments supplémentaires, tels qu'une intention frauduleuse, pour que la responsabilité pénale puisse être engagée.[1903]

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique

La Loi-type de 2002 du Commonwealth ne contient aucune disposition criminalisant la falsification informatique.[1904]

Projet de convention internationale de Stanford

Le Projet informel [1905] de Convention internationale de Stanford de 1999 comprend une disposition criminalisant les actes se rapportant aux données informatiques falsifiées.

> ***Article 3 – Infractions***
> *1. Des infractions, au titre de cette Convention, sont commises si une personne s'engage illégalement et intentionnellement dans l'une quelconque des activités suivantes sans autorité, permission ou consentement reconnu légalement:*
> *[...]*
> *(b) crée, stocke, altère, efface, transmet, détourne, achemine incorrectement, manipule ou interfère avec des données dans un système cybernétique dans le but et avec l'effet de fournir de fausses informations afin de causer des dommages substantiels à des personnes ou des biens;*
> *[...]*

La principale différence avec l'article 7 de la Convention du Conseil de l'Europe sur la cybercriminalité tient à ce que l'article 1, paragraphe 1, point (b), ne traite pas de la simple manipulation de données, mais exige une interférence avec un système informatique. Selon l'article 7 de la Convention du Conseil de l'Europe sur la cybercriminalité, un tel acte n'est pas indispensable et il suffit que le délinquant ait agi dans l'intention que les données soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.

6.2.17 Vol d'identité

Eu égard à la couverture médiatique qui lui est accordée,[1906] aux résultats d'études récentes[1907] et aux nombreuses publications juridiques et techniques à ce sujet[1908], il semble que le vol d'identité puisse être décrit comme un phénomène de masse.[1909] Malgré la dimension mondiale de ce phénomène, tous les pays n'ont pas encore introduit dans leur droit pénal interne de dispositions criminalisant tous les actes se rapportant au vol d'identité. La Commission de l'Union européenne (ci-après la « CE ») a déclaré récemment que le vol d'identité n'a pas encore fait l'objet d'une criminalisation dans tous les États membres de l'UE.[1910] Elle a en outre exprimé l'opinion que « la coopération européenne en matière de répression bénéficierait du fait que l'usurpation d'identité soit érigée en infraction pénale dans tous les États membres » et annoncé qu'elle engagerait prochainement des consultations pour déterminer s'il est judicieux de légiférer en la matière.[1911]

Lorsqu'on tente de comparer les instruments juridiques existants pour lutter contre le vol d'identité, on rencontre notamment le problème qu'ils sont largement disparates.[1912] Le seul élément constant dans les approches appliquées est que le comportement réprimé concerne une ou plusieurs des phases suivantes:[1913]

- phase 1: acte consistant à obtenir des informations sur une identité;
- phase 2: acte consistant à posséder ou à transférer les informations sur cette identité;

- phase 3: acte consistant à utiliser les informations sur cette identité à des fins criminelles.

Sur la base de ce constat, deux approches systématiques se distinguent d'une manière générale dans la criminalisation du vol d'identité:

- la formulation d'une disposition unique qui criminalise les actes consistant à obtenir, posséder et utiliser des informations sur une identité (à des fins criminelles);
- la criminalisation distincte des actes typiques liés à l'obtention d'informations sur une identité (p. ex. l'accès illégal, la production et la diffusion de logiciels malveillants, la falsification informatique, l'espionnage de données et l'atteinte à l'intégrité des données), ainsi que les actes liés à la possession et à l'utilisation de telles informations (p. ex. la fraude informatique).

Exemple d'une approche par une disposition unique

Les exemples les plus connus de dispositions uniques sont la section 18 de l'USC, § 1028(a)(7), et la section 18 de l'USC, § 1028A(a)(1). Ces dispositions couvrent une large gamme d'infractions se rapportant au vol d'identité. Dans cette approche, la criminalisation n'est pas limitée à une phase spécifique, mais s'étend aux trois phases précitées. Il importe toutefois de souligner que la disposition n'englobe pas toutes les activités liées au vol d'identité, en particulier, lorsque l'acte est commis par la victime, et non par le délinquant.

§ 1028. Fraude et activités connexes en rapport avec des documents d'identification, des propriétés d'authentification et l'information

(a) Quiconque, dans des conditions décrites à la sous-section (c) de cette section -

(1) produit en toute connaissance de cause et sans autorisation légitime un document d'information, une caractéristique d'authentification ou un faux document d'identification;

(2) transfère, en toute connaissance de cause, un document d'identification, une caractéristique d'authentification ou un faux document d'identification sachant que ledit document ou ladite caractéristique ont été volés ou produits sans autorisation légitime;

(3) possède, en toute connaissance de cause, avec l'intention de l'utiliser de manière illicite ou transfère de manière illicite cinq documents d'identification ou plus (autres que ceux qui sont délivrés légitimement pour l'utilisation du possesseur), des caractéristiques d'identification ou de faux documents d'identification;

(4) possède, en toute connaissance de cause, un document d'identification (autre que celui émit légitimement pour l'utilisation de son possesseur), une caractéristique d'authentification ou un faux document d'identification, avec l'intention que ledit document ou ladite caractéristique seront utilisés pour frauder les États-Unis;

(5) produit, transfère ou possède, en toute connaissance de cause, un outil de fabrication de documents ou une caractéristique d'identification avec l'intention que cet outil de fabrication de documents ou cette caractéristique d'authentification seront utilisés pour produire un faux document d'identification ou un autre outil de fabrication de documents ou une autre caractéristique d'authentification qui seront utilisés de cette façon;

(6) possède, en toute connaissance de cause, un document d'identification ou une caractéristique d'authentification qui est ou semble être un document d'identification ou une caractéristique d'authentification des Etats-Unis qui a été volé ou produit sans autorisation légitime sachant que ledit document ou ladite caractéristique ont été volés ou produits sans une telle autorisation;

(7) transfère, possède ou utilise, en toute connaissance de cause, sans autorisation légitime un moyen d'identification d'une autre personne avec l'intention de commettre ou d'aider ou d'encourager ou en rapport avec, toute activité illicite qui constitue une violation de la législation fédérale ou qui constitue un acte délictueux grave au titre de toute législation applicable locale ou d'Etat; ou

(8) fait trafic, en toute connaissance de cause, de fausses ou de véritables caractéristiques d'identification pour utilisation dans de faux documents d'identification, dans des outils de fabrication de documents ou dans des moyens d'identification;

sera puni comme il est prévu à la sous-section (b) de cette section.

[…]
§ 1028A. Vol d'identité aggravé
(a) Infractions.
(1) En général, quiconque, pendant et en relation avec un acte délictueux grave mentionné à la sous-section (c) transfère, possède ou utilise, en toute connaissance de cause, sans autorisation légitime, un moyen d'identification d'une autre personne sera, en plus de la peine encourue pour un tel acte délictueux grave, passible d'une peine de prison de deux ans.
[…]

Phase 1

Afin de commettre des infractions liées au vol d'identité, un délinquant doit prendre possession de données d'identification.[1914] En criminalisant le « transfert » de moyens d'identification dans l'intention de commettre une infraction, les dispositions criminalisent les actes relevant de la première phase dans un sens très large.[1915] Étant donné que les dispositions se concentrent sur l'acte de transfert, elles n'incluent pas les actes que le délinquant a réalisés préalablement au début du processus de transfert.[1916] Les actes tels que l'envoi de messages de phishing et la conception de logiciels malveillants, qui peuvent être accomplis afin d'obtenir des données d'identification informatiques auprès des victimes, ne sont pas couverts par la section 18 de l'USC, § 1028(a)(7), et la section 18 de l'USC, § 1028A(a)(1).

Phase 2

En criminalisant la possession dans l'intention de commettre une infraction, les dispositions adoptent à nouveau une approche large quant à la criminalisation des actes relevant de la deuxième phase. Parmi ceux-ci figurent, entre autres, la possession d'informations d'identification dans l'intention de les utiliser ultérieurement aux fins d'une des infractions traditionnelles liées au vol d'identité.[1917] La possession de données d'identification sans l'intention de les utiliser n'est pas visée.[1918]

Phase 3

En criminalisant l'« utilisation » dans l'intention de commettre une infraction, les dispositions englobent les actes relevant de la troisième phase. Ainsi que cela a été évoqué plus haut, la section 18 de l'USC, § 1028(a)(7), n'est pas associée à une infraction particulière (comme la fraude).

Un autre exemple réside dans la section 14 du texte législatif sur la cybercriminalité qui a été élaboré par les pays bénéficiaires dans le cadre de l'initiative HIPCAR.[1919]

Infractions liées à l'identité
14.
Toute personne qui, intentionnellement et sans justification ou excuse légitime ou au-delà d'une justification ou d'une excuse légitime, en utilisant un système informatique à un stade quelconque de l'infraction, transfère, possède ou utilise intentionnellement, sans justification ou excuse légitime, un moyen d'identification d'une autre personne dans l'intention de commettre, d'aider ou d'inciter un quelconque acte illégal qui constitue une infraction, ou dans le cadre d'un tel acte, si elle est jugée coupable, est passible d'une peine de prison d'une durée maximale de [durée de la peine] ou d'une amende maximale de [montant] ou des deux.

Cette disposition inclut les principales phases d'une atteinte à l'identité typique telles qu'elles ont été décrites ci-dessus. Seule la première phase, dans laquelle le délinquant obtient les informations d'identification, n'est pas couverte. Le « transfert » d'un moyen d'identification couvre les processus de transmission de données d'un ordinateur à un autre système informatique. Cet acte revêt une importance particulière pour cibler la vente (et le transfert connexe) d'informations d'identification.[1920] La « possession » désigne le contrôle qu'une personne exerce intentionnellement sur des informations d'identification. L'« utilisation » réunit une large gamme de pratiques, telles que la saisie des informations en cause aux fins d'achats en ligne. S'agissant de l'élément moral, la disposition exige que le délinquant agisse intentionnellement en ce qui concerne tous les éléments objectifs et qu'il ait de surcroît l'intention

spécifique de se livrer à l'acte de commettre, d'aider ou d'inciter un quelconque acte illégal allant au-delà du transfert, de la possession ou de l'utilisation d'informations d'identification.

Exemple d'une approche de disposition multiple

La principale différence entre la Convention du Conseil de l'Europe sur la cybercriminalité et les approches articulées autour d'une disposition unique (comme aux États-Unis, par exemple) est que la Convention sur la cybercriminalité n'établit pas d'infraction informatique spécifique pour l'utilisation illégale d'informations d'identification.[1921] D'une manière similaire à la situation prévalant pour la criminalisation de l'obtention d'informations d'identification, la Convention sur la cybercriminalité ne couvre pas tous les actes potentiels liés à l'utilisation illégale d'informations personnelles.

Phase 1

La Convention du Conseil de l'Europe sur la cybercriminalité[1922] contient une série de dispositions qui criminalisent les actes de vol d'identité sur l'internet à la première phase, en particulier:

- Accès illégal (article 2) [1923]
- Interception illégale (article 3) [1924]
- Atteinte à l'intégrité des données (article 4) [1925]

Eu égard aux procédés multiples par lesquels un délinquant peut accéder à des données, il convient de souligner que tous les actes possibles à la première phase ne sont pas couverts. Un exemple d'infraction qui est souvent associée à la phase 1 du vol d'identité, mais n'est pas couverte par la Convention du Conseil de l'Europe sur la cybercriminalité, est l'espionnage de données.

Phase 2

Les actes réalisés entre l'obtention d'informations et leur utilisation à des fins criminelles peuvent difficilement être couverts par la Convention du Conseil de l'Europe sur la cybercriminalité. En particulier, il n'est pas possible d'empêcher l'expansion d'un marché noir d'informations d'identification en criminalisant la vente de telles informations en vertu de la Convention sur la cybercriminalité.

Phase 3

La Convention du Conseil de l'Europe sur la cybercriminalité définit une série d'infractions relevant de la cybercriminalité, dont certaines peuvent être commises par leur auteur à l'aide d'informations d'identification. Un exemple est la fraude informatique, qui est souvent évoquée dans le cadre du vol d'identité.[1926] Les études sur le vol d'identité révèlent que la plupart des données obtenues servent à des escroqueries aux cartes de crédit.[1927] Si l'escroquerie aux cartes de crédit est commise en ligne, son auteur peut sans doute être poursuivi sur la base de l'article 8 de la Convention du Conseil de l'Europe sur la cybercriminalité. Les autres infractions susceptibles d'être commises au moyen d'informations d'identification obtenues préalablement qui ne sont pas énoncées dans la Convention sur la cybercriminalité échappent à ce cadre juridique. Il est notamment impossible de poursuivre l'utilisation d'informations d'identification dans l'intention de dissimuler son identité.

6.2.18 Fraude informatique

La fraude est une infraction répandue dans le cyberespace.[1928] Elle constitue également un problème courant dans le monde réel, si bien que la plupart des législations nationales ont prévu des dispositions criminalisant les infractions de fraude.[1929] Il peut toutefois être difficile d'appliquer les dispositions existantes aux cas commis sur l'internet lorsque le droit pénal national s'appuie sur la fausseté d'une personne.[1930] Dans de nombreux cas de fraude sur l'internet, c'est en réalité un système informatique qui réagit à un acte du délinquant. Si les dispositions pénales traditionnelles sur la fraude ne couvrent pas les systèmes informatiques, le droit national doit être actualisé.[1931]

Convention du Conseil de l'Europe sur la cybercriminalité

La Convention sur la cybercriminalité a pour objet, au travers d'un article sur la fraude informatique, de rendre passible d'une sanction pénale toute manipulation abusive au cours d'un traitement de données en vue d'effectuer un transfert illicite de propriété:[1932]

Disposition

> ***Article 8*** *– Fraude informatique*
> *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:*
>
> *a. par toute introduction, altération, effacement ou suppression de données informatiques;*
> *b. par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.*

Actes couverts

L'article 8, paragraphe a, dresse une liste des actes de fraude informatique les plus pertinents.[1933] L'« introduction » de données informatiques inclut toutes les formes de manipulation de l'introduction, comme la saisie de données inexactes dans l'ordinateur, les manipulations des logiciels informatiques et tout autre acte d'ingérence dans le traitement des données.[1934] L'« altération » se réfère à la modification de données existantes.[1935] La notion de « suppression » de données informatiques décrit une action qui affecte l'accessibilité des données.[1936] L'« effacement » correspond à la définition donnée à ce terme à l'article 4 sur les actes par lesquels des informations sont éliminées.[1937]

En complément à la liste d'actes, l'article 8, sous-paragraphe b, énonce la disposition générale qui érige en infraction pénale l'« atteinte au fonctionnement d'un système informatique » dans un contexte de fraude. Cette formule a été ajoutée à la liste des actes couverts afin que la disposition puisse être étendue à de nouveaux développements.[1938]

Le Rapport explicatif souligne que l'« atteinte au fonctionnement d'un système informatique » se rapporte à des actes tels que les manipulations de matériel, les actes empêchant les sorties sur imprimante et les actes affectant les enregistrements ou les flux de données, ou l'ordre dans lequel les programmes sont exécutés.[1939]

Perte économique

Selon la plupart des législations pénales nationales, l'acte criminel doit provoquer une perte économique. La Convention sur la cybercriminalité s'inspire d'un concept similaire, limitant la criminalisation aux actes dans lesquels les manipulations occasionnent directement à autrui un préjudice économique ou matériel, qui concerne de l'argent ou des immobilisations corporelles ou incorporelles ayant une valeur économique.[1940]

Elément moral

Comme pour les autres infractions énumérées, l'article 8 de la Convention du Conseil de l'Europe sur la cybercriminalité exige que le délinquant ait agi intentionnellement. L'intention porte à la fois sur la manipulation et sur la perte financière.

De plus, la Convention sur la cybercriminalité impose que le délinquant ait agi avec une intention frauduleuse ou malhonnête en vue d'obtenir un avantage économique ou autre pour lui-même ou pour autrui.[1941] À titre d'exemples d'actes exclus de la responsabilité pénale en raison de l'absence d'intention spécifique, le Rapport explicatif cite les activités commerciales relatives à la concurrence qui peuvent causer un préjudice économique à une personne et apporter un bénéfice à une autre, mais qui ne sont pas pratiquées dans une intention frauduleuse ou malhonnête.[1942]

Sans droit

Une fraude informatique ne peut être poursuivie en vertu de l'article 8 de la Convention sur la cybercriminalité que si elle est commise « sans droit »,[1943] ce qui implique l'exigence que le bénéfice économique soit obtenu sans droit. Les rédacteurs de la Convention sur la cybercriminalité ont souligné que les activités menées en vertu d'un contrat en bonne et due forme passé entre les personnes concernées ne sont pas réputées exécutées sans droit.[1944]

Modèle de loi du Commonwealth relative à la criminalité informatique et liée à l'informatique

La Loi-type de 2002 du Commonwealth ne contient aucune disposition criminalisant la fraude informatique.[1945]

Projet de convention internationale de Stanford

Le Projet informel[1946] de Convention internationale de Stanford de 1999 ne contient pas de disposition criminalisant la fraude informatique.

6.2.19 Infractions portant atteinte à la propriété intellectuelle

Le passage de la distribution analogique à la distribution numérique de contenus protégés par des droits de propriété intellectuelle marque un virage dans la violation des droits de propriété intellectuelle.[1947] La reproduction d'œuvres musicales et de vidéos a toujours été limitée car la reproduction d'une source analogique était souvent accompagnée d'une perte de qualité de la copie, ce qui, à son tour, limitait la possibilité d'utiliser la copie comme source pour d'autres reproductions. Avec le passage aux sources numériques, la qualité est préservée et il est possible d'obtenir des copies d'une qualité constante.[1948]

L'industrie du spectacle a réagi en mettant en place des mesures techniques (gestion des droits numériques ou DRM) pour empêcher la reproduction[1949], mais, jusqu'à présent, ces mesures ont généralement été contournées peu après leur introduction.[1950] Il existe divers outils logiciels sur Internet qui permettent aux utilisateurs de copier des CD de musique et des DVD de films protégés par des systèmes DRM. En outre, l'Internet offre des possibilités de distribution illimitées. Il en résulte que les atteintes aux droits de propriété intellectuelle (notamment de droits d'auteur) sont des infractions très courantes sur Internet.[1951]

Convention du Conseil de l'Europe sur la cybercriminalité

La Convention sur la cybercriminalité comporte une disposition couvrant les infractions portant atteintes à la propriété intellectuelle qui s'efforce d'harmoniser les diverses réglementations que l'on trouve dans la législation nationale. Cette disposition s'avère être l'un des principaux obstacles à l'application de la Convention sur la cybercriminalité au-delà des frontières européennes.

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes
(1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des oeuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
(2) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
(3) Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

L'atteinte à la propriété intellectuelle est déjà criminalisée dans plusieurs pays[1952] et est visée dans un certain nombre de traités internationaux.[1953] La Convention sur la cybercriminalité a pour objectif d'établir des principes fondamentaux concernant la criminalisation des atteintes à la propriété intellectuelle, afin d'harmoniser les législations nationales déjà existantes. Les violations concernant les brevets ou les marques déposées ne sont pas couvertes par cette disposition.[1954]

Références à des accords internationaux

Contrairement aux autres cadres juridiques, la Convention sur la cybercriminalité ne désigne pas de façon explicite les actes à criminaliser mais se réfère à un certain nombre d'accords internationaux.[1955] Il s'agit de l'un des aspects critiqués vis-à-vis de l'article10. Outre que cet aspect de la Convention rende plus difficile de déterminer l'étendue de la criminalisation et que ces accords risquent d'être modifiés ultérieurement, la question de savoir si la Convention sur la cybercriminalité oblige les états signataires à signer les accords internationaux, mentionnés à l'article10, se pose. Les rédacteurs de la Convention sur la cybercriminalité ont souligné qu'aucune obligation de ce type ne serait introduite par la Convention du Conseil de l'Europe sur la cybercriminalité.[1956] Les états, qui n'ont pas signé les accords internationaux mentionnés, ne sont donc ni obligés de signer les accords ni contraints de criminaliser les actes liés à des accords qu'ils n'ont pas signés. L'article10 n'impose donc des obligations qu'aux Parties qui ont signé l'un des accords mentionnés.

Elément moral

Du fait de sa nature générale, la Convention sur la cybercriminalité limite la criminalisation aux actes qui ont été commis au moyen d'un système informatique.[1957] Outre les actes commis au moyen d'un système informatique, la responsabilité pénale est limitée aux actes qui sont commis délibérément et sur une échelle commerciale. Le terme « délibérément » correspond à « intentionnellement » qui est utilisé dans les autres dispositions du droit substantiel de la Convention sur la cybercriminalité et tient compte de la terminologie utilisée à l'article 61 de l'Accord sur les aspects des droits de propriété intellectuelle qui touche au commerce (ADPIC)[1958], qui régit l'obligation de criminaliser les violations de la propriété intellectuelle.[1959]

Echelle commerciale

La limitation à des actes qui sont commis sur une échelle commerciale tient compte également de l'APDIC qui exige des sanctions pénales uniquement pour « piratage sur une échelle commerciale ». La plupart des violations de propriété intellectuelle dans des systèmes de partage de fichiers ne sont pas commises sur une échelle commerciale et ne sont donc pas couvertes par l'article 10. La Convention sur la cybercriminalité s'efforce de fixer des normes minimales pour les infractions liées à l'Internet. Aussi, les Parties peuvent-elles aller au-delà du seuil de « l'échelle commerciale » dans la criminalisation des violations de propriété intellectuelle.[1960]

Sans droit

D'une manière générale, les dispositions du droit pénal substantiel, définies par la Convention du Conseil de l'Europe sur la cybercriminalité, exigent que l'acte soit commis « sans droit ».[1961] Les rédacteurs de la Convention sur la cybercriminalité ont souligné que le terme « violation » impliquait déjà que l'acte était commis sans autorisation.[1962]

Restrictions et réserves

Le paragraphe 3 permet aux signataires d'émettre une réserve pour autant que d'autres remèdes efficaces soient disponibles et que la réserve ne déroge pas aux obligations internationales des Parties.

Projet de Convention Internationale de Stanford

Le projet informel[1963] de Convention Internationale de Stanford de 1999 (« Projet Stanford ») n'inclut pas de disposition criminalisant les violations de propriété intellectuelle. Les rédacteurs du projet de Convention de Stanford ont fait remarquer que les infractions en matière de propriété intellectuelle n'étaient pas incluses du fait des difficultés associées.[1964] Au lieu de cela, ils se sont référés directement aux accords internationaux existants.[1965]

6.2.20 Utilisation d'Internet à des fins terroristes

Comme mentionnée ci-dessus, l'expression « utilisation d'Internet à des fins terroristes » est employée pour décrire un ensemble d'activités allant de la diffusion de messages de propagande à des attaques ciblées. La réponse juridique, quant à elle, peut être envisagée selon trois approches différentes et systématiques.

Approches systématiques

Application de la législation déjà existante relative à la cybercriminalité

La première approche consiste à avoir recours à la législation relative à la cybercriminalité qui existe déjà (développée pour couvrir des actes non-terroristes) afin de criminaliser l'utilisation d'Internet à des fins terroristes. Dans ce contexte précis, trois aspects doivent être pris en considération. Tout d'abord, les provisions du droit pénal substantiel, mises en place pour couvrir les actes non-terroristes tels que le brouillage de système[1966], pourraient s'appliquer aux cas de nature terroriste, mais, très souvent, le type de condamnations diffèrera de la législation spécifique au terrorisme. Une telle approche pourrait donc influencer la possibilité d'utiliser des instruments d'enquête sophistiqués, réservés aux enquêtes sur les actes terroristes ou le crime organisé. Ensuite, dans les cas d'utilisation d'Internet à des fins terroristes, l'utilisation d'instruments d'enquête spécifiques à la cybercriminalité est un peu moins problématique, dans la mesure où la plupart des pays ne limitent pas seulement l'utilisation d'instruments d'enquête sophistiqués aux infractions liées à la cybercriminalité, dites traditionnelles, mais aussi à toute infraction impliquant des données informatiques. Enfin, les instruments juridiques régionaux, développés pour faire face au problème de la cybercriminalité et non pas de l'utilisation d'Internet à des fins terroristes en particulier, présentent souvent des exemptions relatives à la coopération internationale, notamment en ce qui concerne les infractions de nature politique. L'article 27, paragraphe 4 a de la Convention du Conseil de l'Europe sur la cybercriminalité en est un exemple.[1967]

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables
[…]
4. Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:
a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.
[…]

La disposition autorise les Parties de la Convention à refuser des demandes d'entraide mutuelle, si elles sont relatives à une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique. Une telle disposition peut sérieusement entraver les enquêtes. Par conséquent, les cadres juridiques spécifiques au terrorisme, comme la Convention du Conseil de l'Europe sur la prévention du terrorisme (2005)[1968], exclut la clause d'exception politique.

Article 20 – Exclusion de la clause d'exception politique
1 Aucune des infractions mentionnées aux articles 5 à 7 et 9 de la présente Convention ne sera considérée, pour les besoins de l'extradition ou de l'entraide judiciaire, comme une infraction politique ou comme une infraction connexe à une infraction politique, ou comme une infraction inspirée par des mobiles politiques. De ce fait, une demande d'extradition ou d'entraide judiciaire basée sur une telle infraction ne pourra être refusée au seul motif que cela concerne une infraction politique ou une infraction connexe à une infraction politique ou une infraction inspirée par des mobiles politiques.
[…]

Utiliser la législation contre le terrorisme déjà existante

La deuxième approche consiste à avoir recours à législation relative au terrorisme qui existe déjà et à engager des poursuites judiciaires contre l'utilisation d'Internet à des fins terroristes. La Convention du Conseil de l'Europe pour la prévention du terrorisme (2005) constitue, par exemple, un tel instrument traditionnel.[1969]

Article 5 – Provocation publique à commettre une infraction terroriste
1. Aux fins de la présente Convention, on entend par « provocation publique à commettre une infraction terroriste » la diffusion ou toute autre forme de mise à disposition du public d'un message, avec l'intention d'inciter à la commission d'une infraction terroriste, lorsqu'un tel comportement, qu'il préconise directement ou non la commission d'infractions terroristes, crée un danger qu'une ou plusieurs de ces infractions puissent être commises.
2. Chaque Partie adopte les mesures qui s'avèrent nécessaires pour ériger en infraction pénale, conformément à son droit interne, la provocation publique à commettre une infraction terroriste telle que définie au paragraphe 1, lorsqu'elle est commise illégalement et intentionnellement.

Article 6 – Recrutement pour le terrorisme
1. Aux fins de la présente Convention, on entend par « recrutement pour le terrorisme » le fait de solliciter une autre personne pour commettre ou participer à la commission d'une infraction terroriste, ou pour se joindre à une association ou à un groupe afin de contribuer à la commission d'une ou plusieurs infractions terroristes par l'association ou le groupe.
2. Chaque Partie adopte les mesures qui s'avèrent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le recrutement pour le terrorisme, tel que défini au paragraphe 1 de cet article, lorsqu'il est commis illégalement et intentionnellement.

La Convention pour la prévention du terrorisme évoquent plusieurs types d'infractions comme notamment la provocation publique à commettre des infractions terroristes et le recrutement pour le terrorisme mais, par exemple, ne présente aucune disposition criminalisant les attaques d'ordre terroriste contre les systèmes informatiques. Par ailleurs, la Convention ne présente aucun instrument procédural. Des instruments procéduraux spécifiques sont souvent requis, tout particulièrement lors des enquêtes sur des infractions relatives à Internet. L'indentification de l'auteur d'une infraction, qui a encouragé des actes terroristes en ayant recours à des sites Internet, exige des instruments sophistiqués tels que la préservation immédiate des données de trafic.

Législation spécifique

La troisième approche consiste à développer une législation spécifique, adressant l'utilisation d'Internet à des fins terroristes.

Exemples de législation spécifique

Comme mentionnée ci-dessus, l'expression « utilisation d'Internet à des fins terroristes » est employée pour décrire un ensemble d'activités allant de la diffusion de messages de propagande à des attaques ciblées. Quant à la réponse juridique, il existe deux grands domaines une réglementation s'avère nécessaire: les attaques de type informatique et le contenu illicite.

Attaques de type informatique

La section 66F de la loi indienne sur les technologies de l'information (Indian Information Technology Act) (2000), amendée en 2008, présente une approche possible de disposition adressant spécifiquement les attaques informatiques d'ordre terroriste:

66F Condamnation des actes relatifs au cyber-terrorisme - Loi sur les technologies de l'information, 2000 [Comme amendé par la loi sur les technologies de l'information (Amendement) de 2008)
(I) Quiconque,
(A) a l'intention de menacer l'unité, l'intégrité, la sécurité ou la souveraineté de l'Inde ou de semer la terreur au sein de sa population ou d'une portion de sa population:
(i) en empêchant l'accès ou en causant le refus d'accès à une personne autorisée à accéder à une ressource informatique; ou,
(ii) en tentant de s'infiltrer ou d'accéder à une ressource informatique sans autorisation ou en outrepassant l'accès autorisé; ou
(iii) en introduisant ou en provoquant l'introduction d'un Programme Malveillant.
et, du fait de cette conduite, provoque ou est susceptible de provoquer le décès de personnes ou leurs blessures, ou d'endommager ou de détruire la propriété ou, interrompt ou est conscient que de tels actes sont susceptibles d'endommager ou d'interrompre la délivrance de biens ou de services essentiels à la vie de la communauté ou, atteint de façon défavorable l'infrastructure d'informations critique comme spécifiée dans la section 70 ou
(B) pénètre ou accède, en toute conscience ou intentionnellement, à une ressource informatique sans autorisation ou en outrepassant l'accès autorisé, et, du fait de cette conduite, accède à des informations, des données ou des bases de données informatiques protégées pour des raisons de Sécurité de l'Etat ou de relations étrangères; ou à toutes informations, données ou bases de données informatiques protégées, avec pour raison de croire que de telles informations, données ou bases de données informatiques, ainsi obtenues, puissent être utilisées pour porter atteinte ou soient susceptibles de porter atteinte aux intérêts de la souveraineté et de l'intégrité de l'Inde, à la sécurité de l'Etat, aux relations amicales avec les Etats étrangers, à l'ordre public, la décence ou la moralité, ou dans une situation d'outrage à la Cour, est l'auteur de diffamations ou incite à une infraction, ou, au profit d'une nation étrangère, d'un groupe d'individus ou autre, commet une infraction de cyber-terrorisme.
(2) Celui qui commet ou conspire dans le but de commettre un acte de cyber-terrorisme sera passible d'une peine d'emprisonnement pouvant s'étendre à perpétuité.

La Section 66F de la loi indienne sur les technologies de l'information (Indian Information Technology Act) ne requiert pas seulement que l'auteur de l'infraction agisse avec l'intention de commettre des actes d'ordre terroriste (« a l'intention de menacer l'unité, l'intégrité, la sécurité ou la souveraineté de l'Inde ou de semer la terreur au sein de sa population ou d'une portion de sa population ») mais aussi que l'infraction commise engendre des conséquences graves comme le décès, les blessures ou la perturbation des services affectant l'infrastructure d'informations critique.

Contenu illicite

Le contenu illicite, tels que les messages de propagande terroriste, est un domaine vis-à-vis duquel les états adoptent tout particulièrement des approches neutres sur le plan technologique. L'Article 10 de la loi fédérale russe 149-FZ du 27/07/2006 sur l'information, les technologies de l'information et la protection de l'information constitue un exemple d'une telle approche neutre sur le plan technologique.

> ***Article 10**. Diffusion d'informations ou distribution d'informations*
> *[…]*
> *6. Il est interdit de diffuser des informations relatives à la propagande de guerre, à la discrimination nationale, raciale ou religieuse, et à l'hostilité ainsi que toutes autres informations dont la diffusion est assujettie à la responsabilité pénale ou administrative.*

Cette disposition n'adresse pas spécifiquement la diffusion de contenu illicite par le biais de réseaux informatiques ou le fait de rendre ce contenu disponible sur de tels réseaux, mais a été rédigée de manière à rester neutre sur le plan technologique.

L'article 3 de l'amendement de 2008 à la Décision-cadre du Conseil de l'UE[1970] relative à la lutte contre le terrorisme[1971] constitue un autre exemple d'approche neutre sur le plan technologique.

> ***Article 3** – Infractions liées aux activités terroristes*
> *1. Aux fins de la présente décision-cadre, on entend par:*
> *(a) «provocation publique à commettre une infraction terroriste», la diffusion ou toute autre forme de mise à disposition du public d'un message, avec l'intention d'inciter à la commission d'un des actes énumérés à*
> *l'article 1er, paragraphe 1, points a) à h), lorsqu'un tel comportement, qu'il préconise directement ou non la commission d'infractions terroristes, crée un danger qu'une ou plusieurs de ces infractions puissent être commises;*
> *(b) «recrutement pour le terrorisme», le fait de solliciter une autre personne pour commettre l'un des actes énumérés à l'article 1er, paragraphe 1, ou à l'article 2, paragraphe 2;*
> *(c) «entraînement pour le terrorisme», le fait de fournir des instructions pour la fabrication ou l'utilisation d'explosifs, d'armes à feu, d'autres armes ou de substances nocives ou dangereuses, ou pour d'autres méthodes ou techniques spécifiques, en vue de commettre l'un des actes énumérés à l'article 1er, paragraphe 1, en sachant que la formation dispensée a pour but de servir à la réalisation d'un tel objectif.*
> *2. Chaque État membre prend les mesures nécessaires pour que soient également considérés comme des infractions liées aux activités terroristes les actes intentionnels suivants:*
> *(a) la provocation publique à commettre une infraction terroriste;*
> *(b) le recrutement pour le terrorisme;*
> *(c) l'entraînement pour le terrorisme;*
> *(d) le vol aggravé commis en vue de réaliser l'un des actes énumérés à l'article 1er, paragraphe 1;*
> *(e) le chantage en vue de réaliser l'un des actes énumérés à l'article 1er, paragraphe 1;*
> *(f) l'établissement de faux documents administratifs en vue de réaliser l'un des actes énumérés à l'article 1er, paragraphe 1, points a) à h), ainsi qu'à l'article 2, paragraphe 2, point b).*
> *3. Pour qu'un acte soit passible de poursuites comme prévu au paragraphe 2, il n'est pas nécessaire qu'une infraction terroriste soit effectivement commise.»*

Les rédacteurs soulignent dans l'introduction que le cadre juridique existant criminalise tout acte visant à aider, à encourager ou à inciter au terrorisme, mais ne criminalise pas la dissémination d'une expertise terroriste sur Internet. Dans ce contexte, les rédacteurs ont fait remarquer qu'« Internet est utilisé pour inspirer et mobiliser des réseaux terroristes locaux et des individus en Europe et, constitue également une source d'informations sur les moyens et les méthodes terroristes, fonctionnant ainsi comme 'un camp d'entraînement virtuel'. »[1972] En dépit du fait que l'utilisation d'Internet à des fins terroristes ait été explicitement mentionnée dans l'introduction, la disposition proposée est rédigée selon une approche neutre sur le plan technologique et par conséquent, couvre à la fois les actes d'entraînement pour le terrorisme réalisés en ligne ou dans le monde réel.[1973] L'une des difficultés relatives à l'application de cette disposition, dans des cas liés à l'Internet, tient à la complexité même de prouver que l'auteur de l'infraction a agi en sachant que les compétences proposées seraient intentionnellement employées à ces fins. Il est assez probable que la nécessité de telles preuves limitera l'applicabilité de la disposition aux guides d'armements en ligne. Comme la plupart des armes et des explosifs peuvent être utilisés pour commettre des crimes courants ainsi que des infractions d'ordre terroriste, la simple publication de ce type d'informations ne prouve pas que la personne les ayant publiées savait comment ces informations allaient être utilisées. Par conséquent, le contexte de la publication (par exemple, le fait qu'elle apparaisse sur un site opéré par une organisation terroriste) devra être pris en considération. Ceci peut s'avérer problématique si l'information est publiée en dehors du contexte d'un autre contenu relatif au terrorisme, comme par exemple, des informations disséminées par le biais de systèmes de partage de fichiers ou de services d'hébergement de fichiers.

L'Article 5 des réglementations chinoises relatives aux réseaux informatiques, à la sécurité, à la protection et à la gestion d'Internet (Computer Information Network and Internet Security, Protection and Management Regulations) constitue un exemple d'une approche spécifique à l'Internet.

> *"**Article 5**: Aucune unité ou individu n'est autorisé à utiliser Internet pour créer, copier, extraire ou transmettre des informations qui:*
>
> *(1) Incitent à résister ou à enfreindre la Constitution ou les lois ou l'exécution des réglementations administratives;*
>
> *(2) Incitent à renverser la gouvernance du régime socialiste;*
>
> *(3) Incitent à diviser le pays, portent atteinte à l'unification nationale;*
>
> *(4) Incitent à la haine ou à la discrimination contre les nationalités ou portent atteinte à l'unité des nationalités;*
>
> *(5) Véhiculent des mensonges ou déforment la vérité, font courir des rumeurs, détruisent le bon ordre de la société;*
>
> *(6) Défendent des superstitions féodales, présentent un contenu aux connotations sexuelles, encouragent le jeu, la violence, le meurtre;*
>
> *(7) Incitent au terrorisme ou incitent autrui à commettre des actes criminels; insultent ouvertement autrui ou déforment la vérité pour calomnier autrui;*
>
> *(8) Injurient la réputation des organes de l'Etat;*
>
> *(9) Encouragent d'autres activités contre la Constitution, la loi ou les réglementations administratives.»*

Cyberguerre

Bien que la question des menaces liées à la cyberguerre soit débattue depuis plusieurs décennies, le débat sur la réponse juridique à apporter s'amorce tout juste. Bien plus que les cyberdélits, la cyberguerre est régie par le droit international. Les Conventions de La Haye, les Conventions de Genève et la Charte des Nations Unies constituent des instruments majeurs du droit international, qui présentent des réglementations régissant les lois relatives à la guerre. Alors que ces instruments sont appliqués de manière régulière et significative aux conflits armés traditionnels, leur application aux attaques informatiques ou de réseaux se trouve confrontée à plusieurs difficultés. Ceci peut être démontré en analysant l'applicabilité de l'article 2 (4) de la Charte des Nations Unies, interdisant l'emploi de la force.

***Art. 2** Charte des Nations Unies*
L'Organisation des Nations Unies et ses Membres, dans la poursuite des buts énoncés à l'Article 1, doivent agir conformément aux principes suivants:
[...]
(4) Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies.
[...]

L'interdiction de l'emploi de la force vise à appliquer une interdiction plus vaste de tous les types de force, exceptés pour ceux s'inscrivant en cohérence avec la Charte des Nations Unies.[1974] Au cours des dernières décennies, l'interdiction de l'emploi de la force, comme mentionnée dans l'article 2 (4), a été mise à l'épreuve à plusieurs reprises. L'une des difficultés principales a été le passage des guerres totales, qui constituaient le centre d'attention principal à l'époque de la ratification de la Charte des Nations Unies, après la Deuxième Guerre Mondiale, aux guerres de petite envergure, bien plus fréquentes de nos jours.[1975] L'inclusion des attaques d'ordre informatique ajoutent une autre dimension à cette complexité, dans la mesure où, non seulement l'envergure mais aussi les méthodes et les outils employés durant le conflit, diffèrent.[1976] Par conséquent, la difficulté principale dans l'application de l'article 2 tient à l'interprétation de l'expression « emploi de la force. » Ni la Charte des Nations Unies, ni aucun instrument international apparenté ne définissent clairement l'expression « emploi de la force. » Il est largement accepté que la Charte des Nations Unies n'interdit pas toutes les formes d'actes hostiles. Les attaques avec des armes conventionnelles sont incluses, par exemple, mais la menace de l'emploi de la force ou de la coercition économique ne le sont pas.[1977]

L'emploi de la force se compose de deux éléments: l'usage des armes et l'implication d'acteurs étatiques. Même si l'importance de ce dernier, en particulier, a été remis en cause par les résolutions du Conseil de Sécurité, après les attaques du 11 septembre, les deux éléments restent essentiels quant à l'interdiction de l'emploi de la force.

Usage des armes/destruction de vies et de propriété

Le premier élément constituant correspond à l'usage des armes. La technologie informatique employée pour commettre des attaques relatives à l'Internet peut à peine être considérée comme une arme traditionnelle, dans la mesure où de telles armes impliquent en général un impact cinétique.[1978] Cependant, la nécessité d'inclure les armes chimiques et biologiques a déjà requis le passage d'une définition fondée sur la notion d'action à une définition fondée sur la notion d'impact. Dans le cadre de cette approche plus globale, les armes pourraient donc être définies comme un outil de destruction de vie ou de propriété.[1979]

Pourtant, même en se basant sur une interprétation plus vaste comme celle-ci, il est difficile de considérer les attaques informatiques ou de réseaux comme l'emploi de la force et la technologie informatique comme une arme, puisque l'impact de ces attaques est différent.[1980] Non seulement les méthodes employées mais aussi leurs conséquences diffèrent par rapport aux conflits armés traditionnels.[1981] Les stratégies militaires traditionnelles, impliquant l'usage d'armes, se concentrent sur l'annihilation physique des capacités militaires de l'ennemi. Les attaques informatiques et de réseaux peuvent, quant à elles, être commises avec un minimum de dommages matériels et de pertes de vies.[1982] Contrairement à une attaque missile, une attaque par déni-de-service qui empêche temporairement l'accès à un site gouvernemental, n'engendre pas de véritables dommages matériels. Cependant, ce serait penser à tort que de prétendre que les attaques informatiques ne mènent à aucune dommage grave. Une attaque par déni-de-service (DoS) contre le système informatique d'un hôpital ou d'une banque du sang peut sérieusement menacer la santé et mettre en danger la vie d'un grand nombre de personnes. La découverte du potentiel impact matériel du ver informatique Stuxnet constitue un autre exemple montrant que les attaques informatiques ne sont pas nécessairement sans conséquences matérielles. Si les attaques informatiques et de réseaux ont un tel impact matériel, alors elles peuvent être considérées comme étant similaires aux armes traditionnelles.[1983]

Conflits entre états

Comme mentionné ci-dessus, le second élément permettant l'application de l'article 2 de la Charte des Nations Unies correspond à l'emploi de la force par un état contre un autre état. En dépit des tendances récentes visant à étendre l'application de la Charte des Nations Unies, les actes commis par des acteurs non étatiques ne sont pas pris en compte par l'article 2 de la Charte des Nations Unies. Il s'agit d'un point tout à fait pertinent dans la prise en compte de la cyberguerre, dans la mesure où — contrairement aux guerres traditionnelles — les acteurs non étatiques y jouent un rôle plus important. La question de la prolifération inquiète sérieusement, du fait que les acteurs non étatiques peuvent acquérir des ressources puissantes pouvant même aller au-delà de celles contrôlées par les états.[1984] Les plus grands botnets comprennent plusieurs millions de systèmes informatiques. Ce nombre est possiblement plus grand que le nombre de systèmes informatiques sous contrôle d'état, disponibles pour des interventions militaires dans la plupart des états. Les capacités des acteurs non étatiques sont extrêmement compétentes, dans la mesure où ils agissent tout d'abord en dehors du cadre juridique international qui unit les états. Ceci donne ainsi lieu à des préoccupations vis-à-vis de l'attribution de responsabilité. L'application de l'article 2 de la Charte des Nations Unies requiert, à ce jour, qu'une attaque informatique puisse être remontée jusqu'à un état. Des cas d'incidents ayant eu lieu en Estonie, en 2007, et en Géorgie, en 2008, démontrent que, dans la plupart des cas, l'identification ou la vérification de la source d'une attaque peut s'avérer être d'une extrême difficulté.

6.3 Preuves numériques

Bibliography (selected): *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf; *Gercke*, Impact of Cloud Computing on the work of law enforcement agencies, published in *Taeger/Wiebe*, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4; *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002; *Hayes*, Forensic Handwriting Examination, 2006; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2; *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital

Investigations, 2010; *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No.1; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1; *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

Grâce, notamment, à la capacité croissante des disques durs[1985] et à la baisse du coût[1986] du stockage de documents numériques par rapport au stockage de documents papier, le nombre de documents numériques ne cesse d'augmenter.[1987] De nos jours, une quantité considérable de données est uniquement stockée sous format numérique.[1988] De plus, les technologies informatiques et de réseaux sont devenues partie intégrante de la vie quotidienne dans les pays développés et, de plus en plus aussi, dans les pays en voie de développement. Par conséquent, les documents électroniques comme les documents textes, les vidéos numériques et les photos numériques [1989] ont un rôle à jouer dans les enquêtes liées à la cybercriminalité et dans les procès qui lui sont associés.[1990]

Pourtant, l'impact de la numérisation et l'importance des preuves numériques vont bien au-delà des enquêtes relatives à la cybercriminalité: même les auteurs d'une infraction traditionnelle sont susceptibles de laisser des traces numériques, comme, par exemple, des informations sur la localisation de leur téléphone portable[1991] ou des recherches suspectes sur des moteurs de recherche.[1992] La possibilité d'avoir recours à des outils d'enquête spécifiques pour le traitement de données et de présenter des preuves numériques au tribunal est donc considérée comme essentielle, à la fois pour les enquêtes relatives à la cybercriminalité comme pour celles liées aux infractions traditionnelles.[1993]

L'utilisation de « preuves numériques » présente un certain nombre de difficultés,[1994] mais ouvre également de nouvelles possibilités pour les enquêtes comme pour le travail des experts en criminalistique informatique et des tribunaux. Dès la première étape de l'enquête, — la collecte de preuves — la nécessité de pouvoir manipuler des preuves numériques a changé le travail des enquêteurs. Ils nécessitent, en effet, des outils d'enquête spécifiques pour mener les enquêtes. Par ailleurs, la disponibilité de tels instruments est particulièrement pertinente si les preuves traditionnelles, comme les empreintes digitales ou la présence de témoins, viennent à manquer. Dans ces cas-là, la collecte et l'analyse correctes des preuves numériques peuvent permettre l'identification et la poursuite en justice réussies de l'auteur de l'infraction.[1995] Pourtant, bien au-delà de la collecte de preuves, la numérisation influence également la façon dont les services chargés de l'application des lois et les tribunaux traitent les preuves.[1996] Alors que les documents traditionnels sont introduits en donnant l'original lors du procès, les preuves numériques

requièrent, dans certains cas, des procédures spécifiques qui ne permettent pas leur conversion en une preuve traditionnelle, comme, par exemple, une version imprimée des documents ou des autres données trouvées.[1997]

Le chapitre suivant offre une vue d'ensemble sur les aspects pratiques et juridiques des preuves numériques et des enquêtes liées à la cybercriminalité.

6.3.1 Définition des preuves numériques

La numérisation et l'utilisation grandissante des TIC ont un impact considérable sur les procédures de collecte de preuves et sur l'emploi de ces dernières lors des procès.[1998] En réponse au développement technique, les preuves numériques ont été acceptées comme nouvelle source de preuve.[1999] Cependant, il n'existe pas une seule définition des preuves numériques ou électroniques.[2000] Le code de la police et des preuves criminelles du Royaume-Uni (UK Police and Criminal Evidence Code) définit les preuves numériques comme correspondant à « toutes les informations contenues sur un ordinateur. »[2001] Une approche plus large définit les preuves numériques comme tout type de données stockées ou transmises en ayant recours à la technologie informatique, qui viennent appuyer la théorie démontrant la commission d'une infraction.[2002]

6.3.2 Importance des preuves numériques dans les enquêtes relatives à la cybercriminalité

Les preuves numériques jouent un rôle important dans plusieurs phases des enquêtes relatives à la cybercriminalité. Il est, en général, possible de distinguer deux phases principales[2003]: la phase d'enquête (identification de preuves pertinentes[2004], collecte et archivage des preuves[2005], analyse de la technologie informatique et des preuves numériques) et, la présentation ainsi que l'utilisation des preuves lors du procès.

La première phase est liée à la criminalistique informatique qui sera expliquée ci-après plus en détails. Le terme « criminalistique informatique » désigne l'analyse systématique des équipements informatiques dans le but de trouver des preuves numériques.[2006] Etant donné que la quantité de données stockées sous format numérique augmente constamment, les enquêteurs se voient confrontés à des problèmes de logistique.[2007] Il est donc important qu'ils adoptent des procédures scientifiques automatisées, notamment en faisant des recherches fondées sur les valeurs de hachage pour trouver des images pédopornographiques connues[2008] ou des recherches par mots-clés[2009], outre les recherches manuelles.[2010] Selon les enquêtes, les experts en criminalistique informatique peuvent analyser le matériel et les logiciels informatiques utilisés par un suspect[2011], restaurer des fichiers effacés[2012], décrypter des fichiers[2013] ou identifier des internautes en analysant les données relatives au trafic.[2014]

La deuxième phase de l'enquête consiste à présenter les preuves numériques devant le tribunal. Comme les informations numériques ne peuvent être rendues visibles que si elles sont imprimées ou montrées à l'aide d'une technologie informatique, cette démarche dépend étroitement de procédures spécifiques et nécessaires.

6.3.3 Importance grandissante des preuves numériques dans les enquêtes relatives aux infractions traditionnelles

Le fait que les enquêteurs puissent chercher des données ou saisir des preuves et que les tribunaux puissent considérer les preuves numériques ne se limite pas uniquement aux enquêtes relatives à la cybercriminalité. En raison de l'intégration grandissante de la technologie informatique dans le quotidien de tout un chacun, les preuves numériques sont en passe de devenir une source importante de preuves, même dans les enquêtes traditionnelles. Lors d'un procès pour meurtre, ayant eu lieu aux Etats-Unis, l'historique des recherches Internet réalisées sur l'ordinateur du suspect avait été enregistré et utilisé pour prouver que, préalablement au meurtre, le suspect avait eu recours aux moteurs de recherche, de manière intensive, afin d'y trouver des informations sur des poisons indétectables.

6.3.4 De nouvelles opportunités pour les enquêtes

Selon que le suspect utilise des services TIC ou internet, il/elle laisse une grande variété de traces numériques derrière lui/elle.[2015] Si, par exemple, un suspect a recours à des moteurs de recherche pour trouver des documents de pédopornographie, sa recherche, puis ses adresses IP et, dans certains cas, voire même des informations supplémentaires relatives à son identité (comme son nom d'utilisateur Google) sont enregistrées.[2016] Les appareils-photos numériques utilisés pour prendre des photos à caractère pédopornographique, incluent, dans certains cas, des renseignements géographiques dans le fichier, permettant aux enquêteurs d'identifier le lieu d'où la photo a été prise, si de telles photos sont saisies sur un serveur.[2017] Les suspects qui téléchargent du contenu illicite à partir de réseaux de partage de fichiers peuvent, dans certains cas, être retrouvés grâce à leur nom d'utilisateur unique, généré lors de l'installation du programme de partage de fichier.[2018] La falsification d'un document électronique peut aussi générer des métadonnées permettant à l'auteur initial du document d'en prouver la manipulation.[2019]

En outre, la neutralité et la sécurité des preuves numériques sont fréquemment citées comme un avantage.[2020] Si comparées à certaines des autres catégories de preuves, telles que les déclarations de témoins, les preuves numériques sont certainement moins susceptibles d'être manipulées d'une façon qui viendrait gêner la conservation des preuves.[2021]

6.3.5 Difficultés

Au tout début de l'utilisation de la technologie informatique, la possibilité d'appliquer la loi pour mener des enquêtes impliquant des données numériques était limitée, en raison du manque d'équipements et d'expertise en criminalistique informatique.[2022] Aussi, l'importance grandissante des preuves numériques a-t-elle vu naître un nombre croissant de laboratoires de criminalistique informatique. Pourtant, bien que les aspects logistiques de la question semblent pouvoir être résolus assez facilement, il subsiste un certain nombre de difficultés.

La raison sous-jacente à ces difficultés reste le fait que, en dépit du nombre de similarités que les preuves numériques et les autres catégories de preuves partagent, il existe, tout de même, entre elles des différences majeures. Certains des principes généraux[2023], comme la nécessité d'utiliser des preuves authentiques, complètes, fiables[2024] et exactes, et la nécessité d'avoir une collecte de preuves réalisée en vertu des obligations légales, sont toujours valides.[2025] Cependant, outre ces similarités, il existe un certain nombre d'aspects donnant aux preuves numériques un caractère unique et requérant ainsi une attention toute particulière, lors de l'utilisation de preuves numériques dans les enquêtes criminelles.

Nécessité d'une recherche scientifique et besoins en formation

Les preuves numériques forment une catégorie de preuves relativement nouvelle dont le domaine se développe rapidement. Malgré le temps très limité imparti à la recherche scientifique de base, il est déjà nécessaire aujourd'hui que les procédures de recherche, de saisie et d'analyse des preuves numériques, soient fondées sur des principes et des procédures scientifiquement fiables.[2026] En dépit du travail de recherche intensif déjà entrepris, plusieurs domaines requièrent l'attention des scientifiques. Il est par conséquent important que la recherche scientifique dans des domaines controversés, comme la fiabilité des preuves en général[2027] ou la quantification des taux d'erreur potentiels,[2028]se poursuive. L'évolution constante de ce secteur et son impact ne se limitent pas seulement à la nécessité d'une recherche scientifique régulière. Etant donné que les développements dans ce domaine sont susceptibles de créer de nouveaux défis auprès des équipes scientifiques[2029], il est donc nécessaire de former régulièrement les experts.

Nécessité de normes juridiques contraignantes

Bien que les technologies informatiques et de réseau soient utilisées dans le monde entier et que les difficultés associées à la recevabilité des preuves numériques dans les tribunaux — en dépit des différents systèmes juridiques existants — soient les mêmes, des normes juridiques contraignantes relatives aux preuves numériques n'ont pas encore été mise en place dans la plupart des états.[2030] A ce jour, seuls quelques pays ont commencé à mettre à jour la législation adéquate afin de permettre aux tribunaux de

recevoir directement des preuves numériques.[2031] Quant au droit pénal substantiel et aux instruments procéduraux utilisés dans la lutte contre la cybercriminalité, ici aussi les normes juridiques, en ce qui concerne les preuves numériques, manquent d'harmonisation internationale.

Aspects quantitatifs

Comme mentionné plus haut, le coût peu élevé[2032] du stockage de documents numériques par rapport à celui des documents papier a favorisé le nombre croissant de documents numériques.[2033] Malgré la disponibilité des outils nécessaires à l'automatisation des processus de recherche[2034], l'identification de la preuve numérique adéquate sur un appareil de stockage pouvant contenir des millions de documents s'avère être un véritable défi logistique pour les enquêteurs.[2035]

Faire confiance aux déclarations des experts

L'analyse et l'évaluation des preuves numériques requièrent des compétences spécifiques et une connaissance technique qui ne font pas nécessairement partie de la formation suivie par les juges, les procureurs et les avocats. Par conséquent, ces derniers comptent de plus en plus sur l'assistance des experts dans le processus de récupération de preuves numériques.[2036] Alors qu'une telle situation n'est pas considérablement différente des autres techniques d'enquête sophistiquées, telles que le séquençage d'ADN, elle invite cependant à un débat nécessaire sur les conséquences d'une telle dépendance. Pour éviter toute influence négative, il est recommandé aux tribunaux de remettre en cause la fiabilité des preuves et d'émettre une certaine réserve quant à l'incertitude associée.[2037]

Fragilité des preuves numériques

Pour les experts, le fait que les données numériques soient extrêmement fragiles et puissent être si facilement effacées[2038] ou modifiées[2039] est alarmant.[2040] Comme les autres catégories de preuves, les données numériques présentent un certain degré d'incertitude.[2041] Pour éviter un impact négatif sur leur fiabilité, la collecte de preuves numériques est souvent soumise à certains critères techniques. L'arrêt d'un système informatique résultera, par exemple, en la perte de toute la mémoire stockée sur la mémoire RAM du système[2042], à moins que des mesures techniques spéciales soient prises pour prévenir de ce processus.[2043] Pour les cas où les données sont stockées dans une mémoire vive, la technique de collecte des preuves peut s'avérer différente du processus de collecte de preuves numériques traditionnelles.[2044] Une approche aussi sophistiquée peut être nécessaire si, par exemple, le suspect a recours à une technologie de cryptage et que les enquêteurs veulent déterminer si les informations stockées dans la mémoire RAM peuvent les aider à accéder aux informations cryptées.[2045]

Les données peuvent être modifiées intentionnellement par l'auteur de l'infraction tout comme accidentellement par les enquêteurs. La perte ou la modification des données peuvent, dans le pire des cas, mener à des condamnations injustifiées.[2046]

En réponse à cette fragilité, le maintien de l'intégrité des preuves numériques, l'un des plus grands principes fondamentaux de la criminalistique informatique, s'avère une nécessité.[2047] Dans ce contexte, la notion d'intégrité peut être définie comme la propriété selon laquelle des données numériques n'ont pas été altérées sans autorisation depuis le moment de leur création, transmission ou stockage par une source autorisée.[2048] La protection de l'intégrité des données est nécessaire pour assurer leur fiabilité et leur exactitude.[2049] La manipulation de preuves de ce type requiert des normes et des procédures particulières afin de maintenir un système de qualité efficace. Ceci comprend des aspects généraux comme l'enregistrement des dossiers, l'utilisation d'une technologie et de procédures largement reconnues, l'intervention d'experts qualifiés uniquement[2050], ainsi que l'application de méthodes spécifiques comme les sommes de contrôle, les algorithmes de hachage et les signatures numériques.[2051] Cependant, les méthodes requises sont coûteuses et ne peuvent pas assurer l'exclusion totale des risques d'altération.[2052]

Quantité limitée de données enregistrées

Il est surprenant pour de nombreux internautes de voir la quantité d'informations stockées sur leurs activités. L'utilisateur moyen n'est peut-être pas conscient que, lorsqu'il/elle se connecte à Internet ou effectue des actions spécifiques comme, par exemple, l'utilisation d'un moteur de recherche[2053], il/elle

laisse des traces. Celles-ci peuvent s'avérer être une source précieuse de preuves numériques lors d'une enquête relative à la cybercriminalité. Néanmoins, les informations numériques générées lors de l'utilisation d'une technologie informatique ne sont pas toutes stockées. De nombreuses actions et informations, comme les clics et les frappes ne sont pas conservées, à moins qu'un logiciel de surveillance spécial n'ait été installé.[2054]

Couche d'abstraction

Même si les activités d'un suspect créent des preuves numériques, ces preuves sont séparées dans le temps des évènements qu'elles enregistrent et constituent, par conséquent, davantage un historique qu'une observation en temps réel.[2055] Par ailleurs, ces preuves ne sont pas nécessairement personnalisées. Si, par exemple, un suspect se rend dans un café Internet pour accéder à des documents de pédopornographie, les traces laissées ne contiennent pas nécessairement des informations relatives à l'identité permettant une identification. A moins que le suspect ne télécharge, dans le même temps, ses e-mails ou n'utilise des services nécessitant une inscription, dans quel cas un lien est alors créé. Mais, comme il n'en est pas toujours le cas, les experts font remarquer que ceci mène à une couche d'abstraction qui peut introduire des erreurs.[2056]

Besoins relatifs aux infrastructures

Depuis des décennies, et même depuis des siècles dans certains pays, la conception des tribunaux suit les mêmes principes. Mises à part les questions de sécurité (par exemple, l'installation de détecteurs de métaux et de scanners) et de confort (par exemple, la climatisation), il est tout à fait possible d'utiliser un tribunal conçu et équipé il y a une centaine d'années, pour un procès pénal.[2057] La nécessité d'utiliser des preuves numériques pose plusieurs difficultés, en termes de couche d'abstraction et de matériel, — les preuves numériques ne pouvant pas être présentées sans outils comme des imprimantes ou des écrans. De tels besoins ont des conséquences sur la conception des tribunaux.[2058] Des écrans doivent être installés pour s'assurer que les juges, le procureur, les avocats de la défense, l'accusé et, bien sûr, le jury puissent suivre la présentation des preuves. L'installation et la maintenance de tels équipements engendrent un coût considérable pour les institutions juridiques.

Un environnement technique en évolution

Comme mentionné plus haut, la technologie ne cesse d'évoluer. Ceci invite donc à une révision constante des procédures et de l'équipement employés ainsi que des formations qui y sont associées, afin d'assurer des enquêtes à la fois adéquates et efficaces.[2059] Avec des versions toujours plus récentes des systèmes d'exploitation et des produits logiciels, la façon de stocker des données pertinentes pour les enquêtes peut changer. Des développements similaires sont notés pour le matériel informatique.[2060] Avant, les données étaient stockées sur des disquettes. Aujourd'hui, les enquêteurs choisiront peut-être de stocker des informations pertinentes sur des lecteurs MP3 ou sur des montres avec port USB. Les difficultés ne se limitent pas au fait de suivre les dernières tendances en matière de technologie informatique.[2061] Les experts scientifiques ont aussi besoin de maintenir l'équipement nécessaire pour pouvoir utiliser des technologies qui ne sont plus disponibles, comme les disquettes 13 cm (5 ¼ pouces). Outre les changements de matériel, les logiciels qui ne sont plus disponibles doivent rester accessibles: les documents créés à partir d'anciens logiciels ne peuvent souvent pas être ouverts sans utiliser le logiciel original.

Il est aussi nécessaire d'étudier attentivement les changements fondamentaux dans le comportement des utilisateurs. Par exemple, la disponibilité des connexions haut-débit et des serveurs de stockage en ligne influence la manière dont les informations sont stockées. Alors que, par le passé, les enquêteurs pouvaient se concentrer sur le domicile du suspect pour trouver des preuves numériques, aujourd'hui, il leur est nécessaire de prendre en considération le fait que les documents puissent être physiquement stockés à l'étranger et accessibles à distance par le suspect, quand cela s'avère nécessaire.[2062] Le recours grandissant au stockage "dans les nuages" présente de nouvelles difficultés auxquelles les enquêteurs doivent faire face.[2063]

6.3.6 Equivalences entres les preuves numériques et les preuves traditionnelles

Une recherche menée en Europe en 2005-2006 a mis en évidence différents points d'équivalence entre les preuves numériques et les preuves traditionnelles, sur les 16 pays analysés.[2064] L'équivalence la plus courante est celle qui existe entre les documents électroniques et les documents papier. Les autres équivalences communément notées sont celles qui existent entre le courrier électronique et le courrier traditionnel, les signatures électroniques et les signatures manuscrites traditionnelles, les actes notariés électroniques et les actes notariés traditionnels.[2065]

6.3.7 Relation entre les preuves numériques et les preuves traditionnelles

En ce qui concerne la relation entre les preuves numériques et les preuves traditionnelles, il est possible de distinguer deux processus: le remplacement des preuves traditionnelles par les preuves numériques, et l'introduction des preuves numériques comme source de preuve complémentaire aux preuves de type traditionnel, comme les documents et les témoins.

L'utilisation grandissante des e-mails à la place des lettres illustre bien comment les preuves numériques viennent à remplacer certaines preuves traditionnelles.[2066] Dans les cas où aucune lettre papier n'est envoyée, les enquêtes doivent se concentrer sur des preuves numériques. Ceci a aussi des implications sur les méthodes disponibles pour analyser et présenter ces preuves. Avant, quand les lettres manuscrites constituaient le moyen dominant de la communication non verbale, l'analyse scientifique se concentrait sur une enquête graphologique.[2067] Déjà à l'époque, quand les machines à écrire devinrent populaires, les méthodes employées dès lors par les experts scientifiques passèrent de l'analyse graphologique à l'analyse dactylographique.[2068] Avec le passage constant des lettres aux e-mails, il est donc nécessaire que les enquêteurs aient plutôt recours à l'analyse[2069]scientifique des e-mails.[2070] Alors que, d'une part, le potentiel des enquêtes en question se trouve limité par l'impossibilité qui en résulte d'avoir recours à des documents papier, d'autre part, l'avantage, pour les enquêteurs, est de pouvoir utiliser désormais des outils leur permettant d'automatiser des enquêtes à partir d'e-mails.[2071]

Bien que dans la majorité des cas impliquant une communication électronique, l'attention sera probablement portée sur les preuves numériques[2072], il n'en reste pas moins que les autres catégories de preuves peuvent jouer un rôle important dans l'identification de l'auteur d'une infraction. Ceci est d'autant plus pertinent que les opérations réalisées sur ordinateur ne laissent pas toutes des traces numériques et que les traces laissées ne peuvent pas toutes être mises en relation avec le suspect.[2073] Si des ordinateurs publics avec accès Internet sont utilisés pour télécharger des documents de pédopornographie, il se peut qu'il soit impossible de mettre en relation le processus de téléchargement avec une personne identifiable, si cette personne ne s'est pas enregistrée[2074] ou n'a pas laissé d'informations personnelles. Par contre, l'enregistrement sur une caméra de vidéosurveillance ou des empreintes digitales sur le clavier peuvent être utiles, si disponibles. Inversement, dans les infractions de types traditionnel où les empreintes digitales, les traces ADN et les témoins jouent un rôle prépondérant, les preuves numériques peuvent, à leur tour, être une source de preuves additionnelle et précieuse. Des informations relatives à la localisation du téléphone du suspect peuvent permettre aux services chargés de l'application des lois d'identifier sa localisation[2075], tout comme des recherches suspectes sur des moteurs de recherche peuvent mener à la localisation de la victime disparue.[2076] Quant aux infractions impliquant des transactions financières (tel que l'échange commercial de pédopornographie[2077]), les enquêtes peuvent aussi prendre en compte les rapports conservés par les institutions financières pour identifier l'auteur de l'infraction. En 2007, une enquête internationale sur des activités de pédopornographie s'est appuyée sur les rapports des transactions financières relatives à l'achat de pédopornographie, pour identifier les suspects.[2078]

6.3.8 Recevabilité des preuves numériques

En ce qui concerne les preuves numériques, il existe deux grands sujets de débat: le processus de collecte des preuves numériques et la recevabilité des preuves numériques devant les tribunaux. Les conditions spécifiques à la collecte de preuves numériques seront abordées plus bas, dans le chapitre suivant relatif au droit procédural. Quant à la recevabilité des preuves numériques, malgré les différences notées avec les preuves traditionnelles, les principes fondamentaux restent les mêmes. En revanche, faire le résumé de ces

principes s'avère être une entreprise difficile puisque, non seulement il existe un manque d'accords internationaux contraignants, mais aussi des différences considérables dans l'approche dogmatique adoptée à l'égard des preuves numériques. Alors que, dans certains pays, la recevabilité ou le refus des preuves numériques restent à l'entière discrétion des juges, d'autres pays ont commencé à développer un cadre juridique pour adresser la question de la recevabilité des preuves devant les tribunaux.[2079]

Légitimité

La légitimité des preuves constitue l'une des exigences les plus fondamentales de la recevabilité des deux catégories de preuves, traditionnelles[2080] et numériques.[2081] Ce principe exige que les preuves numériques aient été collectées, analysées, conservées et finalement présentées devant le tribunal en conformité avec les procédures adéquates et sans violer les droits fondamentaux du suspect.[2082] Les conditions relatives à la collecte, à l'analyse, à la conservation et enfin à la présentation des preuves devant le tribunal, ainsi que les conséquences liées à une violation des droits du suspect diffèrent d'un pays à l'autre. Les principes et les règles qui peuvent éventuellement être violés s'étendent des droits fondamentaux du suspect tels que son droit à la vie privée[2083] au manquement à respecter les exigences procédurales. Souvent, en raison d'une législation inadéquate, les principes généraux relatifs aux preuves sont fréquemment appliqués aux preuves numériques.[2084]

Les exigences relatives à la collecte de preuves numériques sont principalement déterminées par le droit de procédure pénale. Dans la plupart des pays, l'interception de données de contenu nécessite, par exemple, une ordonnance du tribunal, tout comme l'extension d'une recherche à des appareils de stockage à distance nécessite que ces derniers se situent dans le même pays. Si l'interception a lieu sans ordonnance du tribunal, les procédures nécessaires sont alors violées et l'enquête peut donc aller à l'encontre des droits du suspect. Les exigences relatives à la préservation des preuves sont moins souvent définies par la loi.[2085] Cependant, le principe fondamental de la nécessité de protéger l'intégrité des preuves numériques en donne certainement une indication.[2086] Les enquêteurs doivent s'assurer que les preuves ne soient pas altérées sans autorisation dès le moment de leur création, transmission ou stockage par une source autorisée.[2087] La protection de l'intégrité des preuves est nécessaire afin d'en assurer la fiabilité et l'exactitude et d'être en conformité avec le principe de légitimité.[2088] Les procédures de présentation des preuves devant le tribunal sont rarement définies par la loi.

Comme mentionné ci-dessus, non seulement les exigences mais aussi les conséquences d'une violation de procédures ainsi que des droits du suspect varient considérablement.[2089] Alors que certains pays considèrent comme non recevables des preuves uniquement collectées d'une façon qui violent sérieusement les droits du suspect (et non pas, par exemple, si les exigences formelles étaient uniquement violées) et n'excluent pas de telles preuves, d'autres pays — en particulier, ceux appliquant « la doctrine du fruit de l'arbre empoisonné » — appliquent d'autres normes de recevabilité.[2090]

Règle de la meilleure preuve

Pour les juridictions de la « common law », la règle de la meilleure preuve est d'une importance considérable.[2091] Il existe quelques références à une « règle de la meilleure preuve », principalement dans d'anciens dossiers, qui, selon la « common law », spécifie que seule la meilleure preuve disponible d'un fait présenté est considérée comme recevable. Cependant, quel que soit le statut dont cette règle ait jadis joui, il n'y a aujourd'hui que très peu d'autorité en faveur de son maintien et certains affirment même sa fin.[2092]

Aujourd'hui, de manière générale, le fait qu'un élément de preuve donné constitue la meilleure preuve disponible ou pas n'affecterait que son poids dans l'affaire, non pas sa recevabilité.[2093] Etroitement liée à la règle de la meilleure preuve, la « règle des preuves de source primaire » spécifiait auparavant que, dans le cas où des preuves documentaires étaient présentées, seuls les originaux des documents ou une version «finale» de ces documents étaient recevables pour prouver leur contenu et leur authenticité. Cependant, cette ancienne règle a en effet été abandonnée par les tribunaux et, les traces qui en restent sont davantage limitées dans les procès pénaux par la législation (qui désormais autorise, de façon générale, l'utilisation de copies authentifiées).[2094]

La logique d'exiger qu'un document original soit produit quand il est disponible plutôt que de compter sur des copies possiblement insatisfaisantes ou sur la mémoire des témoins, est claire[2095], bien que les techniques modernes amoindrissent les objections faites à la première alternative. Devant l'absence inévitable de la meilleure preuve ou de preuves de source primaire de documents, les tribunaux accepteront des preuves de source secondaire. Ce type de preuves suggère qu'il existe, à première vue, d'autres preuves meilleures que celles-ci. Les documents publics et juridiques sont généralement prouvés par des copies, sans tenir compte de l'absence d'originaux, et, une déclaration contenue dans un document peut, à présent, être prouvée par le présentation d'une copie authentifiée de ce document.[2096] Le principe sous-jacent consiste à réduire les risques de mauvaises transcriptions, de témoignages erronés quant au contenu du document et de modification frauduleuse non détectée.[2097] La règle, dans son interprétation stricte, autorise les preuves de source secondaire (sous forme de copies) quand l'original a été perdu.

Dans le cas des preuves numériques, un certain nombre de questions se posent dans la mesure où il est nécessaire de déterminer ce qui constitue le document original.[2098] Comme les données numériques peuvent en général être copiées sans perte de qualité et que la présentation des données originales devant le tribunal n'est pas toujours possible dans tous les cas, la règle de la meilleure preuve semble être incompatible avec les preuves numériques. Les tribunaux ont cependant commencé à adapter la règle aux nouvelles évolutions technologiques en acceptant une copie électronique aussi bien que le document original.[2099] Dans cette interprétation plus large, la règle de la meilleure preuve ne nécessite pas de témoignage écrit ou de déclaration de témoins dans chaque cas, mais que la meilleure preuve de son contenu, pouvant être obtenue, soit utilisée.[2100] Par ailleurs, la règle de la meilleure preuve a été enchâssée dans la plupart des régimes légaux, établis dans le domaine de la « common law ».[2101]

Règle contre les preuves par ouï-dire

La règle contre la preuve par ouï-dire constitue un autre principe tout particulièrement pertinent dans les pays régis par la « common law ».[2102] Les preuves par ouï-dire correspondent aux preuves données par un témoin lors d'un procès, au sujet d'une déclaration faite par une autre personne n'étant pas présente dans le tribunal, quand de telles preuves sont proposées pour prouver la véracité de la déclaration.[2103] Dans le cadre de la « common law », les preuves par ouï-dire étaient, en général, irrecevables. Cependant, cette règle a été abolie, au Royaume-Uni, pour les procès civils par le Civil Evidence Act (1995), qui permet la recevabilité des preuves par ouï-dire soumises à des exigences légales et, préserve un certain nombre d'exceptions de la « common law » à la règle contre les preuves par ouï-dire.[2104]

Selon la règle de la « common law » contre les preuves par ouï-dire, une affirmation autre que celle faite par une personne lors d'un témoignage oral, au cours d'un procès, et présentée comme preuve des faits cités, n'est pas recevable.[2105] Une déclaration hors du tribunal, dans le cadre de la règle, renvoie à toute déclaration autre que celle faite par un témoin au cours de son témoignage, et peut inclure notamment, une déclaration faite au cours d'un procès antérieur. Par conséquent, cette déclaration a pu être faite sans prêter serment ou en prêtant serment, oralement, par écrit ou même par le biais de signes ou de gestes, par quiconque, appelé ou non comme témoin au cours du procès en question.[2106] En outre, la règle vise à permettre la conduite d'un contre-interrogatoire du véritable témoin et la mise en évidence des points faibles d'une déclaration.[2107] Il est plutôt nécessaire qu'un témoin, connaissant les faits personnellement, prouve cela directement. Non seulement les déclarations d'un témoin peuvent contenir des preuves par ouï-dire qui ne sont pas recevables mais il peut aussi en être de même pour les pièces à conviction.[2108] Un certain nombre de raisons ont été avancées pour justifier la règle de la « common law » contre les preuves par ouï-dire, comme notamment le risque d'avoir des preuves fabriquées, renvoyant au manque de fiabilité potentiel des preuves par ouï-dire. Les règles régissant la recevabilité des preuves par ouï-dire s'appliquent désormais si (et seulement si) le but, ou l'un des buts de la personne faisant la déclaration, semble aux yeux de la cour, avoir poussé une autre personne à croire le contenu de la preuve en question, ou à pousser une autre personne à agir ou une machine à fonctionner sur le prémisse que le contenu de la preuve est conforme à la déclaration.[2109]

Etant donné que les données collectées lors d'une enquête (comme par exemples des fichiers journaux) ont pour but de prouver la véracité du contenu de la preuve numérique-même, l'application stricte de la règle s'avère problématique à une époque, où, très souvent, les preuves numériques constituent la

catégorie la plus pertinente de preuves dans un procès, et où, certains pays, régis par la « common law », ont commencé à mettre en place des exceptions légales à la règle contre les preuves par ouï-dire.[2110] Les preuves produites par des ordinateurs, des appareils-photos ou d'autres machines, excluant une déclaration humaine, ne peuvent constituer des preuves par ouï-dire.[2111] Dans le cadre de la « common law », il était communément accepté que les documents visuels, même si de création humaine, ne constituaient pas des « déclarations » des faits qu'ils étaient censés représenter et, par conséquent, ne pouvaient être considérés comme des preuves par ouï-dire. Cependant, aujourd'hui, il existe une déposition explicite en faveur du contraire.[2112]

Là où aucune exception légale n'existe, l'application de la règle aux preuves numériques est remise en question, notamment par le fait qu'elle ne peut s'appliquer que pour des documents qui contiennent eux-mêmes des affirmations faites par des êtres humains. Dans un tel contexte, toute information générée mécaniquement et sans intervention humaine ne serait donc pas considérée comme une preuve par ouï-dire potentielle[2113], à moins que le processus de création du programme ne soit utilisé comme argument pour pouvoir appliquer la règle même dans ces cas-là.[2114]

Pertinence/Efficacité

La pertinence et l'efficacité constituent d'autres conditions communes à la recevabilité des preuves numériques.[2115] Si l'on prend en considération la quantité de données stockées sur un ordinateur privé, dont seulement une infime proportion peut s'avérer pertinente dans l'affaire, on peut alors comprendre l'importance pratique de ce critère dans une enquête relative à la cybercriminalité. L'application de ce critère est essentiel pour à la fois limiter la collecte de preuves et leur présentation au tribunal. Contrairement aux preuves traditionnelles, pour lesquelles certains éléments de preuve inutiles peuvent tout simplement être ignorés lors de la collecte, le processus de sélection est plus difficile lorsqu'il s'agit de preuves numériques[2116], puisque, au moment où le matériel informatique est saisi, il est presque impossible de déterminer si les appareils de stockage en question contiennent des informations pertinentes ou non.

Transparence

Contrairement aux opérations de perquisition et de saisie traditionnelles, qui sont menées ouvertement et garantissent ainsi que le suspect soit informé du déroulement de l'enquête, les outils d'enquête sophistiqués comme l'interception de communication en temps réel n'impliquent pas une telle obligation d'information. Malgré les moyens techniques, les services chargés de l'application des lois ne sont pas autorisés, dans tous les pays, à mener des opérations dissimulées, ou du moins, il est requis que le suspect en soit informé après les opérations en question. L'usage de la transparence, pendant l'intégralité du processus de collecte, d'analyse et d'utilisation des preuves devant un tribunal, donne au suspect la possibilité de remettre en cause la légitimité et la pertinence des preuves collectées.

6.3.9 Cadre juridique

Alors que des dispositions de droit pénal substantiel adressant les formes les plus communes de cyberdélits existent aujourd'hui dans un grand nombre de pays, la situation en ce qui concerne les preuves numériques reste différente. Seuls quelques pays ont jusqu'à présent adressé les aspects spécifiques relatifs aux preuves numériques et, il manque, par ailleurs, des normes internationales contraignantes.[2117]

Loi type du Commonwealth sur les preuves électroniques (2002)

En 2000, les ministres de la Justice de petites juridictions du Commonwealth décidèrent de créer un groupe de travail afin de développer un modèle de législation relatif aux preuves électroniques. D'après la principale conclusion de l'analyse comparative de la loi à laquelle est arrivé le groupe d'étude, quant à la recevabilité des preuves numériques, la fiabilité du système, par le biais duquel les preuves numériques sont créées, est plus important que le document-même. Le modèle de loi de 2002[2118], fondé sur la législation de Singapour[2119] et du Canada[2120], reflète ces conclusions et englobe les aspects les plus pertinents des preuves numériques à l'égard des pays régis par la « common law », telles que l'application de la règle de la meilleure preuve[2121] et l'intégrité des preuves numériques.

Recevabilité Générale

3. Aucune disposition dans les règles de preuve ne doit s'appliquer dans le but de nier la recevabilité d'un document électronique en tant que preuve, pour la simple raison qu'il s'agisse d'un document électronique.

La section 3 contient un élément commun aux cadres juridiques cherchant à réguler les divers aspects des preuves numériques que l'on peut trouver similairement, par exemple, dans l'article 5 de la Directive du Parlement Européen de 1999 pour les signatures électroniques. [2122] La disposition vise à assurer que les preuves numériques ne soient pas recevables *en soi*. A cet égard, la section 3 établit les fondements de l'utilisation des preuves numériques dans les procès. Cependant, la recevabilité des preuves n'est pas garantie sur le simple fait que la preuve soit numérique. Il est donc nécessaire que les preuves numériques satisfassent aux règles de preuves communes. Si la preuve est une preuve par ouï-dire, elle ne devient pas recevable en raison de l'existence de la section 3.

Portée de la Loi

4. *(1) Cette Loi ne modifie aucune disposition de la « common law » ou de la règle légale relative à la recevabilité des preuves ou des documents, excepté pour les règles relatives à l'authentification et à la meilleure preuve.*
(2) Un tribunal peut avoir à considérer une preuve sous la présente Loi, en appliquant toute règle de la « common law » ou règle légale, relatives à la recevabilité des documents.

Application de la Règle de la Meilleure Preuve

6. *(1) Dans tout procès, sujet à la sous-section (b), où la règle de la meilleure preuve est applicable vis-à-vis des documents électroniques, la règle sera satisfaite sur preuve de l'intégrité du système d'enregistrement électronique dans lequel ou, par le biais duquel, les données ont été enregistrées ou stockées.*
(2) Dans tout procès, au cours duquel une version imprimée d'un document électronique a été manifestement ou pertinemment présentée, utilisée comme appui ou comme version écrite des informations enregistrées ou inscrites sur le document imprimé, alors cette version imprimée fait office de référence dans le cadre de la règle de la meilleure preuve.

Comme précisé ci-dessus, certains des critères relatifs aux preuves numériques sont en conflit potentiel avec les principes traditionnels de la recevabilité des preuves. Ceci est particulièrement pertinent en ce qui concerne la règle de la meilleure preuve, qui est d'une grande importance dans les pays régis par la « common law ».[2123] L'objectif de la règle de la meilleure preuve vise à minimiser les risques de mauvaises transcriptions, de déclarations erronées quant au contenu du document et de falsifications insoupçonnées. [2124] Le principe de recevabilité des preuves requiert que les preuves documentaires constituent les meilleures preuves mises à disposition de la Partie en question. Que les preuves numériques *en soi* soient exclues ou non, reste une question controversée.[2125] La section 4 et la section 6 de la loi type du Commonwealth sur les preuves électroniques constituent des exemples d'exemption légale. Dans ce contexte, la section 4 précise, tout d'abord, que le modèle de loi ne modifie uniquement que les principes d'authentification et de meilleure preuve. En réponse à cette clarification d'ordre général, la section 6 modifie la règle de la meilleure preuve afin d'assurer que les preuves numériques ne soient pas recevables *en soi*. Selon la section 6, les preuves numériques ne sont pas irrecevables en raison de la règle de la meilleure preuve, à condition que l'intégrité du système ayant généré les données soit prouvée.

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique (2002)

Le projet du Modèle de Loi du Commonwealth sur l'informatique et les délits liés à l'informatique a été présenté en 2002.[2126] Outre la présentation de dispositions de droit pénal substantiel et d'instrument procéduraux, ce document inclut aussi une disposition spécifique, relative aux preuves numériques.

Preuves
20. *Dans un procès jugeant une infraction contre une loi du [pays où a lieu le procès], le fait que:*
(a) il y ait allégation d'une infraction commise à l'encontre d'un système informatique; et
(b) des preuves aient été générées à partir de ce système informatique;
n'interdit pas de soi-même la recevabilité des preuves.

Cette approche est similaire à l'article 3 de la loi type du Commonwealth sur les preuves électroniques de 2002, qui est plus spécifique.

6.4 Compétence

Bibliography (selected): *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004. *Hirst,* Jurisdiction and the Ambit of the Criminal Law, 2003; *Inazumi,* Universal Jurisdiction in Modern International Law, 2005; *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf; *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 69 et seq; *Sachdeva*, International Jurisdiction in Cyberspace: A Comparative Perspective, Computer and Telecommunications Law Review, 2007,, page 245 et seq; *Scassa/Currie*, New First Principles? Assessing the Internet's Challenges to Jurisdiction, Georgetown Journal of International Law, Vol. 42, 2001, page 117 et seq, available at: http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF; United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm; *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf; *Van Dervort*, International Law and Organizations: An Introduction, 1998; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

6.4.1 Introduction

La cybercriminalité est une infraction typiquement transnationale, impliquant différentes juridictions. Il n'est pas inhabituel que plusieurs pays soient impliqués. L'auteur de l'infraction a pu agir depuis un pays A, utilisé un service Internet dans un pays B et la victime peut se trouver dans un pays C. Une telle situation pose une réelle difficulté quant à l'application du droit pénal[2127] et suscite des interrogations quant à savoir quels pays ont compétence, quels pays devraient se charger de l'enquête ou encore de quelle manière résoudre les conflits. Alors qu'une telle situation peut déjà paraître complexe, il est nécessaire de prendre en considération que, si l'infraction implique, par exemple, des services de « cloud computing » ou d'Internet «dans les nuages», davantage de juridictions peuvent être sollicitées.[2128]

Le terme « compétence» est employé pour désigner des questions juridiques variées et différentes.[2129] Selon les principes du droit international public, le terme « compétence» désigne l'autorité que détient un état souverain de réguler certaines conduites.[2130] Il s'agit donc d'un aspect appartenant à la souveraineté nationale.[2131] Cependant, dans le contexte d'une enquête relative à la cybercriminalité, le terme « compétence » renvoie à l'autorité que détient un état d'appliquer ses lois nationales.[2132] En général, l'application de la loi ne permettra la mise en place d'une enquête que si le pays a compétence pour agir de la sorte.

6.4.2 Les différents principes de compétence

Il est possible de différencier plusieurs principes distincts de compétence.

6.4.3 Principe de territorialité / Principe de territorialité objective

Le principe de territorialité [2133] est un principe absolument fondamental ainsi que la base la plus fréquente de la compétence. Il s'applique si une infraction, quelle que soit la nationalité de son auteur ou de la victime, est commisse sur le territoire d'un Etat souverain.[2134] Ce principe est plus particulièrement pertinent du fait que le concept de compétence n'a, en général, de sens que s'il peut être appliqué et que l'application de la loi exige des mesures de contrôle (habituellement limitées au territoire national). L'article 22, paragraphe 1.a) de la Convention du Conseil de l'Europe sur la cybercriminalité incarne l'une des approches de codification informatique des principes de territorialité.

Article 22 – Compétence
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:
a. sur son territoire; ou
b. à bord d'un navire battant pavillon de cette Partie; ou
c. à bord d'un aéronef immatriculé selon les lois de cette Partie; ou
d. par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.
[…]

Ces dispositions ont une dimension informatique spécifique puisqu'elles renvoient explicitement aux infractions reprises aux articles 2 à 11 de la Convention sur la cybercriminalité.

Toutefois, leur application à des affaires de cybercriminalité suscite certaines difficultés. Il est indubitable qu'une infraction a été commise lorsque son auteur et la victime sont physiquement présents dans le pays au moment où le contrevenant accède illégalement à l'ordinateur de sa victime. Mais peut-on considérer que l'infraction a été commise sur le territoire d'un Etat si le contrevenant a agi depuis l'étranger d'où il a accédé à l'ordinateur de sa victime, situé dans ce pays-là ?

Ces cas ont une dimension extraterritoriale. Toutefois, dans l'affaire « Lotus », la Cour internationale de justice était d'avis que, même dans les cas où les pays ne faisaient valoir leur compétence que sur la base de la territorialité, des agissements extraterritoriaux pouvaient être considérés comme ayant été commis sur le territoire si l'un des éléments constitutifs de l'infraction (en particulier son effet) s'est déroulé dans le pays en question.[2135] Cette doctrine, également connue sous le nom de « principe de la territorialité objective [2136]», est particulièrement pertinente pour les affaires de cybercriminalité.[2137] Cependant, le fait qu'un logiciel malveillant envoyé par un contrevenant peut affecter des ordinateurs dans plusieurs pays vient rappeler qu'une définition aussi vaste de la territorialité peut facilement entraîner des conflits de compétence.[2138] Le risque de conflits potentiels augmente encore si le principe de territorialité est appliqué à des affaires où ni le contrevenant, ni la victime ne se trouvent sur le territoire national. Seule l'infrastructure située sur ce territoire a été utilisée pour commettre l'infraction, par exemple si un courrier électronique au contenu illicite a été envoyé par le biais d'un fournisseur de messagerie dans un pays donné ou si un site Internet au contenu illicite est stocké sur le serveur d'un hébergeur dans ce pays.

Cette approche relativement large a, entre autres, été codifiée à la section 11.3 (b) de la loi singapourienne sur l'utilisation abusive de l'informatique de 2007 (*Singapore Computer Misuse Act*).

Champ d'application territorial des infractions couvertes par cette loi
[…]
11. — (1) Sous réserve de l'alinéa (2), les dispositions de cette loi s'appliquent à l'égard des personnes concernées, quelle que soit leur nationalité ou citoyenneté, à Singapour ainsi qu'en dehors de son territoire.
(2) Lorsqu'une infraction a été commise en vertu de cette loi par un individu où que ce soit hors de Singapour, il sera traité comme si l'infraction avait été commise sur le territoire singapourien.
(3) Aux fins de cette section, la présente loi s'applique à l'infraction en cause si:
(a) l'accusé se trouve à Singapour au moment des faits; ou
(b) l'ordinateur, le programme ou les données se trouvent à Singapour au moment des faits.

On peut même déduire de cette approche large l'applicabilité de la législation singapourienne aux données ne faisant que transiter par les systèmes informatiques du pays.[2139]

6.4.4 Principe du pavillon

Le principe du pavillon est étroitement lié au principe de territorialité, mais étend l'application de la législation nationale aux avions et navires.[2140] L'existence de solutions d'accès à Internet pour les transports aérien et maritime interroge sur l'applicabilité du droit pénal aux cas où le contrevenant, la victime ou les systèmes informatiques touchés ne se trouve(nt) pas sur le territoire d'un pays, mais hors de ses frontières, à bord d'un navire ou d'un avion.

L'article 22, paragraphes1.b et 1.c de la Convention du Conseil de l'Europe sur la cybercriminalité est un exemple d'une approche visant à réglementer de tels cas.

Article 22 – Compétence
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux article 2 à 11 de la présente Convention, lorsque l'infraction est commise:
a. sur son territoire; ou
b. à bord d'un navire battant pavillon de cette Partie; ou
c. à bord d'un aéronef immatriculé selon les lois de cette Partie; ou
d. par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.
[…]

6.4.5 Théorie des effets / Principe de protection

La théorie des effets s'applique à la détermination de la compétence en cas d'infraction commise par un ressortissant étranger hors du territoire, alors qu'aucun de ses agissements ne s'est déroulé sur celui-ci, mais qu'il y a eu un effet substantiel.[2141] Le principe de protection établissant une compétence dans des cas similaires où un intérêt fondamental de la nation est en jeu y est étroitement lié. Etant donné l'absence sur le territoire du contrevenant, de la victime ou de l'infrastructure utilisée, les liens avec ce pays sont ténus et l'application du principe fait l'objet de controverses.[2142]

6.4.6 Principe de la nationalité active

Le principe de nationalité s'applique lorsqu'une compétence est exercée en raison des activités de ressortissants situés à l'étranger.[2143] Il est associé au pouvoir de l'Etat d'encadrer le comportement de ses ressortissants tant sur son territoire qu'à l'étranger. Ce principe est plus fréquent dans les pays de droit romain que dans ceux de *common law*.[2144] Par conséquent, ces derniers tendent à compenser l'absence de compétence sur la base du principe de nationalité par une interprétation plus large du principe de territorialité.

Le principe de la nationalité active est moins pertinent dans les affaires de cybercriminalité puisque les délits perpétrés sur Internet peuvent l'être sans quitter le territoire national. Cependant, il peut être particulièrement important dans un contexte de production de matériel pédopornographique destiné à être diffusé par voie informatique.[2145]

L'article 22, paragraphe1.d de la Convention du Conseil de l'Europe sur la cybercriminalité est un exemple d'approche visant à encadrer le principe de nationalité.

Article 22 – Compétence
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux article 2 à 11 de la présente Convention, lorsque l'infraction est commise:
a. sur son territoire; ou

b. à bord d'un navire battant pavillon de cette Partie; ou
c. à bord d'un aéronef immatriculé selon les lois de cette Partie; ou
d. par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.
[…]

6.4.7 Principe de la nationalité passive

Le principe de la nationalité passive est associé à une compétence exercée sur la base de la nationalité de la victime. Etant donné son chevauchement avec le principe de territorialité, il n'est pertinent que si un ressortissant est devenu victime d'une infraction alors qu'il résidait hors du pays. L'application de ce principe fait l'objet de controverses,[2146] en particulier parce qu'il indique que le droit étranger est insuffisant pour protéger les non ressortissants. Toutefois, ces dernières décennies l'ont vu de plus en plus souvent accepté.[2147]

La section 7 du Code pénal allemand est une codification, non spécifique à Internet, du principe de la nationalité passive.

Section 7
Infractions commises à l'étranger — Autres cas
(1) Le droit pénal allemand s'applique aux infractions commises à l'étranger à l'encontre d'un ressortissant allemand, si le fait incriminé est une infraction pénale là où il a été perpétré ou si ce lieu n'est placé sous aucune juridiction pénale.

6.4.8 Principe de l'universalité

Le principe de l'universalité établit une compétence pour des infractions spécifiques où les intérêts de la communauté internationale sont en jeu.[2148] Ce principe est particulièrement pertinent en cas de délit grave, comme les crimes contre l'humanité ou les crimes de guerre.[2149] Toutefois, plusieurs pays reconnaissant ce principe ont voulu le développer[2150], ce qui a eu pour conséquence qu'il s'applique aussi, dans certaines circonstances, à la cybercriminalité.

La section 6.6 du Code pénal allemand est un exemple de dispositions applicables à la cybercriminalité.

Section 6
Infractions commises à l'étranger à l'encontre d'intérêts juridiques protégés au niveau international
Le droit pénal allemand s'applique également, quelle que soit la législation du lieu où elles ont été perpétrées, aux infractions suivantes, commises à l'étranger:
1. (abrogé);
2. infractions impliquant l'énergie nucléaire, des explosifs et des radiations au titre des sections 307, 308 (1) à (4), 309 (2) et 310;
3. attentats contre le trafic aérien et maritime (section 316-c);
4. traite d'êtres humains à des fins d'exploitation sexuelle ou de travail et complicité de traite d'êtres humains (sections 232 à 233-a);
5. trafic de drogues illicite;
6. distribution de matériel pornographique au titre des sections 184-a, 184-b (1) à (3) et 184-c (1) à (3), associées à la section 184-d, 1ère phrase;
[...]

Invoquant la section 6.6, l'Allemagne peut faire valoir sa compétence sur des sites Internet proposant du matériel pédopornographique au téléchargement, même si ni l'opérateur du site, ni ses serveurs ne sont situés en Allemagne et qu'aucun internaute allemand n'a accédé à cette page.

6.5 Droit procédural

Bibliography (selected): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1; *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801; *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*; *Gercke/Tropina*, From Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf; *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1.

6.5.1 Introduction

Comme nous l'avons expliqué dans les sections ci-dessus, la lutte contre la cybercriminalité exige des dispositions de droit pénal matériel adaptées.[2151] Dans les pays de droit romain, les services répressifs compétents ne peuvent enquêter sur ce type d'infraction en l'absence de telles dispositions. Mais les besoins des forces de l'ordre dans la lutte contre la cybercriminalité ne se limitent pas aux dispositions de

droit pénal matériel.[2152] Afin de mener les enquêtes qui s'imposent, elles doivent suivre des formations et disposer de l'équipement et des instruments de procédure adéquats leur permettant de prendre les mesures nécessaires pour identifier le contrevenant et rassembler les preuves exigées dans le cadre de poursuites pénales.[2153] Ces mesures peuvent être identiques à celles prévues dans d'autres enquêtes non liées à la cybercriminalité. Mais, étant donné que le contrevenant n'est pas forcément présent, voire proche de la scène du crime, il est très probable que les enquêtes sur la cybercriminalité doivent être menées différemment des enquêtes classiques.[2154]

La raison pour laquelle il convient d'utiliser d'autres techniques d'enquête s'explique par l'indépendance du lieu d'action et de la scène du crime. Dans la plupart des cas, c'est l'association de plusieurs des défis exposés ci-dessus se posant aux autorités répressives qui donnent aux enquêtes sur la cybercriminalité leur dimension particulière.[2155] Si le contrevenant se trouve dans un autre pays[2156], qu'il utilise des services permettant une communication anonyme et, de plus, commet l'infraction par le biais de différents terminaux Internet publics, son crime peut difficilement faire l'objet d'une enquête basée sur des instruments traditionnels, comme les seules perquisitions et saisies. Afin d'éviter tout malentendu, il est important de souligner que les enquêtes en matière de cybercriminalité exigent un travail de détective classique ainsi que l'application de méthodes d'enquête traditionnelles, mais que celles-ci ne suffisent pas à résoudre les défis auxquels elles sont confrontées. [2157]

Certains pays ont d'ores et déjà développé de nouveaux instruments permettant à leurs autorités répressives d'enquêter sur la cybercriminalité ainsi que sur des délits traditionnels exigeant l'analyse de données informatiques.[2158] Comme cela est le cas en matière de droit pénal matériel, la Convention du Conseil de l'Europe sur la cybercriminalité contient un ensemble de dispositions reflétant des normes minimales largement reconnues sur les instruments de procédure exigés dans le cadre d'enquêtes sur la cybercriminalité.[2159] L'aperçu ci-après fera donc référence aux instruments proposés par cette convention internationale tout en soulignant les approches nationales qui vont au-delà des dispositions de la Convention sur la cybercriminalité.

6.5.2 Récupération de données sur ordinateur et enquêtes sur Internet (informatique judiciaire)

Le terme d'informatique judiciaire est utilisé pour décrire la collecte systématique de données et l'analyse de technologies informatiques dans le but de rechercher des preuves numériques.[2160] Une telle analyse se déroule normalement une fois l'infraction commise.[2161] Elle représente donc un élément essentiel en cas de délit informatique et d'enquête cybercriminelle. Les enquêteurs chargés de ces investigations sont confrontés à plusieurs défis décrits en détail au chapitre 3.

La mesure dans laquelle des experts peuvent éventuellement participer aux démarches d'informatique judiciaire est un signe de leur importance dans le cadre de l'enquête. De plus, le succès des enquêtes sur Internet dépend de la disponibilité des ressources policières, d'où la nécessité d'une formation. Ce n'est que si les enquêteurs sont formés à l'informatique judiciaire ou ont accès à des experts en la matière que l'enquête et les poursuites contre les cybercriminels peuvent aboutir.

Définition

Il existe plusieurs définitions de l'« informatique judiciaire ».[2162] Elle peut être définie comme « l'examen des équipements et systèmes informatiques dans le but d'obtenir des informations dans le cadre d'une enquête civile ou pénale ».[2163] Lorsqu'ils commettent leur délit, les criminels laissent des traces.[2164] Ceci est vrai pour les enquêtes traditionnelles comme pour les enquêtes informatiques. La principale différence entre une enquête traditionnelle et une investigation cybercriminelle est que cette dernière exige généralement des techniques d'analyse des données spécifiques et qu'elle peut être facilitée par l'utilisation d'outils logiciels spécialisés.[2165] Outre les instruments de procédure adéquats, une telle analyse exige des autorités qu'elles disposent des compétences nécessaires pour gérer et analyser les données pertinentes. Selon les délits et les technologies informatiques impliquées, les exigences en matière d'outils de procédure d'enquête et les techniques d'analyse policière diffèrent [2166] et présentent des défis particuliers.[2167]

Phases de l'enquête policière

Il est en général possible de faire la distinction entre deux grandes étapes:[2168] l'étape d'investigation (identification des preuves pertinentes[2169], collecte et préservation des éléments de preuve[2170], analyse des technologies informatiques et des preuves numériques), suivie de la présentation et de l'utilisation de ces preuves en justice. Afin d'expliquer les différentes activités concernées, ce chapitre divise le modèle en quatre étapes.

Procédures d'identification des preuves

L'augmentation des capacités[2171] des disques durs ainsi que la baisse du coût[2172] de stockage des documents numériques[2173] par rapport aux documents physiques expliquent la hausse constante du nombre de documents numériques. Etant donné la nécessité de concentrer les enquêtes sur les preuves pertinentes afin d'éviter leur irrecevabilité, il convient de prêter une attention toute particulière à l'identification des preuves.[2174] Par conséquent, les experts judiciaires jouent un rôle important dans la conception des stratégies d'enquête et la sélection des preuves pertinentes. Ils peuvent, par exemple, déterminer l'emplacement de ces preuves dans des systèmes de stockage de grande taille. Cela permet aux enquêteurs de limiter l'étendue de leurs recherches pour se concentrer sur les parties de l'infrastructure informatique pertinentes pour leurs investigations; une telle approche permet aussi aux enquêteurs d'éviter de procéder à des saisies inopportunes et à grande échelle de matériel informatique.[2175] Ce processus de sélection est important puisqu'il existe plusieurs types de périphériques de stockage qui peuvent rendre l'identification du lieu de stockage des preuves pertinentes difficile.[2176] C'est particulièrement vrai si le suspect ne stocke pas localement les informations, mais fait appel à des solutions de stockage à distance. La disponibilité de l'accès à haut débit et de serveurs de stockage à distance a influencé la façon dont les informations sont stockées. Si le suspect stocke des informations sur un serveur situé dans un autre pays, ce simple fait peut rendre plus difficile la saisie de preuves. L'analyse judiciaire peut, dans ce genre de cas, être utilisée pour déterminer si des services de stockage à distance ont été utilisés.[2177] L'identification des informations numériques pertinentes ne se limite pas aux seuls fichiers. Les bases de données d'outils logiciels, accessibles par le biais des systèmes d'exploitation pour identifier rapidement les fichiers, peuvent également contenir des informations pertinentes.[2178] Même les fichiers temporaires, générés par l'ordinateur, peuvent contenir des preuves utiles dans le cadre de procédures pénales.[2179]

Le rôle des experts judiciaires à l'heure de déterminer les bons instruments de procédure est un autre exemple de la nécessaire identification des preuves. Plusieurs pays autorisent leurs forces de l'ordre à mener deux types d'observation en temps réel: la collecte des données relatives au trafic et l'interception des données relatives au contenu. En général, cette dernière approche est plus intrusive que la collecte des données relatives au trafic. Les experts judiciaires peuvent déterminer si la collecte des données relatives au trafic suffit à apporter la preuve de la perpétration d'un crime et ainsi aider les enquêteurs à atteindre le bon équilibre entre la nécessité de collecter des preuves utiles et l'obligation de protéger les droits du suspect en optant pour l'instrument le moins intrusif parmi la gamme d'options ayant les mêmes effets. Ces deux exemples montrent que le rôle des enquêteurs judiciaires ne se limite pas aux aspects techniques d'une investigation, mais inclut la responsabilité de protéger les droits fondamentaux du suspect, évitant ainsi que les preuves collectées ne soient déclarées irrecevables.[2180]

Collecte et préservation des preuves

La participation à la collecte de preuves numériques exige des compétences complexes, car les techniques utilisées pour collecter des preuves stockées sur le disque dur d'un ordinateur personnel et intercepter le processus de transmission des données sont très différentes. Les enquêteurs sont souvent confrontés à des situations qui exigent une prise de décision rapide, surtout lorsqu'elles impliquent de grands délinquants. A titre d'exemple, citons le fait de savoir si un système informatique qui tourne doit être éteint ou non et comment cette procédure doit être exécutée. Afin d'éviter toute mise en danger de l'intégrité des preuves numériques pertinentes, l'une des instructions habituelles est de débrancher l'appareil, puisque cela empêche toute altération des fichiers.[2181] Cependant, une telle rupture de l'approvisionnement en électricité peut activer un cryptage[2182], empêchant ainsi l'accès aux données stockées.[2183] Les premiers

intervenants, chargés de commencer les démarches de collecte des preuves numériques, portent une lourde responsabilité dans le cadre du processus d'enquête global. En effet, toute décision malvenue peut avoir un impact de taille sur la possibilité de préserver les preuves pertinentes.[2184] S'ils prennent les mauvaises décisions en matière de préservation, d'importantes traces peuvent être perdues.

Les experts judiciaires doivent s'assurer que toutes les preuves pertinentes ont été identifiées.[2185] Cette tâche peut être difficile si les contrevenants cachent des fichiers sur un périphérique de stockage afin d'éviter que les forces de l'ordre n'analysent leur contenu. Les enquêtes judiciaires doivent pouvoir identifier des fichiers cachés et les rendre accessibles.[2186] Des processus de récupération similaires sont nécessaires si des informations numériques ont été effacées.[2187] Le simple fait de supprimer des fichiers en les plaçant dans la corbeille virtuelle ne les rend pas forcément inutilisables pour les forces de l'ordre, car ils peuvent être récupérés grâce à des outils logiciels d'analyse spéciaux.[2188] Toutefois, si les criminels utilisent certains outils pour s'assurer que les fichiers seront supprimés de façon sécurisée par écrasement des informations qu'ils contiennent, toute récupération est, en général, impossible.[2189] La collecte de preuves peut donc être confrontée à de vrais défis si les criminels essayent d'empêcher l'accès aux informations pertinentes en utilisant des technologies de cryptage. Celles-ci sont de plus en plus fréquentes.[2190] Etant donné qu'elles empêchent l'accès et l'examen, par les forces de l'ordre, d'informations cryptées, l'utilisation de ce type de technologies représente un défi de taille pour les autorités.[2191] Les experts judiciaires peuvent tenter de décrypter les fichiers encodés.[2192] S'ils n'y parviennent pas, ils peuvent aider les forces de l'ordre à développer des stratégies permettant d'accéder à ces fichiers, par exemple, par le biais d'un enregistreur de frappe (*keylogger*).[2193]

Participer à la collecte de preuves suppose l'évaluation et la mise en œuvre de nouveaux instruments. Parmi les nouvelles approches, citons le débat en cours sur les outils d'analyse à distance.[2194] Ceux-ci permettent aux enquêteurs de collecter des preuves à distance et en temps réel[2195] ou de surveiller, toujours à distance, l'activité[2196] d'un suspect sans que celui-ci ne soit conscient de la surveillance de son système. Là où de tels outils sont disponibles, ils peuvent jouer un rôle dans l'élaboration d'une stratégie de collecte des preuves numériques.

Communication avec les prestataires de services

Les fournisseurs d'accès à Internet (FAI) jouent un rôle important dans le cadre de nombreuses enquêtes cybercriminelles, puisque la plupart des internautes font appel à leurs services pour accéder à Internet ou héberger des sites. Le fait que, dans certains cas, les FAI disposent des capacités techniques nécessaires pour détecter et prévenir les délits et soutenir les forces de l'ordre dans leur enquête a suscité un débat intense sur leur rôle au sein des enquêtes cybercriminelles. Les obligations mentionnées vont de la mise en œuvre obligatoire de technologies préventives à un soutien volontaire à l'enquête.[2197] Les experts judiciaires peuvent également soutenir une investigation en préparant des requêtes qui seront ensuite soumises aux FAI[2198] et en aidant les enquêteurs à compiler les éléments[2199] qui seront par la suite nécessaires pour prouver la fiabilité des preuves collectées. Dans ce contexte, la coopération entre les agences répressives et les FAI exige le suivi de certaines procédures.[2200] Les lignes directrices du Conseil de l'Europe pour la coopération entre les organes de répression et les fournisseurs de services Internet[2201] regroupent une série de procédures essentielles couvrant plusieurs questions comme la fourniture d'explications et d'aide sur les techniques[2202] et priorités[2203] d'enquête. L'assistance d'experts judiciaires peut alors être utile pour améliorer l'efficacité des procédures.

Une coopération étroite avec les FAI est particulièrement pertinente lorsqu'il s'agit d'identifier un suspect. Les personnes suspectées d'avoir commis un crime informatique laissent des traces.[2204] L'analyse des données relative au trafic, qui prend, par exemple, la forme de l'examen des fichiers journaux conservés par les FAI, peut mener les enquêteurs à la connexion utilisée par le contrevenant pour accéder à Internet.[2205] Les criminels peuvent essayer d'entraver les investigations en utilisant des systèmes de communication anonymes.[2206] Mais même dans ces cas, les enquêtes restent possibles si enquêteurs et FAI coopèrent étroitement.[2207] Citons, en guise d'exemple, l'outil d'analyse CIPAV (*Computer and Internet Protocol Address Verifier*), utilisé aux Etats-Unis pour identifier un suspect qui a fait appel à des services de communication anonymes.[2208] Les analyses de messagerie sont un autre exemple de coopération entre les FAI et les enquêteurs. Les courriers électroniques sont devenus un moyen très populaire de

communication.[2209] Afin d'éviter d'être identifiés, les criminels utilisent parfois des adresses de courriel gratuites qu'ils ont pu créer en donnant de fausses informations personnelles. Mais l'analyse des informations d'en-tête[2210] et des fichiers journaux du fournisseur de messagerie permettra quand même, dans certains cas, l'identification du suspect.

La nécessité de coopérer et de communiquer avec les prestataires ne se limite pas aux FAI. Puisque certains délits, comme le hameçonnage[2211] ou la diffusion commerciale de matériel pédopornographique, sont associés à des transactions financières, l'une des stratégies d'identification des criminels consiste en l'obtention de données auprès des établissements financiers impliqués dans ces transactions.[2212] Ainsi, en Allemagne, une enquête a permis d'identifier des contrevenants qui téléchargeaient des fichiers pédopornographiques à partir d'un site commercial grâce à leur relevé de carte de crédit. Suite à une demande des enquêteurs, les sociétés émettrices des cartes de crédit ont analysé les dossiers de leurs clients pour identifier ceux qui avaient utilisé leur carte pour acheter de la pédopornographie sur un site Internet précis.[2213] De telles enquêtes sont rendues plus difficiles lorsque des moyens anonymes de paiement sont utilisés.[2214]

Analyse des TIC

Dans la plupart des enquêtes, la première étape consiste à prouver que le contrevenant pouvait commettre le crime. L'une des principales tâches des experts judiciaires est d'examiner le matériel informatique et les logiciels saisis.[2215] Cette vérification peut se faire sur place, lors de la perquisition chez le suspect[2216] ou après la saisie. Afin de permettre le bon déroulement de l'enquête, les premiers intervenants saisissent normalement tous les périphériques de stockage pertinents, chacun pouvant potentiellement contenir des millions de fichiers, ce qui représente souvent un défi logistique.[2217] Comme nous l'avons rappelé plus haut, les principes de la pertinence et de l'efficacité sont essentiels à la recevabilité des preuves numériques.[2218] Identifier et sélectionner le bon matériel est donc l'une des principales missions dans le cadre d'une enquête.[2219]

L'analyse des composants de matériel disponibles peut, par exemple, apporter la preuve que l'ordinateur du suspect était en mesure d'exécuter une attaque par déni de service[2220] ou est équipé d'une puce empêchant toute manipulation du système d'exploitation. L'analyse du matériel informatique peut également s'avérer nécessaire pour l'identification du suspect. Certains systèmes d'exploitation analysent la configuration matérielle de l'ordinateur pendant le processus d'installation, puis la transmettent à l'éditeur du logiciel. Si le profil matériel du suspect peut être identifié sur la base des informations fournies par l'entreprise de logiciels, une analyse du matériel peut être utile pour vérifier que l'ordinateur saisi est le bon. L'analyse du matériel informatique ne signifie pas nécessairement de se concentrer sur les composants physiques rattachés à un ordinateur. La plupart des systèmes d'exploitation conservent des journaux du matériel incorporé à l'ordinateur lors de diverses opérations.[2221] En s'appuyant sur les entrées des fichiers journaux comme Windows Registry, les enquêteurs judiciaires peuvent même identifier le matériel utilisé par le passé, mais absent pendant la perquisition et la saisie.

Outre l'analyse du matériel, l'analyse des logiciels est une mission régulière dans les enquêtes de cybercriminalité. Des logiciels informatiques sont nécessaires pour faire fonctionner un ordinateur. En plus des systèmes d'exploitation, d'autres outils logiciels peuvent être installés pour adapter le fonctionnement de l'ordinateur aux besoins de l'utilisateur. Les experts judiciaires peuvent analyser le fonctionnement des logiciels de façon à prouver qu'un suspect était en mesure de commettre un crime spécifique. Ainsi, ils peuvent enquêter pour voir si l'ordinateur d'un suspect contient un logiciel permettant le cryptage de données en images (stéganographie[2222]). Un inventaire des logiciels installés sur l'ordinateur du suspect peut également aider à développer les futures stratégies d'enquête. Si, par exemple, les enquêteurs trouvent des logiciels de cryptage ou des outils utilisés pour supprimer de façon sécurisée des fichiers, ils peuvent plus spécifiquement se mettre à la recherche de preuves cryptées ou supprimées.[2223] Les enquêteurs peuvent aussi déterminer les fonctions de virus informatiques ou d'autres formes de logiciels malveillants afin de reconstituer les processus d'exploitation des logiciels.[2224] Dans certains cas, lorsque des contenus illicites ont été retrouvés sur les ordinateurs de suspects, ceux-ci ont affirmé ne jamais avoir téléchargé ces fichiers, qui l'auraient été par un virus informatique. Dans de tels cas, les enquêtes judiciaires peuvent tenter de détecter la présence de logiciels malveillants installés sur l'ordinateur et déterminer leurs

fonctions. Des enquêtes similaires peuvent être menées si un ordinateur a pu être infecté et intégré à un réseau d'ordinateurs zombies.[2225] De plus, l'analyse des logiciels peut être une étape importante à l'heure de déterminer si un logiciel est produit dans le seul but de commettre des infractions ou peut être utilisé à des fins légitimes et illégales (double usage). Cette distinction peut être pertinente, dans la mesure où certains pays ne considèrent la production de dispositifs illégaux comme criminelle que lorsque ceux-ci sont uniquement ou essentiellement conçus pour commettre une infraction.[2226]

Les enquêtes relatives aux données ne se limitent pas aux fonctions des logiciels. Elles incluent aussi l'analyse de fichiers non exécutables comme des documents PDF ou des fichiers vidéo. Ces enquêtes vont de l'analyse du contenu de fichiers spécifiques à une recherche automatique[2227] sur la base de mots-clés ou d'images pour retrouver des fichiers texte ou des images connues sur l'ordinateur d'un suspect.[2228] L'analyse de fichiers couvre également l'examen de documents numériques qui ont peut-être été falsifiés[2229] ainsi que le traitement de métadonnées.[2230] Une telle analyse peut déterminer l'heure[2231] de la dernière ouverture ou modification[2232] d'un document. De plus, l'analyse des métadonnées peut servir à identifier l'auteur d'un fichier contenant un message menaçant ou encore le numéro de série de l'appareil photo utilisé pour produire une image pédopornographique. Les auteurs peuvent également être identifiés grâce à une analyse linguistique, méthode qui peut contribuer à déterminer si le suspect a déjà écrit des articles ou laissé des informations permettant son identification.[2233]

Suivi et notification

L'un des plus grands défis en matière de preuves numériques est lié à leur extrême fragilité et au fait qu'elles peuvent facilement être supprimées[2234] ou modifiées.[2235] Comme nous l'avons rappelé plus haut, l'une des conséquences de cette fragilité est la nécessité de préserver l'intégrité de ce type de preuves.[2236] L'établissement d'un dossier est donc obligatoire. La participation d'experts qualifiés[2237] à cette élaboration est l'une des manières de protéger l'intégrité des preuves.[2238] Mais les experts judiciaires jouent aussi un rôle lorsque la saisie de matériel informatique est impossible ou inadaptée. Parfois, certains pays autorisent les enquêteurs à copier des fichiers. Une attention toute particulière doit alors être portée lors du processus de copie de façon à protéger l'intégrité des fichiers copiés contre toute altération.[2239]

Présentation des éléments de preuve au tribunal

La dernière étape de l'enquête est normalement la présentation des éléments de preuve au tribunal. Habituellement, cette tâche incombe au procureur et aux avocats de la défense, mais les experts judiciaires peuvent jouer un rôle important dans le cadre de procédures pénales. En tant que témoins experts, ils peuvent aider les participants à l'audience à comprendre les processus utilisés pour générer, collecter et évaluer les preuves.[2240] Etant donné la complexité associée aux preuves numériques, la nécessité d'impliquer des experts judiciaires s'accroît, ce qui entraîne *de facto* une confiance placée par les juges, les jurés, le procureur et les avocats dans les déclarations d'experts.[2241]

Examens scientifiques et techniques

Même si l'informatique judiciaire traite essentiellement de matériel et de données informatiques, ses procédures ne sont pas toujours automatisées; l'informatique judiciaire reste, dans une large mesure, une activité manuelle.[2242] C'est particulièrement vrai pour le développement de stratégies et la recherche d'éventuelles preuves dans le cadre de perquisitions et de saisies. Le temps nécessaire à ce type d'opérations manuelles ainsi que la capacité des criminels à automatiser leurs attaques soulignent les défis auxquels sont confrontées les forces de l'ordre, en particulier dans les enquêtes impliquant un grand nombre de suspects et d'importants volumes de données.[2243] Ceci étant, certains processus, comme la recherche de mots-clés suspects ou la récupération de fichiers supprimés peuvent être automatisés grâce à des outils d'analyse judiciaire spéciaux.[2244]

6.5.3 Sauvegardes

Ces dernières années, les forces de l'ordre ont rappelé, dans le monde entier, le besoin urgent d'instruments d'enquête adéquats.[2245] À cet égard, il peut apparaître surprenant que les parties relatives aux instruments de procédure de la Convention du Conseil de l'Europe sur la cybercriminalité aient été

critiquées. [2246] Ces critiques se concentrent essentiellement sur le fait que la Convention sur la cybercriminalité contient plusieurs dispositions établissant des instruments d'enquête (articles 16 à 21), mais une seule sur les sauvegardes (article 15)[2247]. De plus, il convient de noter que, contrairement aux dispositions de droit pénal matériel de la Convention sur la cybercriminalité, les possibilités d'adaptation nationale de la mise en œuvre de ce texte sont rares.[2248] Les critiques se concentrent donc surtout sur des éléments quantitatifs. Il est vrai que la Convention sur la cybercriminalité suit une approche de réglementation centralisée des sauvegardes plutôt que de les rattacher individuellement à chaque instrument. Toutefois, cela n'entraîne pas nécessairement une protection plus faible des droits du suspect.

La Convention du Conseil de l'Europe sur la cybercriminalité a été conçue dès le départ comme un cadre international et un instrument de lutte contre la cybercriminalité qui ne se limiterait pas uniquement aux pays membres de cette instance.[2249] Lors des négociations sur les instruments de procédure nécessaires, les auteurs de ce texte, parmi lesquels des représentants de pays non européens comme les États-Unis et le Japon, se sont aperçus que les approches nationales existantes en matière de sauvegardes et, plus particulièrement, la façon dont celles-ci protégeaient le suspect dans les divers systèmes de droit pénal étaient si différentes qu'il ne serait pas possible de proposer une solution détaillée convenant à tous les États membres.[2250] Les auteurs de la Convention sur la cybercriminalité ont donc décidé de ne pas y inclure de dispositions spécifiques, mais de demander aux États membres de veiller à ce que les normes fondamentales nationales et internationales en matière de sauvegarde soient respectées.[2251]

Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

L'article 15 s'appuie sur le principe que les États signataires doivent respecter les conditions et sauvegardes existant déjà dans leur législation nationale. Si la loi prévoit des normes communes s'appliquant à tous les instruments d'enquête, ces principes doivent également s'appliquer aux instruments liés à Internet.[2252] Si le droit national ne repose pas sur une réglementation centralisée des sauvegardes et conditions, il sera nécessaire d'analyser les sauvegardes et conditions appliquées aux instruments traditionnels comparables aux instruments liés à Internet.

Mais la Convention sur la cybercriminalité ne fait pas uniquement référence aux sauvegardes existantes dans la législation nationale. Une telle approche aurait l'inconvénient d'être associée à des exigences d'application si diverses qu'elles annuleraient tous les aspects positifs de l'harmonisation. Afin de garantir que les Etats signataires, qui peuvent ne pas avoir les mêmes traditions juridiques et sauvegardes en place, appliquent certains normes[2253], la Convention du Conseil de l'Europe sur la cybercriminalité définit les normes minimales en faisant référence à des cadres fondamentaux, comme la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe de 1950, le Pacte international relatif aux droits civils et politiques des Nations Unies de 1966 ainsi que d'autres instruments internationaux applicables concernant les droits de l'homme.

Puisque la Convention sur la cybercriminalité peut également être signée et ratifiée par des pays non membres du Conseil de l'Europe[2254], il est important de souligner que le Pacte international relatif aux droits civils et politiques des Nations Unies ainsi que la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe seront tous deux pris en compte lors de l'évaluation des systèmes de sauvegardes existants dans les pays signataires de la Convention sur la cybercriminalité non membres du Conseil de l'Europe.

En ce qui concerne les enquêtes cybercriminelles, l'une des dispositions les plus pertinentes de l'article 15 de la Convention du Conseil de l'Europe sur la cybercriminalité est la référence faite à l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme.

Article 8
1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

La Cour européenne des droits de l'homme s'efforce de définir des normes plus précises qui régiraient les enquêtes électroniques et plus particulièrement la surveillance. Aujourd'hui, la jurisprudence est devenue l'une des sources les plus importantes de normes internationales applicables aux enquêtes en matière de communication.[2255] La jurisprudence prend plus particulièrement en compte la gravité de l'interférence avec l'enquête[2256], sa finalité[2257] et sa proportionnalité.[2258] Les principes fondamentaux pouvant être déduits de la jurisprudence sont: la nécessité d'une base juridique suffisante pour les outils d'investigation[2259]; l'exigence d'une base juridique claire en relation avec le sujet de l'enquête[2260]; la prévisibilité des compétences des forces de l'ordre[2261]; la limitation des mesures de surveillance et de communication aux seules infractions graves.[2262]

En outre, l'article 15 de la Convention du Conseil de l'Europe sur la cybercriminalité prend en compte le principe de proportionnalité.[2263] Ses dispositions sont particulièrement pertinentes pour les États signataires non membres du Conseil de l'Europe. Dans les cas où le système national existant de sauvegardes ne protège pas adéquatement les suspects, les États membres sont tenus de développer les sauvegardes nécessaires lors du processus de ratification et de mise en œuvre de la Convention.

Enfin, l'article 15, paragraphe 2, de la Convention du Conseil de l'Europe sur la cybercriminalité fait explicitement référence aux sauvegardes les plus pertinentes[2264], parmi lesquelles la supervision judiciaire et des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

Contrairement aux principes fondamentaux décrits ci-dessus, les sauvegardes mentionnées ici n'ont pas nécessairement besoin d'être appliquées en lien avec un instrument précis, mais uniquement dans les cas appropriés en fonction de la nature de la procédure concernée. Cette décision est laissée au législateur national.[2265]

L'un des aspects importants lié au système de sauvegardes prévu par la Convention du Conseil de l'Europe sur la cybercriminalité est la possibilité, pour les forces de l'ordre, d'utiliser des instruments de façon souple d'un côté, et la garantie de sauvegardes efficaces de l'autre, qui dépend de l'application d'un système progressif de sauvegardes. La Convention sur la cybercriminalité n'empêche pas explicitement les parties d'appliquer les mêmes sauvegardes (par ex. l'exigence d'une injonction du tribunal) à tous les instruments, mais une telle approche aurait un impact sur la souplesse des forces de l'ordre. La capacité de garantir une protection adéquate des droits du suspect dans le cadre d'un système progressif de sauvegardes dépend largement de l'équilibre à atteindre entre l'impact potentiel d'un outil d'enquête et les sauvegardes en question. Pour y parvenir, il est nécessaire de faire la distinction entre les instruments en fonction de leur intensité. La Convention du Conseil de l'Europe sur la cybercriminalité contient plusieurs exemples de ce type de distinction qui permet aux parties de poursuivre le développement d'un système graduel de

sauvegardes. Parmi celles-ci, la distinction entre l'interception des données relatives au contenu (article 21)[2266] et la collecte de données relatives au trafic (article 20).[2267] Contrairement à la collecte des données relatives au trafic, l'interception des données relatives au contenu se limite aux délits graves.[2268] Il existe une différence entre l'injonction de conservation rapide des données stockées sur ordinateur (article 16)[2269] et la présentation des données informatiques conservées sur la base d'une injonction de production (article 18).[2270] L'article 16 permet uniquement aux forces de l'ordre d'ordonner la conservation des données, mais non leur divulgation.[2271] Enfin, l'article 18[2272] fait la distinction entre l'obligation de soumettre les « données relatives aux abonnés »[2273] et les « données informatiques ».[2274]

Si l'intensité d'un outil d'enquête et son impact potentiel sur un suspect sont correctement évalués et des sauvegardes prévues conformément aux conclusions de l'analyse, le système progressif de sauvegardes n'entraîne pas l'application d'un système déséquilibré d'instruments de procédure.

6.5.4 Conservation rapide de données stockées dans un système informatique (Procédure de gel rapide dite « Quick Freeze »)

L'identification de l'auteur du délit informatique exige souvent l'analyse des données relatives au trafic.[2275] L'adresse IP, en particulier, peut aider les forces de l'ordre à retrouver la trace du criminel. A partir du moment où elles ont accès aux données pertinentes relatives au trafic, il leur est parfois même possible d'identifier un contrevenant utilisant des terminaux publics d'accès à Internet n'exigeant aucune identification.[2276]

L'une des plus grandes difficultés auxquelles sont confrontés les enquêteurs est liée au fait que les données relatives au trafic les plus pertinentes sont souvent automatiquement effacées assez rapidement. Cette suppression automatique s'explique par le fait qu'à la fin d'un processus (par ex. l'envoi d'un courriel, l'accès à Internet ou le téléchargement d'un film), les données relatives au trafic générées pendant celui-ci et permettant son exécution ne sont plus nécessaires. D'un point de vue économique, la plupart des fournisseurs d'accès à Internet préfèrent effacer ces informations au plus vite, puisque le stockage de données pendant de longues périodes exige des capacités encore plus importantes (et chères).[2277]

Toutefois, la dimension économique n'est pas la seule raison derrière la nécessité pour les forces de l'ordre de conduire leur enquête rapidement. Certains pays disposent d'une loi interdisant la conservation de certaines données relatives au trafic après la fin d'un processus. L'article 6 de la directive de l'Union européenne sur la protection de la vie privée dans le secteur des communications électroniques en est un exemple.[2278]

Article 6 – Données relatives au trafic
1. Les données relatives au trafic concernant les abonnés et les utilisateurs, traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.
2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

Le temps est donc une composante essentielle des enquêtes Internet. D'une manière générale, puisqu'il est probable qu'un certain temps s'écoule entre le crime, sa découverte et la notification aux forces de l'ordre, il est important de mettre en œuvre des mécanismes évitant que les données pertinentes ne soient effacées pendant le processus parfois long de l'enquête. C'est pourquoi deux approches sont aujourd'hui envisagées[2279]: la rétention des données et la préservation des données (« procédure de congélation rapide » (*quick freeze*).

Une obligation de rétention des données contraint le fournisseur d'accès à Internet à sauvegarder les données relatives au trafic pendant un certain temps.[2280] Les approches législatives les plus récentes

prévoient une conservation jusqu'à 24 mois de ces informations.[2281] Ce délai permet aux forces de l'ordre d'obtenir l'accès aux données nécessaires à l'identification d'un criminel, y compris après que le crime ait été commis.[2282] Une telle obligation de rétention des données a récemment été adoptée par le Parlement européen [2283] et est en cours d'examen aux Etats-Unis. [2284] Vous trouverez ci-dessous davantage d'informations sur les principes de rétention des données.

Convention sur la cybercriminalité

La conservation des données est une autre approche qui vise à garantir que les enquêtes cybercriminelles n'échouent pas simplement parce que les données relatives au trafic ont été effacées pendant les longues procédures d'investigation.[2285] En s'appuyant sur la législation en la matière, les forces de l'ordre peuvent ordonner à un prestataire de services de ne pas supprimer certaines données. La conservation rapide des données informatiques est un outil qui devrait permettre aux forces de l'ordre de réagir immédiatement et d'éviter le risque de suppression de celles-ci lié à la longueur des procédures. [2286] Les auteurs de la Convention du Conseil de l'Europe sur la cybercriminalité ont décidé de parler de « conservation des données » plutôt que de « rétention des données ».[2287] Une disposition en la matière se trouve à l'article 16 de la Convention.

> ***Article 16*** *– Conservation rapide de données informatiques stockées*
> *1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.*
> *2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.*
> *3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.*
> *4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.*

Du point de vue d'un fournisseur d'accès à Internet, la conservation des données est un instrument moins contraignant que la rétention des données.[2288] Les FAI n'ont pas besoin de stocker toutes les données de tous les internautes, mais doivent veiller à ce que certaines données spécifiques ne soient pas effacées à partir du moment où ils reçoivent une injonction émanant d'une autorité compétente. La conservation des données présente plusieurs avantages dans la mesure où elle permet leur préservation par le fournisseur, mais aussi leur protection. Ceci étant, il n'est pas nécessaire de conserver les données de millions d'utilisateurs, mais seulement celles liées à des suspects potentiels dans le cadre d'enquêtes pénales. Quoi qu'il en soit, il est important de rappeler que la rétention des données offre des avantages lorsque celles-ci sont effacées dès la perpétration du délit. Dans ces cas, l'injonction de conservation des données n'empêcherait pas, contrairement à l'obligation de rétention des données, que les données pertinentes soient effacées.

Conformément à l'article 16, l'injonction n'oblige le fournisseur qu'à sauvegarder les données qu'il a traitées et qui n'avaient pas été effacées au moment où il a reçu l'injonction.[2289] Cette obligation ne se limite pas aux données relatives au trafic, puisque celles-ci ne sont citées qu'à titre d'exemple. L'article 16 ne force pas non plus le fournisseur à commencer à collecter des informations qu'il ne stockerait pas normalement.[2290] De plus, l'article 16 ne contraint pas le fournisseur à transférer les données pertinentes aux autorités. Ses dispositions n'autorisent les forces de l'ordre qu'à prévenir la suppression de données pertinentes, mais n'engagent pas les fournisseurs à les transmettre. L'obligation de transfert est régie par les articles 17 et 18 de la Convention du Conseil de l'Europe sur la cybercriminalité. Le fait d'avoir séparé

l'obligation de conserver les données de celle de les divulguer offre l'avantage d'imposer différentes conditions à leur application.[2291] S'il est important de réagir immédiatement, il serait, par exemple, utile de renoncer à l'exigence d'une injonction du tribunal pour permettre au Parquet ou à la police d'ordonner la conservation.[2292] Cela permettrait aux autorités compétentes de réagir plus vite. La protection des droits du suspect peut alors être garantie en exigeant une injonction du tribunal pour la divulgation de ces données.[2293]

La divulgation des données conservées est l'un des éléments réglementés à l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité:

> ***Article 18*** *– Injonction de produire*
> *1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:*
> *a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et*
> *b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.*
> *2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.*
> *3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:*
> *a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;*
> *b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;*
> *c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.*

Sur la base de l'article 18, paragraphe 1.a de la Convention du Conseil de l'Europe sur la cybercriminalité, les fournisseurs ayant stocké des données peuvent être contraints à les divulguer.

L'article 18 de la Convention sur la cybercriminalité ne s'applique pas uniquement une fois une injonction de conservation émise dans les conditions de l'article 16.[2294] Ces dispositions sont un instrument général au service des forces de l'ordre. Si le destinataire de l'injonction de production transmet volontairement les données demandées, les forces de l'ordre ne voient pas leur action limitée à la saisie du matériel informatique, mais peuvent opter pour une injonction de production, moins contraignante. Par rapport à la saisie du matériel informatique, l'injonction de production des informations pertinentes est, en général, moins contraignante. Son application est donc particulièrement pertinente dans les cas où les enquêtes judiciaires n'exigent pas d'avoir accès au matériel informatique.

Outre l'obligation de produire les données informatiques, l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité autorise les forces de l'ordre à ordonner la soumission des données relatives aux abonnés. Cet instrument d'enquête est particulièrement important dans les investigations basées sur l'IP. Si les forces de l'ordre sont capables d'identifier une adresse IP utilisée par le criminel pendant son délit, elles auront besoin d'identifier la personne [2295] ayant utilisé cette adresse IP au moment de l'infraction. L'article 18, paragraphe 1.b, de la Convention sur la cybercriminalité oblige les fournisseurs à soumettre les données relatives aux abonnés détaillées au paragraphe 3 du même article.[2296]

Dans les cas où les forces de l'ordre remontent la piste jusqu'au contrevenant et ont besoin d'un accès immédiat pour identifier le chemin suivi pendant la transmission des communications, l'article 17 leur permet d'ordonner une divulgation partielle rapide des données relatives au trafic.

Article 17 *– Conservation et divulgation rapides de données relatives au trafic*
1. Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

a. pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b. pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Comme nous l'avons rappelé plus haut, la Convention sur la cybercriminalité établit une distinction stricte entre l'obligation de conserver les données à la demande et celle de les divulguer aux autorités compétentes.[2297] L'article 17 prévoit une hiérarchie claire, puisqu'il associe l'obligation de garantir la conservation des données relatives au trafic, dans les cas où plusieurs prestataires de services sont impliqués, à l'obligation de divulguer les informations nécessaires à l'identification de la voie de transmission. Sans une telle divulgation partielle, les forces de l'ordre ne seraient pas en mesure, dans certains cas, de retrouver la trace du criminel si plus d'un fournisseur est impliqué.[2298] Etant donné l'articulation de ces deux obligations, qui affectent différemment les droits du suspect, il convient d'analyser l'accent mis sur les sauvegardes par cet instrument.

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique

Des approches similaires sont proposées par la loi type du Commonwealth de 2002.[2299]

La disposition

Production de données
15. *Lorsqu'un magistrat estime, sur la base d'une requête faite par un officier de police, que des données informatiques spécifiées, ou une impression ou d'autres informations, font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou de poursuites pénales, le magistrat peut ordonner:*

(a) qu'une personne sur le territoire de [État prenant les dispositions], qui contrôle un système informatique, produise des données informatiques spécifiées ou une impression ou d'autres sorties intelligibles à partir de ces données; et

(b) qu'un prestataire de services Internet de [État prenant les dispositions] produise des informations sur des personnes qui sont abonnées ou qui utilisent autrement le service; et

(c)[2300] *qu'une personne sur le territoire de [État prenant les dispositions] qui a accès un système informatique spécifié compile des données informatiques spécifiées à partir du système et les remette à une personne spécifiée.*

Divulgation des données relatives au trafic stockées
16.[2301] *Si un officier de police estime que les données stockées dans un système informatique sont nécessaires aux fins d'une enquête criminelle, il peut, par un avis écrit remis à une personne qui contrôle le système informatique, demander à cette personne de divulguer des données suffisantes relatives au trafic à propos d'une communication spécifiée afin d'identifier:*

(a) les prestataires de services; et

(b) l'itinéraire par lequel la communication a été transmise.

Conservation des données
17. *(1) Si un officier de police estime que:*

(a) les données stockées dans un système informatique sont nécessaires aux fins d'une enquête criminelle; et

(b) qu'il existe un risque que ces données puissent être détruites ou rendues inaccessibles;

ledit officier de police peut, par avis écrit remis à une personne qui contrôle le système informatique, demander à cette personne de veiller à ce que les données spécifiées dans l'avis soient conservées pendant une période d'une durée maximale de 7 jours comme précisé dans l'avis.
(2) Cette période peut être prolongée au-delà de 7 jours si, en cas de requête ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.

6.5.5 Rétention des données

L'obligation de rétention des données force le fournisseur de services Internet à sauvegarder les données relatives au trafic pendant un certain temps.[2302] La mise en œuvre de cette obligation est l'une des approches applicables pour éviter les difficultés dépeintes ci-dessus dans l'obtention de l'accès aux données relatives au trafic avant leur suppression. La directive européenne sur la conservation des données[2303] était un exemple de ce type d'approche ; elle a été déclarée invalide en 2014.[2304]

Article 3 – Obligation de conservation de données
1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour que les données visées à l'article 5 de la présente directive soient conservées, conformément aux dispositions de cette dernière, dans la mesure où elles sont générées ou traitées dans le cadre de la fourniture des services de communication concernés par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans leur ressort.
2. L'obligation de conserver les données visées au paragraphe 1 inclut la conservation des données visées à l'article 5 relatives aux appels téléphoniques infructueux, lorsque ces données sont générées ou traitées, et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'Internet), dans le cadre de la fourniture des services de communication concernés, par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'État membre concerné. La présente directive n'impose pas la conservation des données relatives aux appels non connectés.
Article 4 – Accès aux données
Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicable en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme.
Article 5 – Catégories de données à conserver
1. Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes:
a) les données nécessaires pour retrouver et identifier la source d'une communication:
1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile:
i) le numéro de téléphone de l'appelant;
ii) les nom et adresse de l'abonné ou de l'utilisateur inscrit;
2) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet:
i) le(s) numéro(s) d'identifiant attribué(s);
ii) le numéro d'identifiant et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public;
iii) les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication;
b) les données nécessaires pour identifier la destination d'une communication:
1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile:

i) le(s) numéro(s) composé(s) [le(s) numéro(s) de téléphone appelé(s)] et, dans les cas faisant intervenir des services complémentaires tels que le renvoi ou le transfert d'appels, le(s) numéro(s) vers le(s)quel(s) l'appel est réacheminé;

ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s);

2) en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet:

i) le numéro d'identifiant ou le numéro de téléphone du (des) destinataire(s) prévu(s) d'un appel téléphonique par l'internet;

ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) et le numéro d'identifiant du destinataire prévu de la communication;

c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication:

1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, la date et l'heure de début et de fin de la communication;

2) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet:

i) la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet dans un fuseau horaire déterminé, ainsi que l'adresse IP (protocole internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit;

ii) la date et l'heure de l'ouverture et de la fermeture de la session du service de courrier électronique par l'internet ou de téléphonie par l'internet dans un fuseau horaire déterminé;

d) les données nécessaires pour déterminer le type de communication:

1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, le service téléphonique utilisé;

2) en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet, le service internet utilisé;

e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel:

1) en ce qui concerne la téléphonie fixe en réseau, le numéro de téléphone de l'appelant et le numéro appelé;

2) en ce qui concerne la téléphonie mobile:

i) le numéro de téléphone de l'appelant et le numéro appelé;

ii) l'identité internationale d'abonné mobile (IMSI) de l'appelant;

iii) l'identité internationale d'équipement mobile (IMEI) de l'appelant;

iv) l'IMSI de l'appelé;

v) l'IMEI de l'appelé;

vi) dans le cas des services anonymes à prépaiement, la date et l'heure de la première activation du service ainsi que l'identité de localisation (identifiant cellulaire) d'où le service a été activé;

3) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet:

i) le numéro de téléphone de l'appelant pour l'accès commuté;

ii) la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication;

f) les données nécessaires pour localiser le matériel de communication mobile:

1) l'identité de localisation (identifiant cellulaire) au début de la communication;

2) les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées.

2. Aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive.

Article 6 – Durées de conservation

Les États membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication.

Article 7 – Protection et sécurité des données
Sans préjudice des dispositions adoptées en application des directives 95/46/CE et 2002/58/CE, chaque État membre veille à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications respectent, au minimum, les principes suivants en matière de sécurité des données, pour ce qui concerne les données conservées conformément à la présente directive:

a) les données conservées doivent être de la même qualité et soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

b) les données font l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

c) les données font l'objet de mesures techniques et organisationnelles appropriées afin de garantir que l'accès aux données n'est effectué que par un personnel spécifiquement autorisé;

et

d) les données sont détruites lorsque leur durée de conservation prend fin, à l'exception des données auxquelles on a pu accéder et qui ont été préservées.

Article 8 – Conditions à observer pour le stockage des données conservées
Les États membres veillent à ce que les données visées à l'article 5 soient conservées conformément à la présente directive de manière à ce que les données conservées et toute autre information nécessaire concernant ces données puissent, à leur demande, être transmises sans délai aux autorités compétentes.

Le fait que des informations essentielles sur toutes les communications en ligne sont couvertes par la directive a suscité des critiques virulentes de la part des organisations de défense des droits de l'homme.[2305] Celles-ci pourraient déboucher sur une révision de la directive et des modalités de son application par les cours constitutionnelles.[2306] De plus, dans ses conclusions sur l'affaire Productores de Música de España (Promusicae) contre Telefónica de España,[2307] Juliane Kokott, avocate générale et conseillère de la Cour de justice européenne, a souligné qu'il était permis de se demander si l'obligation de rétention des données peut être appliquée sans entraîner une violation des droits fondamentaux.[2308] Les difficultés liées à la mise en œuvre de ces règles avaient déjà été signalées par le G8 en 2001.[2309]

Cependant, les critiques émises ne se limitent pas à cette question. Le fait que ces obligations peuvent être contournées est une autre raison expliquant la relative inefficacité de la rétention des données dans la lutte contre la cybercriminalité. Parmi les façons les plus simples de contourner l'obligation de rétention des données figure l'utilisation de plusieurs terminaux publics d'accès à Internet ou de services prépayés de transmission de données par téléphone mobile qui n'exigent aucun enregistrement.[2310] Citons également l'utilisation de services de communication anonymes qui sont (au moins partiellement) disponibles dans des pays où l'obligation de rétention des données n'est pas appliquée.[2311]

Si les contrevenants utilisent différents terminaux publics ou des services prépayés de transmission de données par téléphone mobile et qu'ils ne sont pas obligés d'enregistrer les données stockées par les fournisseurs, l'obligation de rétention des données ne mènera les forces de l'ordre qu'à ces derniers, et non aux contrevenants.[2312]

Les criminels peuvent en outre contourner l'obligation de rétention des données en utilisant des serveurs anonymes de communication.[2313] Dans ce cas, les forces de l'ordre pourraient éventuellement le prouver, mais n'ayant pas accès aux données relatives au trafic dans le pays où le serveur anonyme est situé, elles ne pourraient pas prouver la participation des criminels à la perpétration du délit pénal.[2314]

Etant donné la facilité de contournement de cette disposition, la mise en œuvre de la législation sur la rétention des données dans l'Union européenne est associée à la peur de voir le processus exiger des mesures annexes pour garantir l'efficacité de l'instrument. Celles-ci pourraient, par exemple, prévoir une obligation d'enregistrement avant l'utilisation de services en ligne [2315] ou interdire l'utilisation des technologies de communication anonymes.[2316]

En 2014, la Cour de justice des Communautés européennes a finalement constaté la nullité de la directive.[2317] D'après les conclusions de la Cour, la directive comporte une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux liés au respect de la vie privée et à la protection

des données à caractère personnel, sans que cette ingérence soit limitée au strict nécessaire. Les Etats membres ne sont par conséquent plus liés par cette directive, mais les lois nationales mises en œuvre conformément à cette dernière ne sont pas automatiquement invalidées. On ne sait pas pour l'heure si l'Union européenne présentera et adoptera une nouvelle directive.

6.5.6 Perquisition et saisie

Même si de nouveaux outils d'enquête, tels la collecte en temps réel des données relatives au contenu et l'utilisation de logiciels d'enquête judiciaire à distance pour identifier les contrevenants, sont aujourd'hui débattus et même utilisés dans certains pays, les perquisitions et saisies restent deux des principaux instruments d'enquête.[2318] Dès l'identification du contrevenant et la saisie, par les forces de l'ordre, de son équipement informatique, les experts informaticiens judiciaires peuvent analyser son contenu afin de collecter les preuves nécessaires aux poursuites. [2319]

La possibilité de remplacer ou de revoir la procédure de perquisition et de saisie fait actuellement l'objet de discussions dans certains pays européens et aux Etats-Unis.[2320] L'une des façons d'éviter à avoir à entrer dans le domicile du suspect pour perquisitionner et saisir son matériel informatique est de procéder à une perquisition en ligne. Cet instrument, que nous décrirons en détail plus loin, est associé à une procédure où les forces de l'ordre ont accès à l'ordinateur du suspect par le biais d'Internet afin d'y effectuer des recherches secrètes.[2321] Même si les forces de l'ordre pourraient clairement bénéficier du fait que le suspect ne se doute pas qu'une enquête est en cours, l'accès physique à son matériel informatique permet l'application de techniques d'investigation plus efficaces.[2322] Cette réalité souligne le rôle important des procédures de perquisition et de saisie dans le cadre des enquêtes sur Internet.

Convention du Conseil de l'Europe sur la cybercriminalité

Dans la plupart des pays, le droit de la procédure pénale contient des dispositions permettant aux forces de l'ordre de procéder à des perquisitions et de saisir des objets.[2323] La raison pour laquelle les auteurs de la Convention du Conseil de l'Europe sur la cybercriminalité y ont tout de même inclus une disposition en la matière est que souvent, les législations nationales ne prévoient pas de procédure de perquisition ou de saisie de données.[2324] Ainsi, certains pays limitent l'application des procédures de perquisition à la saisie d'objets physiques.[2325] En s'appuyant sur ce type de dispositions, les enquêteurs peuvent saisir tout un serveur, mais ne peuvent se limiter aux données pertinentes qu'il contient en les copiant à partir de celui-ci. Cela peut entraîner des difficultés lorsque les informations pertinentes sont stockées sur un serveur avec les données de centaines d'autres utilisateurs qui ne seraient alors plus disponibles après la saisie du serveur par les forces de l'ordre. Citons également, comme autre exemple de cas où les perquisitions et saisies traditionnelles d'objets physiques ne suffisent pas, les situations où les forces de l'ordre ignorent l'emplacement réel du serveur, mais peuvent y accéder par Internet.[2326] Comme pour d'autres instruments de procédure prévus par la Convention sur la cybercriminalité, l'article 19 ne précise pas les conditions et exigences que les enquêteurs doivent respecter pour mener de telles investigations. La disposition elle-même ne spécifie pas qu'une injonction d'un tribunal est nécessaire, ni ne définit les circonstances dans lesquelles une dérogation à l'obligation d'injonction du tribunal est envisageable. Etant donné que les procédures de perquisition et de saisie[2327] empiètent sur les libertés civiles et les droits des suspects, la plupart des pays préfèrent limiter l'applicabilité de cet instrument.[2328]

L'article 19, paragraphe 1, de la Convention du Conseil de l'Europe sur la cybercriminalité vise à établir un instrument qui permette d'accéder aux systèmes informatiques de façon aussi efficace que les procédures traditionnelles de perquisition.[2329]

> ***Article 19*** *– Perquisition et saisie de données informatiques stockées*
> *1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:*
> *a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et*
> *b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.*

[…]

Même si la procédure de perquisition et de saisie est un instrument fréquemment utilisé par les enquêteurs, plusieurs défis se posent à l'heure de l'appliquer dans le cadre d'enquêtes cybercriminelles.[2330] L'une des principales difficultés rencontrées est que les ordres de perquisition sont souvent limités à certains endroits (par ex. le domicile du suspect)[2331]. Lorsqu'il s'agit de rechercher des données informatiques, il peut apparaître, au cours de l'enquête, que le suspect ne les a pas stockées sur des disques durs locaux, mais sur un serveur externe auquel il a accédé par Internet.[2332] L'utilisation de serveurs en ligne pour stocker et traiter des données est une démarche de plus en plus appréciée par les internautes (« informatique en nuage »). L'un des avantages du stockage d'informations sur un serveur en ligne est que celles-ci sont accessibles de n'importe quel endroit raccordé à Internet. Afin d'en garantir le déroulement efficace, il est important de maintenir une certaine souplesse dans le cadre des enquêtes. Si les enquêteurs découvrent que des informations pertinentes sont stockées sur un autre ordinateur, ils doivent pouvoir étendre leurs recherches à ce dernier.[2333] La Convention du Conseil de l'Europe sur la cybercriminalité régit cette question à l'article 19, paragraphe 2.

Article 19 – Perquisition et saisie de données informatiques stockées
[…]
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.
[…]

La saisie des données informatiques représente un autre défi. Si les enquêteurs arrivent à la conclusion que la saisie du matériel informatique utilisé pour stocker les données n'est pas nécessaire ou ne serait pas adapté, ils peuvent quand même avoir besoin d'autres instruments leur permettant de poursuivre la procédure de perquisition et de saisie pour les données stockées sur ordinateur.[2334] Les instruments nécessaires ne se limitent pas à l'action de copier les données pertinentes.[2335] Il existe, en outre, plusieurs mesures annexes leur permettant d'être aussi efficaces, comme la saisie de l'ordinateur même. L'essentiel est de préserver l'intégrité des données copiées.[2336] Si les enquêteurs ne sont pas autorisés à prendre les mesures nécessaires pour garantir l'intégrité des données copiées, celles-ci peuvent ne pas être acceptées comme preuves dans le cadre de poursuites pénales.[2337] Une fois que les enquêteurs ont copié les données et fait le nécessaire pour en préserver l'intégrité, ils devront décider que faire des données originales. Etant donné qu'ils ne s'empareront pas du matériel lors de la saisie, les informations resteront en général là où elles se trouvent. Les enquêteurs ne pourront pas laisser de telles données sur un serveur, en particulier dans le cadre d'enquêtes sur des contenus illégaux[2338] (par ex. pédopornographiques). C'est pourquoi ils ont besoin d'un instrument leur permettant d'enlever des données ou au moins de garantir qu'elles ne seront plus accessibles.[2339] La Convention du Conseil de l'Europe sur la cybercriminalité aborde ces questions à l'article 19, paragraphe 3.

Article 19 – Perquisition et saisie de données informatiques stockées
[…]
***3.** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:*
a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;
b. réaliser et conserver une copie de ces données informatiques;
c. préserver l'intégrité des données informatiques stockées pertinentes;
d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.
[…]

Les ordres de perquisition portant sur des données informatiques posent un autre défi: il est parfois difficile pour les forces de l'ordre de localiser ces données. Souvent, elles sont stockées dans des systèmes informatiques situés hors du territoire national. Même lorsque leur emplacement précis est connu, le volume de données stockées empêche souvent les enquêtes rapides.[2340] Dans ce cas, ces investigations sont associées à des difficultés particulières, dans la mesure où leur dimension internationale exige une coopération au niveau mondial.[2341] Même lorsque les enquêtes concernent des systèmes informatiques situés sur le territoire national et que les enquêteurs ont identifié l'hébergeur exploitant les serveurs où le criminel a stocké les données pertinentes, ils peuvent avoir des difficultés à identifier la localisation exacte des données. Il est très probable que même les hébergeurs de petite et moyenne taille aient des centaines de serveurs et des milliers de disques durs. Très souvent, les enquêteurs ne peuvent pas identifier la localisation exacte sans l'aide de l'administrateur du système, responsable de l'infrastructure des serveurs.[2342] Mais même s'ils parviennent à identifier un disque dur précis, des mesures de protection peuvent les empêcher de rechercher les données pertinentes. Les auteurs de la Convention sur la cybercriminalité ont décidé de traiter cette question en prévoyant une mesure coercitive destinée à faciliter la perquisition et la saisie de données informatiques. L'article 19, paragraphe 4, permet aux enquêteurs d'obliger un administrateur de système à assister les forces de l'ordre. Même si l'obligation de respecter les ordres des enquêteurs se limite aux informations nécessaires et au soutien à l'affaire, cet instrument modifie la nature des procédures de perquisition et de saisie. Dans de nombreux pays, les ordres de perquisition et de saisie ne peuvent qu'obliger les personnes concernées par l'enquête à tolérer ses procédures, mais elles n'ont pas besoin de soutenir activement les investigations. Pour la personne disposant de connaissances particulières dont ont besoin les enquêteurs, la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité changera la situation de deux manières. D'abord, ces personnes devront fournir les informations nécessaires aux enquêteurs. Le second changement concerne cette obligation. L'obligation d'apporter un soutien (raisonnable) aux enquêteurs libérera ces personnes disposant de connaissances particulières de leurs obligations contractuelles ou des ordres émanant de leur hiérarchie.[2343] La Convention sur la cybercriminalité ne définit pas l'adjectif « raisonnable », mais son rapport explicatif rappelle que ce terme *« peut couvrir la divulgation d'un mot de passe ou d'une autre mesure de sécurité aux autorités chargées de l'enquête »*, bien qu'il ne couvre en général pas *« la divulgation du mot de passe ou d'une autre mesure de sécurité »* lorsque cela *« menacerait de façon déraisonnable la vie privée d'autres utilisateurs ou le caractère privé d'autres données dont la perquisition n'a pas été autorisée »*.[2344]

Article 19 – Perquisition et saisie de données informatiques stockées
[…]
4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.
[…]

Loi type du Commonwealth relative à la criminalité informatique et liée à l'informatique

La loi type du Commonwealth de 2002 adopte une approche similaire.[2345]

Définitions pour la présente partie
11. *Dans la présente partie :*
[…]
« saisir » inclut:
(a) faire et conserver une copie de données informatiques, notamment en utilisant du matériel sur place; et
(b) rendre inaccessible ou retirer des données informatiques dans le système informatique consulté; et
(c) faire une impression de la sortie des données informatiques.
[…]

Mandats de perquisition et de saisie
12[2346] *(1) Lorsqu'un magistrat estime, sur la base de [informations obtenues sous serment] [affidavit]que l'on peut raisonnablement [soupçonner] [croire] qu'il puisse se trouver quelque part un objet ou des données informatiques:*

(a) qui peuvent constituer une preuve matérielle d'une infraction; ou

(b) qui ont pu être obtenues par une personne à la suite d'une infraction;

le magistrat [peut] [doit] délivrer un mandat autorisant un officier [des autorités de police], avec l'assistance qui pourrait s'avérer nécessaire, à pénétrer dans les lieux pour y faire une perquisition et une saisie de l'objet ou des données informatiques.
[…]

Assistance aux forces de police
13 [2347] *(1) Une personne qui est en possession ou qui contrôle un support de stockage de données informatiques ou un système informatique faisant l'objet d'une perquisition au titre de la section 12 doit autoriser, et assister si nécessaire, la personne chargée de la perquisition, en vue:*

(a) d'accéder et d'utiliser un système informatique ou un support de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système; et

(b) obtenir et copier ces données informatiques; et

(c) utiliser l'équipement pour faire des copies; et

(d) obtenir une sortie intelligible d'un système informatique en format simple pouvant être lu par quiconque.

(2) Une personne qui, sans justification ou excuse légale, autorise ou assiste une personne à commettre une infraction est passible, sur condamnation, d'une peine de prison d'une durée maximale de [période] ou d'une amende maximale de [montant], ou des deux.

6.5.7 Injonction de produire

Même si une obligation comme celle prévue à l'article 19, paragraphe 4, de la Convention du Conseil de l'Europe sur la cybercriminalité n'est pas transposée dans la législation nationale, les fournisseurs coopèrent souvent avec les forces de l'ordre afin d'éviter un impact négatif sur leurs activités. Si, en raison d'un manque de coopération du fournisseur, les enquêteurs ne sont pas en mesure de trouver les données ou les périphériques de stockage qu'ils doivent perquisitionner et saisir, il est probable qu'ils auront besoin de saisir plus de matériel que nécessaire. C'est pourquoi les fournisseurs préfèrent en général coopérer et fournir les données pertinentes à la demande des forces de l'ordre. La Convention du Conseil de l'Europe sur la cybercriminalité contient des instruments permettant aux enquêteurs de se passer d'ordres de perquisition si la personne en possession des données pertinentes les leur soumet. [2348]

Bien que ces efforts conjoints des forces de l'ordre et des fournisseurs de services semblent être un exemple positif de partenariat public-privé, y compris dans les cas où il n'y a pas de base juridique, cette coopération non réglementée continue de poser plusieurs difficultés. Outre les problèmes de protection des données, la principale préoccupation réside dans le fait que les fournisseurs de services pourraient violer leurs obligations contractuelles vis-à-vis de leurs clients s'ils répondent à une requête de soumission de certaines données qui ne reposerait pas sur une base juridique suffisante.[2349]

Article 18 – Injonction de produire
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

> *b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.*

L'article 18 contient deux obligations. Conformément à son paragraphe 1.a, toute personne (y compris un fournisseur de services) doit communiquer les données informatiques spécifiées en sa possession ou sous son contrôle. Contrairement au paragraphe 1.b, l'application de cette disposition ne se limite pas à certaines données spécifiques. L'expression « en sa possession » exige que la personne ait un accès physique aux dispositifs de stockage des données où les informations spécifiées sont sauvegardées.[2350] La portée de cette disposition est encore étendue par le terme de « contrôle ». Des données sont placées sous le contrôle d'une personne si celle-ci les gère, même en l'absence d'un accès physique. C'est, par exemple, le cas si le suspect a stocké des données pertinentes sur un système de stockage en ligne à distance. Dans leur rapport explicatif, les auteurs de la Convention sur la cybercriminalité rappellent toutefois que la simple capacité technique d'accéder à distance aux données stockées ne constitue pas nécessairement un contrôle de celles-ci.[2351] L'application de l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité est donc limitée aux cas où le degré de contrôle du suspect dépasse son éventuelle capacité à y accéder.

L'alinéa 1 .b mentionne une injonction de produire limitée à certaines données. Sur cette base, les enquêteurs peuvent ordonner à un fournisseur de services de soumettre les informations relatives à ses abonnés. Ces données peuvent être nécessaires à l'identification d'un criminel. Si les enquêteurs sont en mesure de retrouver l'adresse IP utilisée par le contrevenant, ils doivent ensuite la relier à un individu.[2352] Dans la plupart des cas, une adresse IP ne mène qu'à un prestataire Internet ayant fourni cette adresse à l'utilisateur. Avant d'autoriser l'utilisation d'un service, les fournisseurs d'accès à Internet exigent en général des utilisateurs qu'ils s'inscrivent en soumettant leurs informations personnelles.[2353] L'article 18, paragraphe 1.b,permet aux enquêteurs d'ordonner au fournisseur de produire ces informations. Dans ce contexte, il est important de souligner que l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité n'impose toutefois pas d'obligation de rétention des données[2354] ou d'obligation pour les fournisseurs de services d'enregistrer les informations relatives à leurs abonnés.[2355]

La distinction faite entre « données informatiques » au paragraphe 1.a et « données relatives aux abonnés » au paragraphe 1.b semble à première vue inutile, dans la mesure où ce type de données, lorsqu'elles sont stockées sous forme numérique, est également couvert par le paragraphe 1.a. Cette distinction s'explique d'abord par les différentes définitions de « données informatiques » et de « données relatives aux abonnés ». Contrairement aux « données informatiques », le terme de « données relatives aux abonnés » n'exige pas que celles-ci soient stockées en tant que données informatiques. L'article 18, paragraphe 1.b, de la Convention du Conseil de l'Europe sur la cybercriminalité permet aux autorités répressives compétentes de présenter des informations conservées dans un format non numérique.[2356]

> ***Article 1** – **Définitions***
> *Aux fins de la présente Convention:*
> *[…]*
> *b. l'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;*

> ***Article 18** – Injonction de produire*
> *[…]*
> *3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:*
>
> > *a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;*

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;
c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

La seconde raison expliquant la distinction faite entre « données informatiques » et « données relatives aux abonnés » est qu'elle permet aux législateurs de prévoir différentes exigences pour l'application des instruments juridiques.[2357] Ainsi, il leur est possible d'imposer des conditions plus strictes[2358] pour une injonction de production au titre du paragraphe 1.b, puisque cet instrument permet aux forces de l'ordre d'accéder à toutes sortes de données informatiques, y compris celles relatives au contenu.[2359] La distinction entre la collecte en temps réel des données relatives au trafic (article 20)[2360] et celle des données relatives au contenu (article 21)[2361] montre que les auteurs de la Convention sur la cybercriminalité se sont aperçus qu'en fonction de la nature des données auxquelles ont accès les forces de l'ordre, différentes sauvegardes doivent être prévues.[2362] En faisant la différence entre « données informatiques » et « données relatives aux abonnés », l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité permet à ses Etats signataires de mettre sur pied un système similaire de sauvegardes graduelles pour l'injonction de production.[2363]

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique

Une approche similaire est proposée par la loi type du Commonwealth de 2002.[2364]

Production de données
15. *Lorsqu'un magistrat estime, sur la base d'une demande faite par l'officier de police, que des données informatiques spécifiées, ou une impression d'autres informations, sont raisonnablement nécessaires aux fins d'une enquête criminelle ou de poursuites pénales, il peut ordonner:*
(a) qu'une personne sur le territoire de [État prenant les dispositions] qui contrôle un système informatique produise, à partir du système, des données informatiques spécifiées ou une impression ou toute autre forme de sortie intelligible de ces données; et
(b) qu'un prestataire de services Internet dans [État prenant les dispositions] produise des informations sur des personnes qui sont abonnées ou utilisent autrement le service; et
(c)[2365] qu'une personne sur le territoire de [État prenant les dispositions] ayant accès à un système informatique spécifié compile des données informatiques spécifiées à partir du système et les transmette à une personne désignée.

6.5.8 Collecte de données en temps réel

La surveillance téléphonique est un instrument utilisé dans de nombreux pays dans le cadre d'enquêtes sur des délits majeurs.[2366] Nombre d'infractions nécessitent l'utilisation d'un téléphone, en particulier portable, que ce soit pour la préparation ou l'exécution du délit. Dans les affaires de trafic de drogue notamment, l'écoute de conversations entre criminels peut être une étape essentielle au succès de l'enquête. Cet instrument permet aux enquêteurs de rassembler de précieuses informations, même s'il se limite à celles échangées sur les lignes/téléphones sous écoute. Si le contrevenant utilise d'autres moyens de communication (par ex. des lettres) ou des lignes qui ne sont pas placées sous écoute, les enquêteurs ne pourront pas enregistrer ces conversations. D'une manière générale, la situation est la même lorsqu'il s'agit de conversations directes ne se déroulant pas au téléphone.[2367]

Aujourd'hui, l'échange de données a remplacé les conversations téléphoniques traditionnelles. L'échange de données ne se limite pas aux courriels ou aux transferts de fichiers. De plus en plus souvent, la communication vocale se fait grâce à des technologies basées sur des protocoles Internet (voix sur IP).[2368] D'un point de vue technique, un appel téléphonique voix sur IP est plus proche d'un échange de courriels que d'un appel conventionnel passant par un fil téléphonique. L'interception de ce type d'appel pose des difficultés particulières.[2369]

Etant donné que la criminalité informatique fait souvent appel à des échanges de données, la possibilité de les intercepter ou d'utiliser les données liées à ces échanges peut être une condition essentielle de l'aboutissement des enquêtes. L'application des dispositions existantes en matière de surveillance téléphonique et des dispositions sur l'utilisation des données relatives au trafic de télécommunications dans le cadre d'enquête cybercriminelles s'est avérée difficile dans certains pays. Les obstacles rencontrés sont de nature technique[2370] et juridique. D'un point de vue juridique, l'autorisation d'enregistrer une conversation téléphonique n'équivaut pas nécessairement à autoriser l'interception des processus de transfert de données.

La Convention du Conseil de l'Europe sur la cybercriminalité vise à combler les lacunes existantes dans les capacités des forces de l'ordre de surveiller les processus de transfert de données.[2371] Dans cette approche, la Convention sur la cybercriminalité distingue deux modalités d'observation des transferts de données. L'article 20 autorise les enquêteurs à collecter les données relatives au trafic, terme défini à l'article 1 d) de la Convention.

Article 1 – Définitions
[…]
d. « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

La distinction entre « données relatives au contenu » et « données relatives au trafic » est la même que celle appliquée dans la plupart des législations nationales sur ces questions. [2372]

6.5.9 Collecte des données relatives au trafic

Convention du Conseil de l'Europe sur la cybercriminalité

Ayant à l'esprit que la définition des données relatives au trafic varie d'un pays à un autre,[2373] les auteurs de la Convention du Conseil de l'Europe sur la cybercriminalité ont décidé de définir ce terme de façon à améliorer l'application des dispositions y afférentes dans le cadre d'enquêtes internationales. Le terme de « données relatives au trafic » est utilisé pour décrire les données générées par les ordinateurs pendant le processus de communication permettant d'acheminer la communication de son point d'origine à sa destination. Dès qu'un utilisateur se connecte à Internet, télécharge ses courriels ou ouvre un site, des données relatives au trafic sont générées. Pour les enquêtes cybercriminelles, les plus pertinentes, pour retracer l'origine et la destination des données, sont les adresses IP identifiant les parties à la communication en ligne.[2374]

Contrairement aux « données relatives au contenu », le terme de « données relatives au trafic » ne couvre que les données générées dans le cadre de processus de transfert de données et non les données transmises elles-mêmes. Même si l'accès aux données de contenu peut être nécessaire dans certains cas, puisqu'il permet aux forces de l'ordre d'analyser les communications de façon bien plus efficace, les données relatives au trafic jouent un rôle important dans les investigations cybercriminelles.[2375] Alors que l'accès aux données relatives au contenu permet aux forces de l'ordre d'analyser la nature des messages ou des fichiers échangés, les données relatives au trafic sont nécessaires pour identifier le contrevenant. Dans les affaires de pédopornographie, les données relatives au trafic permettent, par exemple, aux enquêteurs d'identifier le site Internet d'où le criminel télécharge des images pédopornographiques. En contrôlant les données relatives au trafic générées pendant l'utilisation de services Internet, les forces de l'ordre peuvent identifier les adresses IP du serveur actif et ensuite, essayer de déterminer sa localisation physique.

Article 20 – Collecte en temps réel des données relatives au trafic
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:

> *a. à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et*
> *b. à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:*
> *i. à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou*
> *ii. à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.*
> *2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.*
> *3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.*
> *4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.*

L'article 20 prévoit deux approches différentes pour la collecte des données relatives au trafic. Toutes deux sont censées être mises en œuvre.[2376]

La première prévoit une obligation pour les fournisseurs d'accès à Internet de permettre aux forces de l'ordre de collecter directement les données pertinentes. Cette approche exige, en général, l'installation d'une interface que les forces de l'ordre peuvent utiliser pour accéder à l'infrastructure du FAI.[2377]

La seconde approche prévoit la possibilité pour les forces de l'ordre de contraindre un FAI à collecter des données à leur demande. Elle permet aux forces de l'ordre d'utiliser les capacités techniques existantes et les connaissances dont disposent en général les fournisseurs. En associant ces deux approches, l'une des intentions est de garantir que les forces de l'ordre seront en mesure de mener à bien leur enquête (sur la base de l'article 20, paragraphe 1.b, sans l'aide du fournisseur, si celui-ci ne dispose pas des technologies nécessaires à l'enregistrement de données.[2378]

La Convention du Conseil de l'Europe sur le cybercriminalité n'a pas été rédigée pour privilégier une certaine technologie, ni établir des normes qui exigeraient des investissements financiers plus importants pour le secteur concerné.[2379] Partant, l'article 20, paragraphe 1.a, de la Convention sur la cybercriminalité semble être la meilleure solution. Toutefois, les dispositions de l'article 20, paragraphe 2, montrent que les auteurs de la Convention sur la cybercriminalité étaient conscients du fait que certains pays pourraient rencontrer des difficultés dans la mise en œuvre d'une législation permettant aux forces de l'ordre de mener directement les investigations.

L'un des principaux problèmes posés par les investigations basées sur l'article 20 est l'utilisation de moyens de communication anonyme. Comme nous l'avons expliqué ci-dessus,[2380] les contrevenants peuvent utiliser des services Internet permettant une communication anonyme. S'ils utilisent, par exemple, un service de communication anonyme comme le logiciel Tor,[2381] les enquêteurs seront, dans la plupart des cas, incapables d'analyser les données relatives au trafic et d'identifier avec succès les partenaires de communication. Les criminels peuvent obtenir des résultats similaires en utilisant des terminaux publics d'accès à Internet.[2382]

Par rapport aux procédures traditionnelles de perquisition et de saisie, l'un des avantages de la collecte de données relatives au trafic est que le suspect d'un crime ne s'aperçoit pas nécessairement qu'une enquête est en cours,[2383] ce qui limite ses possibilités de manipuler ou d'effacer des preuves. Pour que les criminels ne soient pas informés par le fournisseur de services de l'enquête en cours, l'article 20, paragraphe 3, oblige les Etats signataires à mettre en œuvre une législation garantissant que les FAI préserveront le caractère confidentiel des enquêtes en cours. Pour le prestataire de services, cette approche présente l'avantage de le dispenser de son obligation d'information[2384] des utilisateurs.[2385]

La Convention du Conseil de l'Europe sur la cybercriminalité a été rédigée afin d'améliorer et d'harmoniser la législation relative à la cybercriminalité.[2386] Dans ce contexte, il est important de souligner que le texte

de l'article 21 ne s'applique pas uniquement aux délits liés à la cybercriminalité, mais à tout type d'infraction. Etant donné que l'utilisation de moyens de communication électronique peut être pertinente bien au-delà des affaires de cybercriminalité, l'application de ces dispositions à des délits d'une autre nature peut être un outil d'enquête utile. Il permettrait, par exemple, aux forces de l'ordre d'utiliser les données relatives au trafic générées pendant l'échange de courriels entre contrevenants dans la préparation d'un délit traditionnel. L'article 14, paragraphe 3, accorde aux parties la possibilité de formuler des réserves et de limiter l'application de ces dispositions à certaines infractions précises.[2387]

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique

Une approche similaire est proposée par la loi type du Commonwealth de 2002.[2388]

Interception de données relatives au trafic
19. *(1) Si un officier de police estime que les données relatives au trafic associées à une communication spécifiée sont demandées raisonnablement aux fins d'une enquête criminelle, il peut, par notification écrite remise à une personne qui contrôle de telles données, demander que cette dernière:*

(a) Collecte ou enregistre les données relatives au trafic associées à une communication spécifiée pendant une période désignée; et

(b) autorise et assiste un officier de police désigné à collecter ou à enregistrer ces données.

(2) Si un magistrat estime, sur la base de [informations données sous serment] [affidavit], qu'il existe des motifs valables [de suspecter] que les données relatives au trafic sont nécessaires aux fins d'une enquête criminelle, le magistrat [peut] [devra] autoriser un officier de police à collecter ou à enregistrer les données relatives au trafic associées à une communication désignée pendant une période spécifiée par l'application de moyens techniques.

6.5.10 Interception de données relatives au contenu

Convention du Conseil de l'Europe sur la cybercriminalité

Mis à part le fait que l'article 21 traite des données relatives au contenu, sa structure est proche de celle de l'article 20. La possibilité d'intercepter des échanges de données peut s'avérer importante dans les cas où les forces de l'ordre savent déjà qui sont les partenaires de communication, mais n'ont aucune information sur le type de communication. L'article 21 leur donne la possibilité d'enregistrer les communications de données et d'en analyser le contenu.[2389] Ceci inclut les fichiers téléchargés à partir de sites Internet ou de systèmes de partage de fichiers, les courriels envoyés ou reçus par le contrevenant et les conversations par *chat*.

Article 21 – Interception de données relatives au contenu
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne:

a. à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b. à obliger un fournisseur de services, dans le cadre de ses capacités techniques:

i. à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Contrairement aux données relatives au trafic, la Convention du Conseil de l'Europe sur la cybercriminalité ne donne pas de définition des données relatives au contenu. Comme le terme le dit implicitement, les « données relatives au contenu » font référence au contenu de la communication.

Parmi les exemples de données relatives au contenu couvertes par les enquêtes cybercriminelles, citons:

- le sujet d'un courriel;
- le contenu d'un site Internet ouvert par le suspect;
- le contenu d'une conversation VoIP.

L'une des principales difficultés des enquêtes basées sur l'article 21 est l'utilisation de technologies de chiffrement.[2390] Comme nous l'avons expliqué en détail plus haut, l'utilisation de ce type de technologies permet aux criminels de protéger les contenus échangés de façon à rendre impossible leur accès par les forces de l'ordre. Si le criminel crypte les contenus qu'il/elle transfère, les forces de l'ordre ne pourront qu'intercepter la communication cryptée, mais non analyser son contenu. Sans la clé utilisée pour le cryptage de ces fichiers, tout éventuel décryptage pourrait prendre très longtemps.[2391]

Loi-type du Commonwealth relative à la criminalité informatique et liée à l'informatique

Une approche similaire est proposée par la loi type du Commonwealth de 2002.[2392]

> ***Interception de communications électroniques***
> *18. (1) Si un [magistrat] [juge] estime, sur la base des informations [obtenues sous serment] [affidavit] qu'il existe des motifs valables [de suspecter] [de penser] que le contenu de communications électroniques est nécessaire aux fins d'une enquête criminelle, le magistrat [peut] [doit]:*
>
> *(a) ordonner à un prestataire de services Internet dont les services sont disponibles dans [État prenant les dispositions] de collecter ou enregistrer par l'utilisation de moyens techniques, ou autoriser ou assister les autorités compétentes en vue de collecter ou enregistrer des données relatives au contenu associées à des communications spécifiques transmises au moyen d'un système informatique; ou*
> *(b) autoriser un officier de police à collecter ou à enregistrer ces données par l'utilisation de moyens techniques.*

6.5.11 Règlementation concernant les technologies de chiffrement

Comme nous l'avons rappelé ci-dessus, les criminels peuvent aussi entraver l'analyse des données de contenu en utilisant des technologies de chiffrement. Plusieurs logiciels existent qui permettent aux utilisateurs de protéger efficacement leurs fichiers ainsi que les processus de transfert des données contre tout accès non autorisé.[2393] Si les suspects ont utilisé de tels logiciels et que les autorités chargées de l'enquête n'ont pas accès à la clé utilisée pour le cryptage des fichiers, le décryptage nécessaire peut prendre très longtemps.[2394]

L'utilisation de technologies de chiffrement par les criminels représente un défi pour les forces de l'ordre.[2395] Plusieurs approches nationales et internationales[2396] s'attaquent à ce problème.[2397] Etant donné les différences d'estimation de la menace que constituent les technologies de cryptage, il n'y a pas encore d'approche mondiale largement acceptée pour résoudre ce problème.

L'une des possibilités est d'autoriser les forces de l'ordre à percer le cryptage, si nécessaire.[2398] Sans une telle autorisation ou la possibilité d'émettre une injonction de production, les autorités d'enquête pourraient ne pas être en mesure de rassembler les preuves nécessaires. De plus, il est également possible pour les enquêteurs d'être autorisés à utiliser des logiciels d'espionnage de clavier pour intercepter une phrase de chiffrement d'un fichier crypté dans le but de le décoder.[2399]

Une autre approche consiste à diminuer la performance du logiciel de chiffrement en limitant la longueur de la clé.[2400] En fonction du degré de limitation, les enquêteurs pourront décoder les clés dans un délai raisonnable. Les opposants à une telle solution craignent que cette limitation ne permette aux enquêteurs de percer le cryptage, mais aussi de faciliter la tâche aux espions d'entreprise tentant d'obtenir l'accès à

des informations commerciales cryptées.[2401] De plus, cette restriction ne stopperait pas les criminels utilisant un cryptage plus puissant, si ces outils sont disponibles. Il conviendrait d'abord d'adopter des règles internationales empêchant les concepteurs de produits de cryptage avancé de proposer leurs logiciels dans les pays n'ayant pas de restriction adaptée de la longueur de clé. Quoi qu'il en soit, il sera relativement aisé pour les contrevenants de développer leur propre logiciel de chiffrement sans aucune limite de longueur de clé.

L'obligation de créer un compte séquestre de clé ou d'établir une procédure de récupération de clé est une autre approche pour les produits de chiffrement puissants.[2402] L'application de telles règles permettrait aux internautes de continuer à utiliser ces technologies de cryptage puissantes, tout en donnant accès aux enquêteurs aux données pertinentes en forçant les utilisateurs à communiquer leur clé à une autorité spéciale qui les conserve et les fournit aux enquêteurs, si nécessaire.[2403] Les détracteurs d'une telle solution craignent que les gens n'aient accès aux clés transmises et, par leur biais, à des informations secrètes décryptées. De plus, les contrevenants pourraient assez facilement contourner les règles en développant leur propre logiciel de chiffrement qui n'exigerait pas la transmission des clés à l'autorité compétente.

La dernière possibilité pour les pays est de répondre à cette question en faisant appliquer une injonction de production.[2404] Ce terme décrit l'obligation de dévoiler la clé utilisée pour crypter des données. La mise en œuvre d'un tel instrument a été discutée lors de la réunion du G8 à Denver en 1997.[2405] Plusieurs pays ont depuis créé une telle obligation.[2406] C'est le cas de la section 69 de la loi indienne sur les technologies de l'information de 2000.[2407] La section 49 de la loi britannique de réglementation des pouvoirs d'enquête de 2000 en est un autre exemple national.[2408]

Notification de l'obligation de divulgation

***49**. (1) Cette section s'applique lorsqu'une information protégée*

(a) est devenue la possession de quiconque au moyen de l'exercice d'un pouvoir conféré par la loi de saisir, détenir, inspecter, perquisitionner ou autre pour interférer avec des documents ou autres propriétés ou est susceptible de le devenir;

(b) est devenue la possession de quiconque au moyen de l'exercice d'un pouvoir conféré par la loi d'intercepter des communications, ou est susceptible de le devenir;

(c) est devenue la possession de quiconque au moyen de l'exercice de tout pouvoir conféré par une autorisation au titre de la Sec. 22 (3) ou de la Partie II, ou à la suite d'une notification adressée au titre de la Sec. 22 (4), ou est susceptible de le devenir;

(d) est devenue la possession de quiconque après avoir été fournie ou divulguée conformément à un devoir conféré par la loi (survenant ou non à la suite d'une demande d'information), ou est susceptible de le devenir; ou

(e) est devenue la possession par tout moyen légitime n'impliquant pas l'exercice de pouvoirs conférés par la loi, de tout service de renseignement, de la police, ou des douanes, ou est susceptible de devenir la possession d'un quelconque de ces services, de la police ou des douanes.

(2) toute personne titulaire de l'autorisation appropriée au titre du « schedule 2 » estimant, en s'appuyant sur des motifs valables,

(a) qu'une personne possède une clé pour les informations protégées,

(b) que l'imposition d'une exigence de divulgation concernant les informations protégées est

(i) nécessaire conformément à la sous-section (3) ou

(ii) nécessaire aux fins de garantir un exercice efficace ou les performances correctes de la part de toute autorité publique ayant un pouvoir conféré par la loi ou une obligation prévue par la loi,

(c) que l'imposition d'une telle exigence est proportionnée à ce que l'on cherche à atteindre par cette imposition, et

(d) que, raisonnablement, il est difficile pour la personne ayant l'autorisation appropriée d'obtenir la possession des informations protégées dans une forme intelligible sans donner une notification au titre de cette section,

Cette personne peut, en notifiant celle qu'elle croit posséder la clé, imposer une exigence de divulgation concernant les informations protégées.

(3) une exigence de divulgation concernant les informations protégées s'impose pour des motifs conformes à cette sous-section si cela est nécessaire-

(a) dans l'intérêt de la sécurité nationale;
(b) aux fins d'empêcher ou de détecter une activité criminelle; ou
(c) dans l'intérêt de l'économie du Royaume-Uni.
(4) Une notification au titre de cette section imposant une exigence de divulgation concernant toute information protégée-
(a) doit être donnée par écrit ou (si elle n'est pas donnée par écrit) doit être donnée de manière à laisser une trace prouvant que cette notification a été donnée;
(b) doit décrire les informations protégées auxquelles cette notification se rapporte;
(c) doit préciser les questions du ressort de la sous-section (2)(b)(i) ou (ii) en se référant à la raison pour laquelle la notification est donnée;
(d) doit préciser le bureau, la fonction ou le poste occupé par la personne donnant la notification;
(e) doit préciser le bureau, la fonction ou le poste de la personne qui, aux fins du Schedule 2, a accordé l'autorisation de donner la notification ou (si la personne donnant la notification était habilitée à le faire sans l'autorisation d'une autre personne) doit fixer les circonstances dans lesquelles ce droit est valable;
(f) doit préciser le moment auquel la notification doit être respectée; et
(g) doit définir la divulgation demandée par la notification ainsi que la forme et la manière dont elle doit être faite;
et le moment précisé aux fins du paragraphe (f) doit autoriser une période de mise en conformité raisonnable dans toutes les circonstances.

Afin de garantir que la personne obligée de dévoiler la clé respecte l'injonction et transmette vraiment celle-ci, la loi britannique de 2000 sur les pouvoirs d'enquête contient une disposition criminalisant la non exécution de l'injonction.

Non-respect d'une notification
53*. (1) Quiconque ayant reçu une notification au titre de la Sec. 49 est jugé coupable d'une infraction si, en toute connaissance de cause, conformément à ladite notification, il n'exécute pas la divulgation requise par le fait qu'il a reçu ladite notification.*
(2) Dans le cas de poursuites visant une personne pour une infraction commise au titre de cette section, s'il est démontré que cette personne était en possession d'une clé concernant des informations protégées à tout moment avant la réception de la notification au titre de la Sec. 49, cette personne sera considérée, aux fins de ces poursuites, comme ayant continué à posséder cette clé ultérieurement sauf s'il est démontré que la clé n'était pas en sa possession après remise de la notification et avant le moment où cette personne a été requise de divulguer la clé.
(3) Aux fins de cette section, une personne est considérée comme ayant prouvé qu'elle n'était pas en possession d'une clé pour protéger les informations à un moment particulier si-
(a) des preuves suffisantes du fait sont invoquées pour soulever un problème à ce propos; et
(b) le contraire n'est pas prouvé au-delà d'un doute raisonnable.
(4) Dans toute poursuite contre quiconque pour une infraction au titre de cette section, cette personne pourra user de ce moyen de défense si elle peut prouver:
(a) qu'il n'était pas raisonnablement possible pour elle de divulguer la clé requise conformément à la remise de la notification au titre de la section 49 avant le moment où elle a été requise conformément à cette injonction; mais
(b) qu'elle a divulgué la clé immédiatement après le moment où cela est devenu raisonnablement possible pour elle de le faire.
(5) Toute personne coupable d'une infraction au titre de cette section sera passible-
(a) sur condamnation après mise en accusation, d'une peine de prison d'une durée maximale de deux ans ou d'une amende ou des deux;
(b) sur déclaration de culpabilité par procédure sommaire, d'une peine de prison d'une durée maximale de six mois ou d'une amende ne dépassant pas le maximum prévu par la loi ou des deux.

[…]

La loi de 2000 sur la réglementation des pouvoirs d'enquête oblige le suspect d'un crime à collaborer avec les forces de l'ordre.[2409] Ces dispositions suscitent une interrogation majeure au sujet du fait que l'obligation crée un conflit potentiel avec le droit fondamental d'un suspect de ne pas témoigner contre lui-même.[2410] Plutôt que de laisser l'enquête aux autorités compétentes, le suspect doit activement soutenir celle-ci. La forte protection contre l'auto-incrimination qui existe dans de nombreux pays pose donc la question de savoir jusqu'où une telle règle peut devenir la solution type pour relever le défi posé par les technologies de chiffrement.[2411]

Une autre inquiétude réside dans le fait que perdre la clé pourrait déclencher une enquête pénale. Même si le caractère pénal est lié au refus du contrevenant de dévoiler la clé, émis sciemment, cette perte pourrait impliquer des personnes utilisant des clés de cryptage dans des poursuites pénales qu'elles ne souhaitaient pas. Toutefois, la section 53 (2), en particulier, peut potentiellement interférer avec la charge de la preuve.[2412]

Enfin, il existe des solutions techniques permettant aux contrevenants de contourner l'obligation de dévoiler la clé utilisée pour le chiffrement des données. Citons, par exemple, l'utilisation d'un logiciel de cryptage basé sur le principe du « démenti plausible ».[2413] [2414]

6.5.12 Logiciel judiciaire à distance

Comme nous l'avons expliqué ci-dessus, la recherche de preuves sur l'ordinateur du suspect exige d'avoir physiquement accès au matériel pertinent (système informatique et supports de stockage externes). En général, cette procédure implique d'avoir accès à l'appartement, à la maison ou au bureau du suspect. Celui-ci sera alors mis au courant de l'enquête en cours dès que les enquêteurs commenceront leurs recherches.[2415] Cette information pourrait entraîner un changement de son comportement.[2416] Si le contrevenant, par exemple, a attaqué quelques systèmes informatiques afin de tester ses capacités pour se préparer à une série d'attaques de plus grande ampleur, qu'il prévoit de mener avec d'autres criminels, la procédure de recherche pourrait empêcher les enquêteurs d'identifier les autres suspects puisqu'il est très probable que le contrevenant arrête de communiquer avec eux.

Afin d'éviter que les enquêtes en cours ne soient détectées, les forces de l'ordre exigent de disposer d'un instrument leur permettant d'avoir accès aux données informatiques stockées sur l'ordinateur du suspect et pouvant être secrètement utilisées. La surveillance téléphonique est un exemple de ce type d'instruments pour le contrôle des appels téléphoniques.[2417] Un tel instrument permettrait aux forces de l'ordre d'accéder à distance à l'ordinateur du suspect pour y rechercher des informations. Actuellement, la question de l'utilité de ces instruments fait l'objet de discussions intenses.[2418] En 2001 déjà, des rapports signalaient que le FBI américain était en train de développer un outil d'enregistrement de frappe destiné aux enquêtes liées à Internet et baptisé la « lanterne magique ».[2419] En 2007, des documents ont été publiés affirmant que les forces de l'ordre américaines utilisaient des logiciels pour retrouver la trace de suspects ayant utilisé des moyens de communication anonyme.[2420] Ces rapports faisaient référence à un mandat de perquisition qui exigeait l'utilisation d'un outil baptisé CIPAV.[2421] [2422] Après que la Cour fédérale allemande ait décidé que les dispositions existantes du Code de procédure pénal ne permettaient pas aux enquêteurs d'utiliser des logiciels judiciaires à distance pour rechercher en secret des informations stockées sur l'ordinateur d'un suspect, un débat sur la nécessité d'amender les législations existantes en la matière a été lancé.[2423] A cette occasion, des informations ont été publiées selon lesquelles des autorités responsables d'enquêtes avaient illégalement utilisé de tels logiciels dans quelques investigations.[2424]

Plusieurs concepts de « logiciel judiciaire à distance » ont été débattus, de même que les éventuelles fonctions d'un tel outil.[2425] D'un point de vue théorique, ce logiciel pourrait avoir les fonctions suivantes: d'abord, une fonction de recherche. Celle-ci permettrait aux forces de l'ordre de rechercher des contenus illégaux et de collecter des informations sur les fichiers stockés sur l'ordinateur.[2426] Puis, une fonction d'enregistrement. Les enquêteurs pourraient enregistrer les données traitées par le système informatique du suspect, mais non stockées de façon permanente. Si, par exemple, le suspect utilise des services voix sur IP pour communiquer avec d'autres suspects, le contenu de leur conversation ne sera, en général, pas

stocké.[2427] Le logiciel judiciaire à distance pourrait enregistrer les données traitées afin de les conserver pour les enquêteurs. Si le logiciel judiciaire à distance contient un module d'enregistrement des pressions sur touche, il pourrait servir à enregistrer les mots de passe utilisés par le suspect pour crypter ses fichiers.[2428] De plus, un tel outil pourrait inclure des fonctions d'identification qui permettraient aux enquêteurs de prouver la participation du suspect à un délit pénal, même s'il/elle a utilisé des services de communication anonyme rendant difficile la tâche des enquêteurs d'identifier le contrevenant en retrouvant l'adresse IP utilisée.[2429] Enfin, le logiciel à distance pourrait être utilisé pour activer une webcam ou un microphone afin d'observer la pièce où l'équipement se trouve.[2430]

Même si les éventuelles fonctions du logiciel semblent pouvoir être très utiles aux enquêteurs, il est important de rappeler qu'il existe plusieurs difficultés juridiques et techniques liées à l'utilisation d'un tel outil. D'un point de vue technique, les aspects suivants doivent être pris en compte. Difficultés liées au processus d'installation

Le logiciel doit être installé sur le système informatique du suspect. La multiplication de logiciels malveillants prouve que l'installation d'un logiciel sur l'ordinateur d'un internaute sans sa permission est possible. Mais la principale différence entre un virus et un logiciel judiciaire à distance est que ce dernier doit être installé sur un système informatique précis (l'ordinateur du suspect) alors qu'un virus informatique a pour but d'infecter le plus grand nombre d'ordinateurs sans avoir besoin de cibler un système informatique spécifique. Plusieurs techniques existent pour transmettre un logiciel vers l'ordinateur du suspect, comme l'installation avec accès physique au système informatique; le placement du logiciel sur un site Internet pour téléchargement; l'accès en ligne au système informatique par contournement des mesures de sécurité; et la dissimulation du logiciel dans le flux de données généré pendant les activités en ligne, pour n'en citer que quelques-unes.[2431] Etant donné les mesures de protection dont sont équipés la plupart des ordinateurs, comme les scanners anti-virus et les pare-feu, toutes les méthodes d'installation à distance présentent des difficultés pour les enquêteurs.[2432]

Avantage de l'accès physique

Plusieurs analyses conduites (par ex. inspection physique des supports de traitement des données) exigent l'accès au matériel informatique. De plus, les logiciels judiciaires à distance ne permettent aux enquêteurs que d'analyser les systèmes informatiques connectés à Internet.[2433] Enfin, agissant à distance, il est difficile de conserver l'intégrité du système informatique du suspect.[2434] Au vu de ces éléments, les logiciels judiciaires à distance ne pourront en général pas remplacer l'examen physique du système informatique d'un suspect.

En outre, plusieurs considérations juridiques doivent être prises en compte avant d'appliquer une disposition qui permettra aux enquêteurs d'installer des logiciels judiciaires à distance. Les sauvegardes prévues dans les codes de procédure pénale ainsi que les constitutions de nombreux pays limitent les fonctionnalités potentielles de tels logiciels. En plus de la dimension nationale, l'installation de logiciels judiciaires à distance pourrait violer le principe de la souveraineté nationale.[2435] Si le logiciel est installé sur un ordinateur portable qui quitte le pays après le processus d'installation, le logiciel pourrait permettre aux enquêteurs de mener leurs investigations pénales sur un territoire étranger sans l'autorisation autrement nécessaire des autorités compétentes.

Exemple

Le texte législatif développé par les Etats bénéficiaires dans le cadre de l'initiative HIPCAR[2436] est un exemple de ce type d'approche.

Logiciel de criminalistique

27. *(1) Si un [juge/magistrat] est convaincu, sur la base d'[informations obtenues sous serment/une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de police à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes:*

(a) le suspect de l'infraction, si possible avec ses nom et adresse; et

(b) une description du système informatique ciblé; et

(c) une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et

(d) les raisons justifiant la nécessité de l'utilisation.

(2) Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, puisse être annulé à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner

(a) le moyen technique utilisé ainsi que la date et l'heure de l'application; et

(b) l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et

(c) toute information obtenue.

Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé.

(3) La durée de l'autorisation mentionnée à l'article 27 (1) est limitée à [3 mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser.

(4) L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect.

(5) Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20.

(6) Si nécessaire, un agent [des services répressifs] [de police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation.

(7) [Liste des infractions]

(8) Un pays peut décider de ne pas mettre en œuvre l'article 27.

Les auteurs du texte législatif ont rappelé qu'ils étaient conscients que l'instrument pouvait être très intrusif et éventuellement empiéter sur les droits fondamentaux du suspect.[2437] Plusieurs sauvegardes ont donc été prévues. D'abord, l'utilisation d'un tel logiciel exige que les preuves ne puissent être collectées par d'autres moyens. Ensuite, une injonction émise par un juge ou un magistrat est requise. Enfin, son application doit porter sur quatre éléments clés et les actions autorisées sont limitées par les paragraphes 1 et 2.

6.5.13 Exigence d'autorisation

Les contrevenants peuvent prendre certaines mesures pour compliquer l'enquête. En plus d'utiliser des logiciels permettant une communication anonyme,[2438] ils peuvent rendre leur identification plus difficile encore en utilisant des terminaux publics d'accès à Internet ou des réseaux sans fil ouverts. Des restrictions appliquées à la production de logiciels permettant à l'utilisateur de cacher son identité et à l'accès à des terminaux Internet publics n'exigeant aucune identification permettraient aux forces de l'ordre de mener leurs investigations de façon plus efficace. L'article 7[2439] du décret italien 144,[2440] promulgué en 2005 (loi n° 155/2005)[2441] est un exemple de restriction d'utilisation des terminaux publics dans le but de perpétrer un délit pénal. Cette disposition oblige quiconque souhaite proposer un accès public à Internet (par ex. cafés Internet ou universités)[2442] de demander une autorisation. De plus, cette personne ou entité est tenue d'exiger l'identification de ses clients avant de leur donner accès au service. Puisqu'un particulier créant un réseau d'accès sans fil n'est, en général, pas couvert par cette obligation, ce contrôle peut facilement être contourné si les contrevenants utilisent des réseaux privés non protégés pour cacher leur identité.[2443]

Il est permis de se demander si la plus grande efficacité des enquêtes justifie cette restriction d'accès à Internet et à des services de communication anonyme. La liberté d'accès à Internet est aujourd'hui reconnue comme une dimension importante du libre accès à l'information, un droit protégé par la constitution de nombreux pays. L'obligation d'enregistrement peut empiéter sur le droit de proposer des services Internet sans autorisation, mis en avant par la Déclaration conjointe de 2005, signée par le rapporteur spécial de l'ONU pour la liberté d'opinion et d'expression, le représentant de l'OSCE pour la liberté des médias et le rapporteur spécial de l'OEA pour la liberté d'expression.[2444] Il est probable que l'exigence d'identification affectera l'utilisation de l'Internet, dans la mesure où les internautes devront toujours craindre une surveillance de leur navigation. Même lorsque les utilisateurs savent que leurs activités sont légales, cela peut influencer leurs interactions et leur navigation.[2445] Dans le même temps, les criminels souhaitant éviter d'être identifiés peuvent facilement contourner la procédure d'identification. Ils peuvent, par exemple, utiliser des cartes téléphoniques prépayées, achetées à l'étranger, qui n'exigent aucune identification pour accéder à Internet.

Des craintes semblables se font jour à propos des législations ciblant les services de communication anonyme. Le débat continue sur la pertinence d'appliquer aux technologies et services de communication anonyme des instruments similaires à ceux envisagés pour les technologies de chiffrement.[2446] Outre le conflit entre la protection de la vie privée et la nécessité de permettre l'investigation des délits, les arguments contre l'(impossible) applicabilité des différentes approches juridiques au défi du cryptage valent aussi pour la communication anonyme.

6.6 Coopération internationale

Bibliography (selected): *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4; *Choo,* Trends in Organized Crime, 2008, page 273 *et seq.*; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005; *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992; *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2; *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296; *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931; *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9; *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.6.1 Introduction

De plus en plus de cybercrimes ont une dimension internationale.[2447] Comme nous l'avons rappelé plus haut, derrière ce phénomène se cache, entre autres, le fait que le criminel n'a que très peu besoin de se trouver physiquement là où le service est proposé.[2448] Les contrevenants n'ont, en général, pas besoin d'être là où se trouve leur victime. Etant donné l'absence d'un cadre juridique mondial complet ou

d'instance supranationale capable d'enquêter sur ces délits, les crimes transnationaux exigent des autorités des pays concernés de coopérer.[2449] La mobilité des contrevenants, la présence non nécessaire des criminels sur le lieu du délit et l'impact de celui-ci contraignent les forces de l'ordre et les autorités judiciaires à coopérer et à soutenir l'Etat s'étant déclaré compétent.[2450] Etant donné les divergences existant entre les législations nationales et la limitation du nombre d'instruments, la coopération internationale est considérée comme l'un des principaux défis à la mondialisation de la criminalité.[2451] C'est vrai tant pour les formes traditionnelles de criminalité transfrontalière que pour la cybercriminalité. L'une des principales exigences des enquêteurs collaborant dans des investigations transnationales est la réaction immédiate de leurs homologues dans le pays où le criminel se trouve.[2452] Sur ce point en particulier, les instruments traditionnels de coopération judiciaire internationale en matière de droit pénal ne remplissent très souvent pas les exigences de vitesse liées aux enquêtes sur Internet.[2453]

6.6.2 Mécanismes de coopération internationale

Pour les enquêtes cybercriminelles, les mécanismes formels les plus pertinents favorisant la coopération internationale sont l'entraide judiciaire et l'extradition D'autres mécanismes existent, comme le transfert de prisonniers, le transfert des poursuites pénales, la confiscation des produits du crime et le recouvrement des avoirs, mais ils sont moins importants dans la pratique. En plus des mécanismes formels, il existe des modalités informelles de coopération comme l'échange de renseignements entre forces de l'ordre de différents pays.

6.6.3 Aperçu des instruments applicables

Trois grands scénarios s'imposent à l'heure de choisir l'instrument applicable pour la coopération internationale. D'abord, les procédures applicables peuvent être prévues par des accords internationaux, comme la Convention des Nations Unies contre la criminalité transnationale organisée (Convention CTO)[2454] et ses trois protocoles,[2455] ou par des conventions régionales, comme la Convention interaméricaine sur l'assistance mutuelle pour la criminalité,[2456] la Convention européenne d'entraide judiciaire en matière pénale[2457] et la Convention du Conseil de l'Europe sur la cybercriminalité.[2458] La deuxième possibilité est une réglementation des procédures par des accords bilatéraux. De tels accords font en général référence à des requêtes spécifiques pouvant être présentées, puis définissent les procédures et modalités de contact pertinentes de même que les droits et obligations des Etats requérant et requis.[2459] Ainsi, l'Australie a signé plus de 30 accords bilatéraux avec d'autres pays régissant les conditions d'extradition.[2460] Parfois, la négociation de ce type d'accord a également inclus la cybercriminalité, mais il n'est pas certain que les accords actuels encadrent adéquatement ce phénomène.[2461] Si aucun accord bilatéral ou multilatéral n'est applicable, la coopération internationale dépend en général de la courtoisie internationale, basée sur la réciprocité.[2462] Etant donné que la coopération basée sur des accords bilatéraux et la courtoisie dépend dans une grande mesure des circonstances de l'affaire et des pays impliqués, l'aperçu ci-dessous se concentre sur les conventions régionales et internationales.

6.6.4 Convention des Nations Unies contre la criminalité transnationale organisée

Le principal instrument international de coopération judiciaire en matière pénale est la Convention des Nations Unies contre la criminalité transnationale organisée (Convention CTO).[2463] Cette convention contient des instruments importants pour la coopération internationale, mais n'a pas été spécifiquement rédigée pour traiter des questions liées à la cybercriminalité. Elle ne contient pas non plus de dispositions spécifiques sur la manière de traiter les requêtes urgentes de conservation des données.

Application de la Convention des Nations Unies contre la criminalité transnationale organisée

Conformément au paragraphe 1 de son article 3, la Convention ne s'applique aux affaires cybercriminelles que si le délit est le fait d'un groupe du crime organisé. L'article 2 de la Convention CTO définit un groupe criminel organisé comme un groupe structuré, composé de trois personnes ou plus.

***Article 2**. Terminologie*
Aux fins de la présente Convention:

> *(a) L'expression « groupe criminel organisé » désigne un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves ou infractions établies conformément à la présente Convention, pour en tirer, directement ou indirectement, un avantage financier ou un autre avantage matériel;*
>
> *[...]*
>
> ***Article 3**. Champ d'application*
>
> *1. La présente Convention s'applique, sauf disposition contraire, à la prévention, aux enquêtes et aux poursuites concernant:*
>
> *(a) les infractions établies conformément aux articles 5, 6, 8 et 23 de la présente Convention; et*
>
> *(b) les infractions graves telles que définies à l'article 2 de la présente Convention; lorsque ces infractions sont de nature transnationale et qu'un groupe criminel organisé y est impliqué.*

La Convention est donc particulièrement pertinente pour les affaires impliquant des formes de criminalité organisée. Il ne fait aucun doute que la criminalité organisée est liée à la cybercriminalité. Toutefois, l'étendue de cette implication et donc l'applicabilité de la CTO aux enquêtes cybercriminelles transnationales sont incertaines. De fait, déterminer le degré de participation de la criminalité organisée est particulièrement important. Toutefois, l'analyse du lien entre la criminalité liée à l'identité et la criminalité organisée présente des difficultés. Le premier obstacle, et le plus important, est l'absence de recherches scientifiques fiables en la matière. Contrairement aux aspects techniques des délits, la dimension liée à la criminalité organisée des infractions a moins souvent été analysée. Plusieurs enquêtes ont abouti à l'identification de gangs criminels impliqués dans la cybercriminalité, mais la structure de ces groupes n'est pas nécessairement comparable à celles des groupes traditionnels du crime organisé. Les groupes cybercriminels ont tendance à avoir une structure plus lâche et plus souple.[2464] De plus, ils sont souvent plus petits par rapport aux groupes criminels organisés traditionnels.[2465] L'Internet permet une étroite coopération entre leurs membres et une coordination de leurs activités qui se déroule sans jamais qu'ils aient besoin de se rencontrer en personne.[2466] Cela permet aux criminels de travailler ensemble au sein de groupes *ad hoc* fluides.[2467]

Demandes d'entraide judiciaire

Les procédures d'entraide judiciaire sont définies à l'article 18. Toute une série de procédures est prévue.

> ***Article 18**. Entraide judiciaire*
>
> *1. Les Etats Parties s'accordent mutuellement l'entraide judiciaire la plus large possible lors des enquêtes, poursuites et procédures judiciaires concernant les infractions visées par la présente Convention, comme prévu à l'article 3, et s'accordent réciproquement une entraide similaire lorsque l'Etat Partie requérant a des motifs raisonnables de soupçonner que l'infraction visée à l'alinéa a ou b du paragraphe 1 de l'article 3 est de nature transnationale, y compris quand les victimes, les témoins, le produit, les instruments ou les éléments de preuve de ces infractions se trouvent dans l'Etat Partie requis et qu'un groupe criminel organisé y est impliqué.*
>
> *2. L'entraide judiciaire la plus large possible est accordée, autant que les lois, traités, accords et arrangements pertinents de l'Etat Partie requis le permettent, lors des enquêtes, poursuites et procédures judiciaires concernant des infractions dont une personne morale peut être tenue responsable dans l'Etat Partie requérant, conformément à l'article 10 de la présente Convention.*
>
> *[...]*

Les paragraphes 1 et 2 de l'article 18 énoncent des principes généraux s'appliquant à la coopération internationale.[2468] Ils sont pertinents à la fois pour les investigations cybercriminelles et les enquêtes traditionnelles. La Convention du Conseil de l'Europe sur la cybercriminalité contient des dispositions similaires.

***Article 18**. Entraide judiciaire*
[...]
3. L'entraide judiciaire qui est accordée en application du présent article peut être demandée aux fins suivantes:
(a) recueillir des témoignages ou des dépositions;
(b) signifier des actes judiciaires;
(c) effectuer des perquisitions et des saisies, ainsi que des gels;
(d) examiner des objets et visiter des lieux;
(e) fournir des informations, des pièces à conviction et des estimations d'experts;
(f) fournir des originaux ou des copies certifiées conformes de documents et dossiers pertinents, y compris des documents administratifs, bancaires, financiers ou commerciaux et des documents de sociétés;
(g) identifier ou localiser des produits du crime, des biens, des instruments ou d'autres choses afin de recueillir des éléments de preuve;
(h) faciliter la comparution volontaire de personnes dans l'Etat Partie requérant;
(i) fournir tout autre type d'assistance compatible avec le droit interne de l'Etat Partie requis.
[...]

Le paragraphe 3 de l'article 18 concerne des demandes spécifiques d'entraide judiciaire. La liste est complexe et va de la collecte de preuves à la localisation des produits du crime. Comme nous l'avons rappelé plus haut, la CTO ne contient pas de texte précis sur les requêtes liées aux données, comme celles émises pour intercepter des communications ou conserver certaines informations. Toutefois, l'alinéa i du paragraphe 3 de l'article 18 s'ouvre à d'autres demandes, permettant à la CTO d'être également utilisée pour les requêtes liées aux données. Bien qu'il soit en général utile de discuter des avantages d'une réglementation spécifique des différentes demandes, les instruments régionaux comparables couvrant des demandes spécifiques, comme la Convention du Conseil de l'Europe sur la cybercriminalité, ne font habituellement référence qu'aux instruments de procédure prévus par le droit national, sans définir de procédures précises en cas de demande d'entraide judiciaire.

***Article 18**. Entraide judiciaire*
[...]
4. Sans préjudice de son droit interne, les autorités compétentes d'un Etat Partie peuvent, sans demande préalable, communiquer des informations concernant des affaires pénales à une autorité compétente d'un autre Etat Partie, si elles pensent que ces informations pourraient l'aider à entreprendre ou à conclure des enquêtes et des poursuites pénales, ou amener ce dernier Etat Partie à formuler une demande en vertu de la présente Convention.
5. La communication d'informations conformément au paragraphe 4 du présent article se fait sans préjudice des enquêtes et poursuites pénales dans l'Etat dont les autorités compétentes fournissent les informations. Les autorités compétentes qui reçoivent ces informations accèdent à toute demande tendant à ce que lesdites informations restent confidentielles, même temporairement, ou à ce que leur utilisation soit assortie de restrictions. Toutefois, cela n'empêche pas l'Etat Partie qui reçoit les informations de révéler, lors de la procédure judiciaire, des informations à la décharge d'un prévenu. Dans ce dernier cas, l'Etat Partie qui reçoit les informations avise l'Etat Partie qui les communique avant la révélation et, s'il lui en est fait la demande, consulte ce dernier. Si, dans un cas exceptionnel, une notification préalable n'est pas possible, l'Etat Partie qui reçoit les informations informe sans retard de la révélation l'Etat Partie qui les communique.
[...]

Les paragraphes 4 et 5 de l'article 18 traitent du partage de renseignements. Ils prévoient une forme de coopération[2469] sur une base volontaire, sans que la partie destinataire n'ait besoin de soumettre une demande d'entraide judiciaire.[2470] Ces dispositions couvrent les informations liées à des affaires pénales, comme celles sur les éventuels consommateurs de pédopornographie situés dans un autre pays et

découvertes au cours de l'enquête. Dans les investigations complexes notamment, quand le recours à des instruments formels est long et peut donc entraver l'enquête, les forces de l'ordre ont tendance à se tourner vers des moyens informels de coopération. Toutefois, le partage d'informations ne peut utilement remplacer la première approche que si l'Etat destinataire des informations est capable de collecter à son niveau toutes les preuves pertinentes. Dans tous les autres cas, une coopération formelle est normalement requise afin de protéger la chaîne de possession. Dans le cadre du débat sur la coopération internationale et le passage des requêtes formelles vers un partage spontané d'informations, il est important de garder à l'esprit que le processus formel a été développé pour protéger l'intégrité des nations ainsi que les droits de l'inculpé. Le partage d'informations ne doit donc pas permettre de contourner le dogme de l'entraide judiciaire.

***Article 18**. Entraide judiciaire*
[...]
6. Les dispositions du présent article n'affectent en rien les obligations découlant de tout autre traité bilatéral ou multilatéral régissant ou devant régir, entièrement ou partiellement, l'entraide judiciaire.
7. Les paragraphes 9 à 29 du présent article sont applicables aux demandes faites conformément au présent article si les Etats Parties en question ne sont pas liés par un traité d'entraide judiciaire. Si lesdits Etats Parties sont liés par un tel traité, les dispositions correspondantes de ce traité sont applicables, à moins que les Etats Parties ne conviennent d'appliquer à leur place les dispositions des paragraphes 9 à 29 du présent article. Les Etats Parties sont vivement encouragés à appliquer ces paragraphes s'ils facilitent la coopération.
8. Les Etats Parties ne peuvent invoquer le secret bancaire pour refuser l'entraide judiciaire prévue au présent article.
9. Les Etats Parties peuvent invoquer l'absence de double incrimination pour refuser de donner suite à une demande d'entraide judiciaire prévue au présent article. L'Etat Partie requis peut néanmoins, lorsqu'il le juge approprié, fournir cette assistance, dans la mesure où il le décide à son gré, indépendamment du fait que l'acte constitue ou non une infraction au droit interne de l'Etat Partie requis.
10. Toute personne détenue ou purgeant une peine sur le territoire d'un Etat Partie, dont la présence est requise dans un autre Etat Partie à des fins d'identification ou de témoignage ou pour qu'elle apporte de toute autre manière son concours à l'obtention de preuves dans le cadre d'enquêtes, de poursuites ou de procédures judiciaires relatives aux infractions visées par la présente Convention, peut faire l'objet d'un transfert si les conditions ci-après sont réunies:
(a) ladite personne y consent librement et en toute connaissance de cause;
(b) les autorités compétentes des deux Etats Parties concernés y consentent, sous réserve des conditions que ces Etats Parties peuvent juger appropriées.
11. Aux fins du paragraphe 10 du présent article:
(a) l'Etat Partie vers lequel le transfert est effectué a le pouvoir et l'obligation de garder l'intéressé en détention, sauf demande ou autorisation contraire de la part de l'Etat Partie à partir duquel la personne a été transférée;
(b) l'Etat Partie vers lequel le transfert est effectué s'acquitte sans retard de l'obligation de remettre l'intéressé à la garde de l'Etat Partie à partir duquel le transfert a été effectué, conformément à ce qui aura été convenu au préalable ou à ce que les autorités compétentes des deux Etats Parties auront autrement décidé;
(c) l'Etat Partie vers lequel le transfert est effectué ne peut exiger de l'Etat Partie à partir duquel le transfert est effectué qu'il engage une procédure d'extradition pour que l'intéressé lui soit soumis;
(d) Il est tenu compte de la période que l'intéressé a passée en détention dans l'Etat Partie vers lequel il a été transféré aux fins du décompte de la peine à purger dans l'Etat Partie à partir duquel il a été transféré.
12. A moins que l'Etat Partie à partir duquel une personne doit être transférée en vertu des paragraphes 10 et 11 du présent article ne donne son accord, ladite personne, quelle que soit sa nationalité, ne sera pas poursuivie, détenue, punie ou soumise à d'autres restrictions à sa liberté de mouvement sur le territoire de l'Etat Partie vers lequel elle est transférée à raison d'actes, d'omissions ou de condamnations antérieurs à son départ du territoire de l'Etat Partie à partir duquel elle a été transférée.
[...]

Les paragraphes 6 à 12 de l'article 18 traitent des aspects procéduraux de l'entraide judiciaire. Les paragraphes 8 et 9 concernent plus particulièrement les affaires de cybercriminalité. Le paragraphe 9 permet aux Etats de refuser les demandes d'entraide judiciaire en invoquant l'absence de double incrimination. C'est particulièrement important dans la mesure où la portée des approches visant à harmoniser les dispositions de droit pénal matériel relatives à la cybercriminalité, comme la Convention du Conseil de l'Europe sur la cybercriminalité, est actuellement limitée. A la mi 2010, seuls 30 pays avaient ratifié cet instrument et fixé des règles minimales pour les infractions cybercriminelles. Cela peut entraver la coopération basée sur la Convention CTO.

***Article 18**. Entraide judiciaire*
[...]
13. Chaque Etat Partie désigne une autorité centrale qui a la responsabilité et le pouvoir de recevoir les demandes d'entraide judiciaire et, soit de les exécuter, soit de les transmettre aux autorités compétentes pour exécution. Si un Etat Partie a une région ou un territoire spécial doté d'un système d'entraide judiciaire différent, il peut désigner une autorité centrale distincte qui aura la même fonction pour ladite région ou ledit territoire. Les autorités centrales assurent l'exécution ou la transmission rapide et en bonne et due forme des demandes reçues. Si l'autorité centrale transmet la demande à une autorité compétente pour exécution, elle encourage l'exécution rapide et en bonne et due forme de la demande par l'autorité compétente. L'autorité centrale désignée à cette fin fait l'objet d'une notification adressée au Secrétaire général de l'Organisation des Nations Unies au moment où chaque Etat Partie dépose ses instruments de ratification, d'acceptation ou d'approbation ou d'adhésion à la présente Convention. Les demandes d'entraide judiciaire et toute communication y relative sont transmises aux autorités centrales désignées par les Etats Parties. La présente disposition s'entend sans préjudice du droit de tout Etat Partie d'exiger que ces demandes et communications lui soient adressées par la voie diplomatique et, en cas d'urgence, si les Etats Parties en conviennent, par l'intermédiaire de l'Organisation internationale de police criminelle, si cela est possible.
14. Les demandes sont adressées par écrit ou, si possible, par tout autre moyen pouvant produire un document écrit, dans une langue acceptable pour l'Etat Partie requis, dans des conditions permettant audit Etat Partie d'en établir l'authenticité. La ou les langues acceptables pour chaque Etat Partie sont notifiées au Secrétaire général de l'Organisation des Nations Unies au moment où ledit Etat Partie dépose ses instruments de ratification, d'acceptation ou d'approbation ou d'adhésion à la présente Convention. En cas d'urgence et si les Etats Parties en conviennent, les demandes peuvent être faites oralement, mais doivent être confirmées sans délai par écrit.
15. Une demande d'entraide judiciaire doit contenir les renseignements suivants:
(a) la désignation de l'autorité dont émane la demande;
(b) l'objet et la nature de l'enquête, des poursuites ou de la procédure judiciaire auxquelles se rapporte la demande, ainsi que le nom et les fonctions de l'autorité qui en est chargée;
(c) un résumé des faits pertinents, sauf pour les demandes adressées aux fins de la signification d'actes judiciaires;
(d) une description de l'assistance requise et le détail de toute procédure particulière que l'Etat Partie requérant souhaite voir appliquée;
(e) si possible, l'identité, l'adresse et la nationalité de toute personne visée; et
(f) le but dans lequel le témoignage, les informations ou les mesures sont demandées.
16. L'Etat Partie requis peut demander un complément d'information lorsque cela paraît nécessaire pour exécuter la demande conformément à son droit interne ou lorsque cela peut faciliter l'exécution de la demande.
[...]

Les paragraphes 13 à 16 de l'article 18 définissent la forme et le contenu des demandes, ainsi que les canaux de transmission. En ce qui concerne ces canaux, la Convention propose que les demandes soient transmises d'une autorité centrale à une autre.[2471] La Convention souligne l'importance de cette procédure pour

garantir une exécution rapide et en bonne et due forme de la demande. Les rôles des autorités centrales peuvent varier et aller de la participation directe au traitement et à l'exécution des demandes à leur transmission aux autorités compétentes. La Convention laisse la possibilité aux Etats d'exiger leur transmission par voie diplomatique. Cette dernière option étant longue, une telle procédure ralentirait drastiquement la transmission et représenterait un obstacle majeur aux mesures rapides comme celle de conservation des données relatives au trafic. Contrairement à la Convention du Conseil de l'Europe sur la cybercriminalité,[2472] la CTO ne définit pas les modalités d'une coopération rapide, mais propose une procédure générale en cas d'urgence. Si les Etats sont d'accord, l'Organisation internationale de police criminelle (Interpol) peut être utilisée comme canal de transmission. Afin de faciliter l'identification de l'autorité compétente dans un autre pays, l'Office des Nations Unies contre la drogue et le crime (ONUDC) conserve un répertoire en ligne.[2473] Celui-ci fournit à l'autorité d'émission les coordonnées de l'autorité centrale de l'Etat requis, les canaux de transmission ainsi que toute autre information pertinente. [2474]

Lors de la soumission de la demande, il convient de respecter les exigences formelles définies aux paragraphes 14 et 15. Les demandes orales ne sont autorisées qu'en cas d'urgence et doivent être suivies d'une requête écrite. Les rapports des Etats Parties sur l'application de la Convention montrent que, même si la législation de nombreux pays exige que les demandes d'entraide judiciaire soient faites par écrit, seule une poignée acceptent les demandes préalables temporaires envoyées par courriel.[2475] Sur ce point, la CTO diffère de la Convention du Conseil de l'Europe sur la cybercriminalité qui encourage les Etats à utiliser les moyens de communication électroniques en cas d'urgence.[2476] La CTO prévoit un logiciel pour la rédaction de telles requêtes dont le but est d'assurer qu'elles sont complètes (rédacteur de requêtes d'entraide judiciaire).[2477]

Article 18. Entraide judiciaire
[...]
17. Toute demande est exécutée conformément au droit interne de l'Etat Partie requis et, dans la mesure où cela ne contrevient pas au droit interne de l'Etat Partie requis et lorsque cela est possible, conformément aux procédures spécifiées dans la demande.
18. Lorsque cela est possible et conforme aux principes fondamentaux du droit interne, si une personne qui se trouve sur le territoire d'un Etat Partie doit être entendue comme témoin ou comme expert par les autorités judiciaires d'un autre Etat Partie, le premier Etat Partie peut, à la demande de l'autre, autoriser son audition par vidéoconférence s'il n'est pas possible ou souhaitable qu'elle comparaisse en personne sur le territoire de l'Etat Partie requérant. Les Etats Parties peuvent convenir que l'audition sera conduite par une autorité judiciaire de l'Etat Partie requérant et qu'une autorité judiciaire de l'Etat Partie requis y assistera.
19. L'Etat Partie requérant ne communique ni n'utilise les informations ou les éléments de preuve fournis par l'Etat Partie requis pour des enquêtes, poursuites ou procédures judiciaires autres que celles visées dans la demande sans le consentement préalable de l'Etat Partie requis. Rien dans le présent paragraphe n'empêche l'Etat Partie requérant de révéler, lors de la procédure, des informations ou des éléments de preuve à décharge. Dans ce dernier cas, l'Etat Partie requérant avise l'Etat Partie requis avant la révélation et, s'il lui en est fait la demande, consulte l'Etat Partie requis. Si, dans un cas exceptionnel, une notification préalable n'est pas possible, l'Etat Partie requérant informe sans retard l'Etat Partie requis de la révélation.
20. L'Etat Partie requérant peut exiger que l'Etat Partie requis garde le secret sur la demande et sa teneur, sauf dans la mesure nécessaire pour l'exécuter. Si l'Etat Partie requis ne peut satisfaire à cette exigence, il en informe sans délai l'Etat Partie requérant.
21. L'entraide judiciaire peut être refusée:
(a) si la demande n'est pas faite conformément aux dispositions du présent article;
(b) si l'Etat Partie requis estime que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels;
(c) au cas où le droit interne de l'Etat Partie requis interdirait à ses autorités de prendre les mesures demandées s'il s'agissait d'une infraction analogue ayant fait l'objet d'une enquête, de poursuites ou d'une procédure judiciaire dans le cadre de sa propre compétence;
(d) au cas où il serait contraire au système juridique de l'Etat Partie requis concernant l'entraide judiciaire d'accepter la demande.

22. Les Etats Parties ne peuvent refuser une demande d'entraide judiciaire au seul motif que l'infraction est considérée comme touchant aussi à des questions fiscales.
23. Tout refus d'entraide judiciaire doit être motivé.
24. L'Etat Partie requis exécute la demande d'entraide judiciaire aussi promptement que possible et tient compte dans toute la mesure possible de tous délais suggérés par l'Etat Partie requérant et qui sont motivés, de préférence dans la demande. L'Etat Partie requis répond aux demandes raisonnables de l'Etat Partie requérant concernant les progrès faits dans l'exécution de la demande. Quand l'entraide demandée n'est plus nécessaire, l'Etat Partie requérant en informe promptement l'Etat Partie requis.
25. L'entraide judiciaire peut être différée par l'Etat Partie requis au motif qu'elle entraverait une enquête, des poursuites ou une procédure judiciaire en cours.
26. Avant de refuser une demande en vertu du paragraphe 21 du présent article ou d'en différer l'exécution en vertu de son paragraphe 25, l'Etat Partie requis étudie avec l'Etat Partie requérant la possibilité d'accorder l'entraide sous réserve des conditions qu'il juge nécessaires. Si l'Etat Partie requérant accepte l'entraide sous réserve de ces conditions, il se conforme à ces dernières.
27. Sans préjudice de l'application du paragraphe 12 du présent article, un témoin, un expert ou une autre personne qui, à la demande de l'Etat Partie requérant, consent à déposer au cours d'une procédure ou à collaborer à une enquête, à des poursuites ou à une procédure judiciaire sur le territoire de l'Etat Partie requérant ne sera pas poursuivi, détenu, puni ou soumis à d'autres restrictions à sa liberté personnelle sur ce territoire à raison d'actes, d'omissions ou de condamnations antérieurs à son départ du territoire de l'Etat Partie requis. Cette immunité cesse lorsque le témoin, l'expert ou ladite personne ayant eu, pour une période de quinze jours consécutifs ou pour toute autre période convenue par les Etats Parties, à compter de la date de laquelle ils ont été officiellement informés que leur présence n'était plus requise par les autorités judiciaires, la possibilité de quitter le territoire de l'Etat Partie requérant, y sont néanmoins demeurés volontairement ou, l'ayant quitté, y sont revenus de leur plein gré.
28. Les frais ordinaires encourus pour exécuter une demande sont à la charge de l'Etat Partie requis, à moins qu'il n'en soit convenu autrement entre les Etats Parties concernés. Lorsque des dépenses importantes ou extraordinaires sont ou se révèlent ultérieurement nécessaires pour exécuter la demande, les Etats Parties se consultent pour fixer les conditions selon lesquelles la demande sera exécutée, ainsi que la manière dont les frais seront assumés.
29. L'Etat Partie requis:
(a) fournit à l'Etat Partie requérant copies des dossiers, documents ou renseignements administratifs en sa possession et auxquels, en vertu de son droit interne, le public a accès;
(b) peut, à son gré, fournir à l'Etat Partie requérant intégralement, en partie ou aux conditions qu'il estime appropriées, copies de tous dossiers, documents ou renseignements administratifs en sa possession et auxquels, en vertu de son droit interne, le public n'a pas accès.
30. Les Etats Parties envisagent, s'il y a lieu, la possibilité de conclure des accords ou des arrangements bilatéraux ou multilatéraux qui servent les objectifs et les dispositions du présent article, leur donnent un effet pratique ou les renforcent.

6.6.5 Convention du Conseil de l'Europe sur la cybercriminalité

La Convention du Conseil de l'Europe sur la cybercriminalité (ci-après la « Convention sur la cybercriminalité ») aborde l'importance croissante de la coopération internationale à ses articles 23 à 35.

Principes généraux relatifs à la coopération internationale

L'article 23 de la Convention du Conseil de l'Europe sur la cybercriminalité pose trois grands principes en matière de coopération internationale entre ses membres dans le cadre d'enquêtes cybercriminelles.

Article 23 – Principes généraux relatifs à la coopération internationale
Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Tout d'abord, les membres sont supposés coopérer le plus largement possible aux investigations internationales. Cette obligation reflète l'importance de la coopération internationale dans les enquêtes cybercriminelles. De plus, l'article 23 note que ces principes généraux ne s'appliquent pas uniquement aux enquêtes cybercriminelles, mais à toute enquête où des preuves sous format électronique doivent être collectées. Cela couvre les investigations cybercriminelles, mais aussi traditionnelles. Si un suspect dans une affaire de meurtre a utilisé un service de messagerie à l'étranger, l'article 23 s'appliquerait aux enquêtes nécessaires sur les données stockées par l'hébergeur.[2478] Le troisième principe veut que les dispositions relatives à la coopération internationale ne remplacent pas les dispositions des accords internationaux d'entraide judiciaire ou d'extradition ou les dispositions pertinentes du droit national en matière de coopération internationale. Les auteurs de la Convention sur la cybercriminalité ont souligné que l'entraide doit en général se concrétiser par l'application des traités pertinents et autres accords de ce type sur l'entraide judiciaire. Par conséquent, la Convention sur la cybercriminalité ne vise pas à créer un régime général séparé d'entraide judiciaire. C'est pourquoi, dans les seuls cas où les traités, lois et arrangements existants ne contiennent pas déjà de dispositions en ce sens, chaque partie doit établir une base juridique lui permettant de participer à la coopération internationale telle que définie par la Convention sur la cybercriminalité.[2479]

Extradition

L'extradition de ressortissants d'autres pays reste l'un des aspects les plus difficiles de la coopération internationale.[2480] Les demandes d'extradition entraînent très souvent des conflits entre la nécessité de protéger le citoyen et celle de soutenir une enquête en cours dans un autre pays. L'article 24 définit les principes de l'extradition. Contrairement à l'article 23, ses dispositions sont limitées aux délits mentionnés dans la Convention sur la cybercriminalité et ne s'appliquent pas si ceux-ci sont mineurs (punissables d'une privation de liberté pour une période maximale d'au moins un an[2481]). Afin d'éviter les conflits liés à la capacité des parties à émettre des réserves, l'article 24 repose sur le principe de la double incrimination.[2482]

Article 24 – Extradition
1a. Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.
b. Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.
2. Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.
3. Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4. Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.
5. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.
6. Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.
7a. Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.
b. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Principes généraux relatifs à l'entraide

En ce qui concerne l'entraide, l'article 25 vient compléter les principes établis à l'article 23. L'une des règles les plus importantes de l'article 25 est celle du paragraphe 3 qui souligne l'importance d'échanges rapides dans le cadre des enquêtes cybercriminelles.[2483] Comme nous l'avons déjà rappelé, plusieurs enquêtes de ce type, conduites au niveau national, échouent parce que les investigations prennent trop de temps et que des données importantes sont alors effacées avant que les mesures procédurales permettant de les conserver ne soient prises.[2484] Les enquêtes exigeant une entraide judiciaire durent d'habitude encore plus longtemps en raison des exigences formelles s'appliquant à la communication entre forces de l'ordre, très prenantes. La Convention sur la cybercriminalité aborde ce problème en soulignant l'importance associée à l'utilisation de moyens rapides de communication.[2485]

Article 25 – Principes généraux relatifs à l'entraide
1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.
2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.
3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.
4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.
5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Au cours d'enquêtes cybercriminelles menées au niveau national, des liens avec des délits liés à un autre pays peuvent être découverts. Si les forces de l'ordre, par exemple, enquêtent sur une affaire de pédopornographie, elles peuvent trouver des informations sur des pédophiles d'autres pays ayant participé à l'échange de contenus pédopornographiques.[2486] L'article 26 fixe les règles nécessaires à l'information par les forces de l'ordre des autorités étrangères sans mettre en danger leur propre enquête. [2487]

Article 26** – **Information spontanée
1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.
2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Comme nous l'avons mentionné plus haut, le remplacement de l'entraide judiciaire par un échange spontané d'informations suscite certaines craintes. Le partage d'informations ne peut fonctionner que si l'Etat destinataire est capable de collecter toutes les preuves pertinentes de son côté. Dans tous les autres cas, une coopération formelle est normalement requise afin de protéger la chaîne de possession. Dans le cadre du débat sur la coopération internationale et le passage des requêtes formelles vers un partage spontané d'informations, il est important de garder à l'esprit que le processus formel a été développé pour protéger l'intégrité des nations ainsi que les droits de l'inculpé. Le partage d'informations ne doit donc pas permettre de contourner le dogme de l'entraide judiciaire.

L'une des dispositions les plus importantes de l'article 26 est liée à la confidentialité des informations. Etant donné que nombre d'investigations ne peuvent être conduites avec succès que si le contrevenant n'en a pas connaissance, l'article 26 permet à l'Etat fournisseur d'exiger la confidentialité des informations transmises. Si celle-ci ne peut être garantie, cette partie peut refuser l'échange.

Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Comme l'article 25, l'article 27 repose sur l'idée que l'entraide judiciaire doit se faire par le biais de l'application des traités pertinents et autres arrangements similaires plutôt qu'en invoquant simplement la Convention sur la cybercriminalité. Les auteurs de ce texte ont décidé de ne pas établir de régime d'entraide judiciaire séparé obligatoire dans le cadre de la Convention sur la cybercriminalité. [2488] Si d'autres instruments existent déjà, les articles 27 et 28 ne s'appliquent pas à une requête concrète. Ce n'est que dans les cas où d'autres règles ne s'appliquent pas que les articles 27 et 28 proposent un ensemble de mécanismes pouvant être utilisés pour exécuter les demandes d'entraide judiciaire.

Les questions les plus importantes réglementées par l'article 27 incluent l'obligation d'établir un point de contact désigné pour le traitement des demandes d'entraide judiciaire,[2489] une exigence de communication directe entre les points de contact dans le but d'éviter des procédures excessivement longues[2490] et la création d'une base de données de tous les points de contact par le Secrétaire général du Conseil de l'Europe.

De plus, l'article 27 définit des limites aux demandes d'entraide. Les Parties à la Convention sur la cybercriminalité peuvent notamment refuser de coopérer sur des délits politiques ou si elles considèrent que cette coopération peut porter atteinte à leur souveraineté, leur sécurité, leur ordre public ou d'autres intérêts essentiels.

Les auteurs de la Convention sur la cybercriminalité ont compris le besoin, d'un côté, de permettre aux parties de refuser de coopérer dans certains cas, tout en soulignant, de l'autre, qu'elles doivent exercer ce refus de coopérer avec retenue de façon à éviter les conflits avec les principes énoncés précédemment.[2491]

Il est donc particulièrement important de définir de façon restrictive le terme « autres intérêts essentiels ». Le rapport explicatif à la Convention sur la cybercriminalité souligne que cela pourrait être le cas si la coopération entraîne des difficultés importantes pour l'Etat Partie requis.[2492] Du point de vue des auteurs, les craintes liées à des lois inadaptées sur la protection des données ne sont pas considérées comme relevant des intérêts essentiels.[2493]

Entraide en matière de mesures provisoires

Les articles 28 à 33 reflètent les instruments de procédure de la Convention sur la cybercriminalité.[2494] Celle-ci contient plusieurs instruments de ce type, conçus pour améliorer les investigations au sein des Etats membres.[2495] En ce qui concerne le principe de souveraineté nationale,[2496] l'utilisation de ces instruments est limitée aux enquêtes menées au niveau national.[2497] Si les enquêteurs s'aperçoivent que des preuves doivent être collectées hors de leur territoire, ils doivent formuler une demande d'entraide judiciaire. Outre l'article 18, chacun des instruments établis par les articles 16 à 21 est associé à une disposition particulière des articles 28 à 33 qui permet aux forces de l'ordre d'appliquer les instruments de procédure à la demande d'une autorité répressive étrangère.

Instrument procédural	Disposition particulière correspondante
Article 16 – Conservation rapide de données informatiques stockées [2498]	Article 29
Article 17 – Conservation et divulgation rapides de données relatives au trafic[2499]	Article 30
Article 18 – Injonction de produire [2500]	Aucune
Article 19 – Perquisition et saisie de données informatiques stockées [2501]	Article 31
Article 20 – Collecte en temps réel des données relatives au trafic [2502]	Article 33
Article 21 – Interception de données relatives au contenu [2503]	Article 34

Accès transfrontière à des données stockées

En plus de refléter ces dispositions de procédure, les auteurs de la Convention sur la cybercriminalité se sont demandé dans quelles circonstances les forces de l'ordre pouvaient avoir accès aux données informatiques qui ne sont ni stockées sur leur territoire, ni placées sous le contrôle d'un individu sur leur territoire. Ils n'ont pu s'accorder que sur deux scénarios où une enquête doit être menée par une autorité répressive sans demande d'entraide judiciaire.[2504] Il n'a pas été possible de pousser plus loin l'accord[2505] et la solution atteinte reste encore aujourd'hui critiquée par plusieurs Etats membres du Conseil de l'Europe.[2506]

Les deux cas de figure où les forces de l'ordre peuvent accéder à des données stockées hors de leur territoire sont les suivants:

- lorsqu'il s'agit d'informations publiques; et/ou
- lorsque l'accès se fait avec le consentement de la personne chargée du contrôle des données.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie:

a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Les autres formes d'accès transfrontalier ne sont pas couvertes par l'article 32, mais n'en sont pas non plus exclues. [2507]

L'article 32 rappelle que si des données pertinentes sont publiques, les forces de l'ordre sont autorisées à y accéder. A titre d'exemple, citons les informations publiées sur des sites Internet sans contrôle d'accès (par mot de passe). Si les enquêteurs n'étaient pas autorisés, contrairement à tout autre utilisateur, à accéder à ces sites, cela pourrait gravement entraver leurs travaux. C'est pourquoi ce cas de figure, traité à l'article 32, est largement accepté.

La seconde situation est celle où les forces de l'ordre sont autorisées à accéder à des données informatiques stockées hors de leur territoire. Cela n'est possible que si les enquêteurs ont obtenu le consentement légitime et volontaire de la personne ayant légalement la compétence de divulguer ces données. Cette autorisation fait l'objet de vives critiques.[2508]

L'une des principales inquiétudes est liée au fait que cette disposition, dans sa formulation actuelle, est probablement en contradiction avec les principes fondamentaux du droit international.[2509] Sur cette base, les enquêteurs doivent respecter la souveraineté nationale lors de leurs investigations. [2510] Ils ne sont notamment pas autorisés à mener leur enquête dans un autre pays sans le consentement des autorités compétentes de ce territoire. La décision d'accorder cette autorisation n'incombe pas à un individu, mais aux autorités de l'Etat, puisque l'interférence avec la souveraineté nationale affecte non seulement les droits des individus, mais aussi les préoccupations des Etats. En ratifiant la Convention sur la cybercriminalité, les pays rejettent en partie ce principe en permettant à d'autres de mener des investigations affectant leur territoire.

Une autre crainte est liée au fait que l'article 32 b ne définit pas les procédures d'enquête. Selon ses dispositions, il n'est pas nécessaire d'appliquer les mêmes restrictions que celles existant en droit national pour les enquêtes nationales comparables. Autre détail intéressant, une telle limitation était prévue dans le projet de Convention sur la cybercriminalité présenté au début de l'an 2000, avant d'être retiré de la 22^{e} mouture du texte. [2511]

En rédigeant l'article 32.b, les auteurs de la Convention sur la cybercriminalité vont purement et simplement à l'encontre du dogme de l'entraide judiciaire de la Convention. Avec l'article 18, les auteurs de la Convention sur la cybercriminalité avaient permis aux enquêteurs d'ordonner la présentation de données dans le cadre d'enquêtes nationales. Si les forces de l'ordre étaient autorisées à utiliser un tel instrument dans le cadre d'enquêtes internationales, il suffirait de l'inclure au catalogue des instruments mentionné en lien avec l'entraide judiciaire. Cependant, cet instrument ne peut être appliqué dans des enquêtes internationales parce que la disposition correspondante du chapitre 3 de la Convention sur la cybercriminalité, consacré à la coopération internationale, est absente. Au lieu de renoncer au dogme de l'entraide judiciaire en autorisant les enquêteurs étrangers à contacter directement la personne contrôlant les données recherchées pour lui en demander la soumission, les auteurs auraient pu se contenter d'inscrire une disposition en ce sens au chapitre 3 de la Convention. [2512]

L'accès transfrontalier aux données informatiques stockées a également été abordé lors de la Conférence ministérielle du G8 de 1999 à Moscou, consacrée à la lutte contre la criminalité transnationale organisée.[2513] L'une des conclusions de cette réunion a été la compilation des principes relatifs à l'accès transfrontalier.[2514] Celle-ci a, selon toute vraisemblance, servi de modèle aux règles instaurées par les auteurs de la Convention sur la cybercriminalité, d'où les similarités.

6. Accès transfrontalier aux données stockées n'exigeant pas d'entraide judiciaire
Nonobstant toute disposition contraire reprise dans les présents principes, un Etat n'a pas besoin d'obtenir l'autorisation d'un autre lorsqu'il agit en conformité avec son droit national dans le but de:

(a) accéder à des données publiques (sources ouvertes), quel que soit l'emplacement géographique de ces données;

(b) accéder, rechercher, copier ou saisir des données stockées dans un système informatique situé dans un autre Etat, s'il bénéficie du consentement légitime et volontaire de la personne ayant la compétence légale de lui divulguer ces données. L'Etat enquêteur doit envisager de notifier l'Etat où ces recherches ont lieu, si une telle notification est autorisée par son droit national et que les données révèlent une violation du droit pénal ou présentent autrement un intérêt pour ce dernier.

La principale différence réside dans la procédure de notification prévue à l'alinéa 6 (b). L'intention de cette disposition est de promouvoir l'échange de renseignements. Toutefois, légèrement modifiée, elle pourrait garantir que les Etats affectés soient tenus au courant des enquêtes en cours sur leur propre territoire. Cela n'empêcherait pas le conflit avec le droit international, mais garantirait au moins un certain degré de transparence.

Réseau de contacts 24/7

Les enquêtes cybercriminelles exigent souvent des réactions immédiates.[2515] Comme nous l'avons expliqué plus haut, c'est particulièrement vrai lorsqu'il s'agit de données relatives au trafic, nécessaires à l'identification d'un suspect. En effet, celles-ci sont souvent effacées assez rapidement.[2516] Afin d'accroître le rythme des enquêtes internationales, la Convention sur la cybercriminalité souligne, à l'article 25, l'importance d'autoriser l'utilisation de moyens rapides de communication. Pour améliorer encore l'efficacité des demandes d'entraide judiciaire, les auteurs de la Convention sur la cybercriminalité obligent les parties à nommer un point de contact chargé de traiter ces requêtes et qui devra être disponible à tout moment.[2517] Les auteurs de la Convention sur la cybercriminalité ont rappelé que la création de ces points de contact est l'un des instruments les plus importants prévus par la Convention.[2518] Toutefois, un récent état des lieux de l'utilisation de ce réseau, disponible 24h/24 et 7j/7, montre qu'il est très peu utilisé dans les pays ayant ratifié la Convention sur la cybercriminalité.

Article 35 – Réseau 24/7
1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:
a. apport de conseils techniques;
b. conservation des données, conformément aux articles 29 et 30;
c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.
2a. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.
b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.
3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

L'idée d'un réseau accessible 24h/24 et 7j/7 est née du réseau existant de contact permanent pour la criminalité internationale liée à la haute technologie et à l'informatique du groupe de pays formant le G8.[2519] En demandant la création d'un réseau des points de contact, disponibles 24h/24 et 7j/7, les auteurs de la Convention sur la cybercriminalité souhaitaient répondre aux défis de la lutte contre ce phénomène, et en particulier ceux liés à la vitesse des échanges de données[2520] ayant une dimension internationale.[2521] Les parties à la Convention sur la cybercriminalité sont obligées d'établir un point de contact et de veiller à ce qu'il puisse agir immédiatement, dans certaines circonstances. Elles doivent également en assurer le service. Comme le rappelle le paragraphe 3 de l'article 34 de la Convention, cela inclut la mise à disposition d'un personnel formé et équipé.

En ce qui concerne le processus de création du point de contact et, plus particulièrement, les principes fondamentaux sous-tendant cette structure, la Convention sur la cybercriminalité donne la plus grande souplesse aux Etats membres. La Convention n'exige pas la création d'une nouvelle autorité et ne précise pas non plus auxquelles des autorités existantes le point de contact peut ou doit être rattaché. Les auteurs de la Convention sur la cybercriminalité ont de plus signalé que le fait que le réseau disponible 24h/24 et 7j/7 doive apporter une aide technique autant que juridique entraînera l'apparition de plusieurs solutions de mise en œuvre.

En ce qui concerne les enquêtes cybercriminelles, la création des points de contact a deux fonctions principales: accélérer la communication en instaurant un point de contact unique et accélérer l'enquête en autorisant celui-ci à mener certaines investigations sans attendre. L'association de ces deux fonctions a le potentiel d'accroître le rythme des enquêtes internationales pour atteindre celui des enquêtes nationales.

L'article 32 de la Convention sur la cybercriminalité définit les compétences minimales exigées du point de contact. Outre l'assistance technique et la fourniture d'informations juridiques, les principales fonctions du point de contact incluent la conservation de données, la collecte de preuves et la localisation des suspects.

Dans ce contexte, il est de nouveau important de rappeler que la Convention ne prescrit pas quelle autorité doit être chargée de faire fonctionner le point de contact 24h/24, 7j/7. Si le point de contact est géré par une autorité ayant les compétences pour conserver les données[2522] et qu'un point de contact étranger demande cette conservation, la mesure peut être immédiatement ordonnée par le point de contact local. Dans le cas contraire, il est important que le point de contact puisse immédiatement contacter les autorités compétentes de façon à garantir que la mesure est exécutée sans délai.[2523]

Lors de la 2e réunion du Comité de la Convention sur la cybercriminalité, il a été explicitement rappelé que la participation au réseau des points de contact disponibles 24h/24 et 7j/7 n'exige ni la signature, ni la ratification de la Convention sur la cybercriminalité.[2524]

En 2008, le Conseil de l'Europe a publié une étude analysant l'efficacité de la coopération internationale dans la lutte contre la cybercriminalité. [2525] En 2009, une étude spécifique a été menée sur le fonctionnement des points de contact pour la cybercriminalité, disponibles 24h/24 et 7j/7.[2526] L'une de ses conclusions est que tous les pays ayant créé des points de contact opérationnels, disponibles 24h/24 et 7j/7, exigence de la Convention, ne l'ont pas nécessairement ratifiée. Une autre conclusion est que, souvent, les pays ayant établi des points de contact ne les utilisent qu'à des fins très limitées, comme la conservation des données relatives au trafic.

6.6.6 La coopération internationale dans le projet de Convention internationale de Stanford

Les auteurs du Projet de Convention internationale de Stanford (le « Projet de Stanford »)[2527] reconnaissent l'importance de la dimension internationale de la cybercriminalité et des défis qui y sont associés. Afin de les relever, ils ont intégré au texte des dispositions spécifiques traitant de la coopération internationale. Celles-ci couvrent les sujets suivants.

- Article 6 – Entraide juridique
- Article 7 – Extradition
- Article 8 – Poursuite
- Article 9 – Mesures conservatoires
- Article 10 – Droits des personnes accusées
- Article 11 – Coopération dans l'application de la loi

Cette approche fait apparaître plusieurs similarités avec celle adoptée par la Convention du Conseil de l'Europe sur la cybercriminalité. La principale différence réside dans le fait que les règles prévues par la Convention sur la cybercriminalité sont plus strictes, plus complexes et mieux définies que celles du Projet de Stanford. Comme l'ont signalé les auteurs de ce texte, l'approche de la Convention sur la cybercriminalité est plus pratique et présente donc certains avantages clairs en termes d'application concrète.[2528] Les

auteurs du Projet de Stanford ont décidé de suivre une approche différente, prévoyant que l'application des nouvelles technologies pourrait entraîner certaines difficultés. En conséquence, ils n'ont proposé que des instructions générales sans les détailler.[2529]

6.7 Responsabilité des fournisseurs d'accès Internet

Bibliography (selected): *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Luotonen*, Web Proxy Servers, 1997; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.7.1 Introduction

La perpétration d'un délit informatique implique automatiquement plusieurs personnes et entreprises, même si le criminel a agi seul. Etant donné la structure de l'Internet, la simple transmission d'un courriel exige l'intervention de plusieurs prestataires de services.[2530] Outre le fournisseur de messagerie, cet envoi associe des fournisseurs d'accès ainsi que des routeurs qui font suivre le courriel à son destinataire. La situation est similaire pour le téléchargement de films à caractère pédopornographique. Le processus de téléchargement implique le fournisseur de contenus qui a mis à disposition ces images (par exemple sur un site Internet), l'hébergeur qui a fourni le support de stockage du site, les routeurs qui ont fait suivre les fichiers à l'utilisateur et enfin le fournisseur d'accès qui a permis à l'internaute de se connecter.

En raison de l'implication de nombreuses parties, les fournisseurs d'accès à Internet sont depuis longtemps au cœur des enquêtes criminelles sur les contrevenants ayant utilisé les services des FAI pour commettre leur délit.[2531] L'une des principales raisons en est que, même si le criminel agit depuis l'étranger, les fournisseurs situés sur le territoire national peuvent faire l'objet d'une enquête pénale sans que le principe de souveraineté nationale ne soit violé.[2532]

Le fait que, d'un côté, un délit informatique ne puisse être commis sans la participation des fournisseurs et que, de l'autre, ceux-ci ne sont souvent pas en mesure de prévenir ces infractions, a suscité une interrogation: doit-on limiter la responsabilité des fournisseurs d'accès à Internet ?[2533] La réponse à cette question est essentielle au développement économique des infrastructures des TIC. Les fournisseurs ne proposeront leurs services que s'ils peuvent éviter la criminalisation de leurs activités régulières. De plus, les forces de l'ordre ont elles aussi un vif intérêt pour cette question. Leur travail dépend très souvent de la coopération des fournisseurs d'accès à Internet. Cela pose problème puisque limiter la responsabilité des FAI pour des actes commis par leurs clients pourrait avoir un impact sur leur volonté de coopérer et de soutenir les enquêtes cybercriminelles ainsi que les efforts concrets de prévention du crime.

6.7.2 L'approche des États-Unis

Plusieurs approches sont suivies pour arriver à un équilibre entre, d'un côté, la nécessité de faire activement participer les fournisseurs aux enquêtes et, de l'autre, de limiter les risques d'actions en responsabilité pénale pour les parties tierces.[2534] Dans cet esprit, citons, à titre d'exemple, l'approche législative adoptée par la section 17 du Code des Etats-Unis (USC) à l'article 517 (a) et (b).

§ 512. Limitations de la responsabilité concernant le matériel en ligne
(a) Communications en transit sur un réseau numérique
Un prestataire de services n'est pas responsable de la réparation pécuniaire, ou, sauf disposition de la sous-section (j), de mesure injonctive ou autre redressement équitable, pour violation de droits d'auteur du fait qu'un prestataire de services transmette, achemine ou fournisse des connexions pour du matériel par un système ou un réseau contrôlé ou exploité par ou pour le prestataire de services, ou du fait du stockage intermédiaire et transitoire de ce matériel pendant de telles activités de transmission, d'acheminement ou de connexion, si –

(1) la transmission du matériel a été déclenchée sur l'ordre d'une personne autre que le prestataire de services;
(2) la transmission, l'acheminement, la connexion ou le stockage sont effectués par le biais d'un processus technique automatique sans sélection du matériel par le prestataire de services;
(3) le prestataire de services ne sélectionne pas les destinataires du matériel sauf en cas de réponse automatique à la demande d'une autre personne;
(4) aucune copie du matériel faite par le prestataire de services pendant le stockage intermédiaire ou transitoire n'est conservée dans le système ou le réseau d'une manière facilement accessible à d'autres personnes que les destinataires supposés et aucune copie n'est conservée sur le système ou le réseau d'une manière facilement accessible au destinataire désigné pendant une période plus longue qu'il n'est raisonnablement nécessaire pour la transmission, l'acheminement ou les connexions; et
(5) le matériel est transmis via le système de réseau sans modification de son contenu.

(b) Système « caching » (antémémoire)
(1) limitation de la responsabilité – un prestataire de services n'est pas responsable de la réparation pécuniaire, ou, sauf disposition de la sous-section (j), de mesure injonctive ou autre redressement équitable, pour violation de droit d'auteur du fait du stockage intermédiaire et provisoire du matériel sur un système ou un réseau contrôlé ou exploité par ou pour le prestataire de services dans le cas où –

(A) le matériel est mis en ligne, à la disposition d'une personne autre que le prestataire de services;
(B) le matériel est transmis de la personne décrite au sous-paragraphe (A) par le biais du système ou du réseau vers une personne autre que la personne décrite au sous-paragraphe (A) ou sur l'ordre de cette autre personne; et
(C) le stockage est exécuté par un processus technique automatique afin que le matériel soit à la disposition des utilisateurs du système ou du réseau qui, après transmission du matériel comme indiqué au sous-paragraphe (B), demandent l'accès au matériel à la personne décrite au sous-paragraphe (A), si les conditions exposées au paragraphe (2) sont satisfaites.

[…]

Cette disposition repose sur la loi américaine sur le droit d'auteur à l'ère du numérique (*Digital Millennium Copyright Act* ou DMCA), promulguée en 1998.[2535] En créant un régime de sphère de sécurité (*safe harbour*), la DMCA exclut de son champ d'application la responsabilité des fournisseurs pour certains services en cas de violation du droit d'auteur par des tiers.[2536] Dans ce contexte, il importe tout d'abord de souligner que tous les fournisseurs ne sont pas couverts par cette limitation.[2537] La limitation de responsabilité ne s'applique qu'aux prestataires de services[2538] et aux fournisseurs de mémoire cache.[2539] De plus, il faut souligner que la responsabilité est liée à certaines exigences. En ce qui concerne les fournisseurs de services, celles-ci sont les suivantes:

- la transmission du matériel doit avoir été faite à l'initiative ou sur les instructions d'une personne autre que le fournisseur de services;

- la transmission s'est déroulée selon un processus technique automatique sans sélection du matériel par le fournisseur de services;
- le fournisseur de services n'a pas sélectionné les destinataires du matériel;
- aucune copie du matériel effectuée par le fournisseur de services pendant le stockage intermédiaire ou temporaire n'a été conservée sur son système ou réseau de façon à être facilement accessible aux personnes autres que les destinataires visés.

On peut trouver un autre exemple de la limitation de la responsabilité des fournisseurs d'accès à Internet à la section 47 de l'USC, article 230 (c), qui repose sur la loi américaine sur la décence dans le domaine des télécommunications (C*ommunications Decency Act*).[2540]

§ 230. Protection contre le blocage et la sélection privée de matériels portant atteinte aux bonnes mœurs
[…]
(c) Protection contre le blocage et la sélection de matériels portant atteinte aux bonnes moeurs selon la clause du « Bon Samaritain »
(1) Traitement de l'éditeur ou du locuteur
Aucun fournisseur ou utilisateur d'un service informatique interactif ne sera traité comme éditeur ou locuteur de toute information fournie par un autre fournisseur de contenus informatifs.
(2) Responsabilité civile
Aucun fournisseur ou utilisateur d'un service informatique interactif ne sera tenu pour responsable au titre de –
(A) toute action exécutée volontairement, en toute bonne foi, visant à restreindre l'accès ou la disponibilité de matériel que le fournisseur ou l'utilisateur juge obscène, libertin, lubrique, sale, excessivement violent, malveillant ou autrement inadmissible, que ce matériel soit ou non protégé constitutionnellement; ou
(B) toute action exécutée pour permettre ou mettre à la disposition de fournisseurs de contenus informatifs ou autres les moyens techniques pour restreindre l'accès au matériel décrit au paragraphe (1).
[…]

Ces deux approches (section 17 de l'USC, article 512 (a) et section 47 de l'USC, article 230 (c)) ont en commun de se concentrer sur la responsabilité de groupes spéciaux de fournisseurs et sur des domaines particuliers du droit. Le reste de ce chapitre donnera donc un aperçu de l'approche législative plus large, adoptée par l'Union européenne.

6.7.3 Directive de l'Union européenne relative au commerce électronique

La directive relative au commerce électronique de l'Union européenne[2541] est un exemple d'approche législative visant à réglementer la responsabilité des fournisseurs d'accès à Internet. Confrontés aux défis découlant de la dimension internationale de la Toile, les auteurs de la directive ont décidé de développer des normes juridiques fournissant un cadre légal pour le développement global de la société de l'information et soutenant le développement de l'économie en général ainsi que les efforts des forces de l'ordre.[2542] Cette réglementation sur la responsabilité est basée sur le principe de la responsabilité progressive.

La directive contient plusieurs dispositions limitant la responsabilité de certains fournisseurs.[2543] Ces limitations sont liées aux différentes catégories de services proposés.[2544] Dans tous les autres cas, la responsabilité n'est pas nécessairement exclue et l'acteur peut voir sa responsabilité pleinement engagée si celle-ci n'est pas limitée par d'autres dispositions. Le but de la directive est de limiter la responsabilité aux cas où le fournisseur n'a que des possibilités limités de prévenir le délit. Les raisons peuvent en être techniques. Ainsi, les routeurs ne peuvent pas filtrer les données passant par eux, à moins d'une perte significative de vitesse, et peuvent difficilement éviter les échanges de données. Les hébergeurs sont en mesure de supprimer des données s'ils ont connaissance d'activités criminelles. Cependant, comme les routeurs, les grands hébergeurs sont incapables de contrôler l'ensemble des données stockées sur leurs serveurs.

En ce qui concerne les différentes capacités de contrôle réel des activités criminelles, la responsabilité des hébergeurs et des fournisseurs d'accès n'est pas du tout la même. Sur cette question, il ne faut pas oublier que l'équilibre de la directive repose sur les normes techniques actuelles. Aujourd'hui, il n'existe aucun outil permettant de détecter automatiquement des images pornographiques inconnues. Mais, si la technologie continue d'évoluer, il pourrait s'avérer nécessaire d'évaluer les capacités techniques des fournisseurs à l'avenir et, si besoin, d'ajuster le système.

6.7.4 Responsabilité du fournisseur d'accès (Directive de l'Union européenne sur le commerce électronique)

Les articles 12 à 15 définissent le degré de limitation de la responsabilité des différents fournisseurs. Sur la base de l'article 12, la responsabilité des fournisseurs d'accès et des opérateurs de routeurs est complètement exclue, tant qu'ils respectent les trois conditions stipulées dans cet article. Par conséquent, le fournisseur d'accès n'est, en général, pas tenu responsable des infractions pénales commises par ses clients. La pleine exclusion de toute responsabilité ne délivre pas le fournisseur de l'obligation de prévenir de nouveaux délits s'il a reçu une injonction d'un tribunal ou d'une autorité administrative en ce sens.[2545]

Section 4: Responsabilité des prestataires intermédiaires
Article 12 *– Simple transport (« Mere conduit »)*
1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire:
a) ne soit pas à l'origine de la transmission;
b) ne sélectionne pas le destinataire de la transmission; et
c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.
2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.
3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation.

Cette approche est comparable à celle de la section 17 de l'USC, article 517 (a).[2546] Ces réglementations visent toutes deux à préciser la responsabilité des fournisseurs d'accès en liant sa limitation à des exigences similaires. La principale différence réside dans le fait que l'application de l'article 12 de la directive de l'UE sur le commerce électronique ne se limite pas aux violations du droit d'auteur, mais exclut toute responsabilité en cas de délit.

6.7.5 Responsabilité liée au stockage, « Caching » (Directive de l'Union européenne sur le commerce électronique)

Dans ce contexte, le terme de « caching » est utilisé pour décrire le stockage de sites Internet populaires sur un support local dans le but de réduire la bande passante et de faciliter l'accès aux données.[2547] L'une des techniques utilisées pour réduire la bande passante est l'installation de serveurs mandataires (*proxy*).[2548] Ici, un serveur proxy peut traiter des requêtes sans contacter le serveur spécifié (c'est-à-dire le nom de domaine tapé par l'utilisateur) en récupérant le contenu sauvegardé sur le support de stockage local lors d'une précédente requête. Les auteurs de la directive ont reconnu l'importance du caching et décidé d'exclure la responsabilité associée au stockage temporaire automatique à condition que le fournisseur remplisse les conditions énoncées à l'article 13. L'une d'entre elles est qu'il respecte les normes largement reconnues en matière de mise à jour des informations.

Article 13 – Forme de stockage dite « caching »
1. Les États membre veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que:

a) le prestataire ne modifie pas l'information;

b) le prestataire se conforme aux conditions d'accès à l'information;

c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises;

d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information; et

e) le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible.

2. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation.

L'article 13 de la directive de l'Union européenne sur le commerce électronique est un autre exemple des similarités existant entre les approches dogmatiques américaine et européenne. L'approche de l'UE est comparable à celle de la section 17 de l'USC, article 512 (b).[2549] Ces réglementations visent toutes deux à préciser la responsabilité des fournisseurs de cache en liant leur limitation à des exigences similaires. En ce qui concerne la responsabilité des fournisseurs de services,[2550] la principale différence entre ces deux approches réside dans le fait que l'application de l'article 13 de la directive de l'UE sur le commerce électronique ne se limite pas aux violations du droit d'auteur, mais exclut toute responsabilité en cas de délit.

6.7.6 Responsabilité de l'hébergeur (Directive de l'Union européenne sur le commerce électronique)

En ce qui concerne les contenus illicites, l'hébergeur joue un rôle particulièrement important lors de la perpétration du délit. Les criminels qui mettent en ligne des contenus illégaux ne les stockent en général pas sur leurs propres serveurs. La plupart des sites Internet sont stockés sur des serveurs mis à disposition par des hébergeurs. Quiconque souhaite exploiter un site Internet peut louer des capacités de mémoire auprès d'un hébergeur afin d'y stocker sa page. Certains fournisseurs proposent même de l'espace web gratuit, moyennant le placement de publicités.[2551]

L'identification de contenus illicites est un défi pour l'hébergeur. Pour les fournisseurs les plus populaires qui gèrent de nombreux sites, des recherches manuelles de contenu illicite sur un aussi grand nombre de pages serait mission impossible. Par conséquent, les auteurs de la directive ont décidé de limiter la responsabilité des hébergeurs. Toutefois, contrairement aux fournisseurs d'accès, la responsabilité des hébergeurs n'est pas toujours exclue. Tant que l'hébergeur n'a pas connaissance d'activités illégales ou de contenu illicite stocké sur ses serveurs, sa responsabilité n'est pas engagée. Dans ce contexte, l'hypothèse selon laquelle du contenu illicite peut être stocké sur un serveur n'équivaut pas à en avoir connaissance. Si le fournisseur apprend que des activités illégales sont conduites ou que des contenus illicites sont stockés, il peut éviter de voir sa responsabilité engagée s'il supprime immédiatement les informations illégales.[2552] Ne pas réagir immédiatement engagerait sa responsabilité.[2553]

Article 14
Hébergement
1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que:

a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente; ou

b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.
3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.

L'article 14 ne s'applique qu'aux fournisseurs limitant leurs services à la location d'infrastructures techniques de stockage de données. Des services Internet populaires, comme les plateformes d'enchères, proposent aussi de type d'hébergement.[2554]

6.7.7 Responsabilité de l'hébergeur (HIPCAR)

Le texte législatif rédigé par les Etats bénéficiaires dans le cadre de l'initiative HIPCAR[2555] représente une autre approche de la responsabilité des hébergeurs.

Hébergeur
30 *(1) Un hébergeur n'est pas responsable pénalement des informations stockées à la demande d'un utilisateur du service, à la condition que:*

(a) l'hébergeur retire ou désactive rapidement l'accès aux informations après avoir reçu de la part de l'autorité publique ou d'un tribunal quelconque une injonction de retirer des informations illégales spécifiques qu'il stocke; ou

(b) l'hébergeur, lorsqu'il a pris connaissance ou conscience d'informations illégales spécifiques stockées autrement que par une injonction émanant des pouvoirs publics, informe rapidement les pouvoirs publics pour leur permettre d'évaluer la nature des informations et, si nécessaire, d'émettre une injonction pour en retirer le contenu.

(2) Le paragraphe 1 ne s'applique pas lorsque l'utilisateur du service agit sous l'autorité ou le contrôle de l'hébergeur.
(3) Si l'hébergeur retire le contenu après avoir reçu une injonction conforme au paragraphe 1, il est exempté de l'obligation contractuelle auprès de son client d'assurer la disponibilité du service.

A l'instar de l'approche de l'Union européenne, la section II, Partie V, 30 (1) (a) limite la responsabilité de l'hébergeur si celui-ci enlève rapidement le contenu problématique après avoir reçu une injonction des pouvoirs publics ou d'un tribunal. Rapidement, en général, signifie en moins de 24 heures.[2556] La principale différence avec l'approche de l'UE réside dans la section II, Partie V, 30 (1) (b). Contrairement à l'approche communautaire, le fournisseur ne détermine pas si le contenu porté à son attention est illégal. S'il apprend l'existence de ce type de contenu, son obligation se limite d'abord à informer les pouvoirs publics (désignés) de l'existence d'un contenu potentiellement illicite. Les auteurs de cette disposition ont décidé qu'il revenait à ces autorités de déterminer la nature du contenu avant d'émettre une injonction de retrait.[2557] Si les informations sont considérées comme illégales, le fournisseur doit les retirer pour éviter que sa responsabilité ne soit engagée.

6.7.8 Exclusion de l'obligation de surveillance (Directive de l'Union européenne sur le commerce électronique)

Avant la mise en œuvre de la directive, la situation était incertaine dans quelques Etats membres quant à la possibilité de lancer d'éventuelles poursuites contre les fournisseurs sur la base d'une violation de leur obligation de contrôler les activités de leurs utilisateurs. Outre les conflits possibles avec les règles de protection des données et le secret des télécommunications, une telle obligation aurait plus particulièrement posé des difficultés aux hébergeurs qui stockent des milliers de sites Internet. Afin d'éviter ces conflits, la directive exclut toute obligation générale de surveiller les données transmises ou stockées.

> ***Article 15 – Absence d'obligation générale en matière de surveillance***
> *1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.*
> *2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.*

6.7.9 Responsabilité en matière d'hyperliens (ECC autrichien)

Les hyperliens jouent un rôle important sur la Toile. Ils permettent à leur fournisseur de guider l'utilisateur vers des informations précises disponibles en ligne. Plutôt que de se contenter de présenter les détails techniques permettant d'accéder à ces informations (par ex. en affichant le nom de domaine du site où les informations se trouvent), l'utilisateur peut directement y accéder en cliquant sur l'hyperlien actif. Celui-ci lance la commande pour que le navigateur web ouvre l'adresse Internet déposée.

Lors de la rédaction de la directive de l'Union européenne, la nécessité de réglementer les hyperliens a fait l'objet de débats intenses.[2558] Les auteurs du texte ont décidé de ne pas contraindre les Etats membres à harmoniser leur législation en la matière. A la place, ils ont prévu une procédure de réexamen pour que la nécessité de propositions portant sur la responsabilité des fournisseurs d'hyperliens et d'instruments de localisation puisse être prise en compte.[2559] Tant que les règles relatives à la responsabilité pour les hyperliens ne seront pas amendées, les Etats membres resteront libres de développer des solutions nationales.[2560] Certains pays de l'UE ont décidé de traiter de cette question par le biais d'une disposition spécifique.[2561] Ces pays ont basé la responsabilité des fournisseurs d'hyperliens sur les mêmes principes que ceux prévus par la directive pour la responsabilité des hébergeurs.[2562] Cette approche est la conséquence logique de la situation comparable dans laquelle se trouvent les hébergeurs et les fournisseurs d'hyperliens. Dans les deux cas, les fournisseurs contrôlent le contenu illégal ou au moins le lien vers celui-ci.

La section 17 de l'ECC autrichien en est un exemple.[2563]

> ***Sec. 17 ECC** (Autriche) – Responsabilité en matière d'hyperliens*
> *(1) Un fournisseur qui autorise l'accès à des informations transmises par un tiers en fournissant un lien électronique n'est pas responsable de ces informations si*
> *1. il n'a pas la connaissance véritable d'activités ou d'informations illégales et, lorsqu'une plainte pour dommage est déposée, il ne connaît ni les faits ni les circonstances à partir desquels le prestataire de services aurait pu déduire que ces activités ou informations fussent illégales; ou*
> *2. après avoir pris connaissance de ces activités ou informations, il a agi rapidement pour retirer le lien électronique.*

6.7.10 Responsabilité en matière de moteurs de recherche

Les fournisseurs de moteurs de recherche proposent des services de recherche permettant de trouver les documents d'intérêt en spécifiant certains critères. Le moteur recherchera les documents pertinents

correspondant aux critères tapés par l'utilisateur. Les moteurs de recherche jouent un rôle important dans le développement réussi d'Internet. Les contenus disponibles sur un site, mais non répertoriés à l'index d'un moteur de recherche ne sont accessibles que si la personne les recherchant connaît l'URL complète. *Introna/Nissenbaum* rappelle que « sans trop exagérer, on peut dire que pour exister, il faut être indexé par un moteur de recherche ».[2564]

Comme cela est le cas pour les hyperliens, la directive de l'Union européenne ne contient pas de normes définissant la responsabilité des opérateurs de moteurs de recherche. C'est pourquoi certains pays de l'UE ont décidé de consacrer une disposition à part à cette question.[2565] Contrairement à ce qui vaut pour les hyperliens, tous les pays n'ont pas basé leur réglementation sur les mêmes principes.[2566] L'Espagne[2567] et le Portugal ont ainsi fondé leur réglementation relative à la responsabilité des opérateurs de moteurs de recherche sur l'article 14 de la directive, alors que l'Autriche[2568] a basé la limitation de leur responsabilité sur l'article 12.

Sec. 14 ECC *(Autriche) – Responsabilité des opérateurs de moteurs de recherche*
(1) Un fournisseur qui propose un moteur de recherche ou d'autres outils électroniques pour rechercher des informations fournies par un tiers n'est pas responsable à condition:
1. qu'il ne déclenche pas la transmission;
2. qu'il ne choisisse pas le destinataire de la transmission; et
3. qu'il ne sélectionne ni ne modifie les informations contenues dans la transmission

[1479] For an overview of legal approaches, see also: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 18 *et seq.*, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1480] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.

[1481] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 255.

[1482] Four definitions are included in Art. 1 and an additional provision was included in Art. 9, Council of Europe Convention on Cybercrime.

[1483] For more information related to legal approaches regulating the liability of access provider see below: § 6.7.4

[1484] With regard to the lawful interception of communication see below: § 6.5.9.

[1485] With regard to the liability of caching provider see below: § 6.7.5.

[1486] For more details related to different legal approaches to criminalize child pornography see below: § 6.2.8.

[1487] With regard to the criminalization of such conduct see below: § 6.2.7.

[1488] Art. 2(a) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1489] Art. 3(a) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1490] Sec. 3(3) HIPCAR Model Legislative Text on Cybercrime.

[1491] With regard to details of the criminalization see below: § 6.2.8.

[1492] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1493] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1494] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1495] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1496] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1497] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1498] Art. 2(c) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1499] Art. 20(2) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1500] With regard to different approaches to criminalize data interference see below: § 6.2.5.

[1501] Regarding the criminalization of data espionage/illegal data acquisition see below: § 6.2.3.

[1502] Art. 1(b) Council of Europe Convention on Cybercrime, ETS 185.

[1503] Art. 1(b) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1504] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1505] Sec. 3(5) HIPCAR Model Legislative Text on Cybercrime.

[1506] Sec.3 (7) HIPCAR Model Legislative Text.

[1507] *Stair/Reynolds/Reynolds*, Fundamentals of Information Systems, 2008, page 167; *Weik*, Computer science and communications dictionary, 2000, page 826; *Stair/Reynolds*, Principles of Information Systems, 2011, page 15.

[1508] Art. 1(a) Council of Europe Convention on Cybercrime, ETS 185.

[1509] Art. 1(a) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The Framework Decision uses the term „information" system instead of computer system.

[1510] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1511] Sec. 3(4) HIPCAR Model Legislative Text on Cybercrime.

[1512] Regarding attacks against critical infrastructure see above: § 1.2

[1513] Regarding the related challenges see above: § 3.2.14.

[1514] With regard to the legal response see below: § 6.5.11.

[1515] Draft African Union Convention on the Establishment of a credible Legal Framework for Cyber Security in Africa, Version 1, January 2011.

[1516] See below: § 6.2.15.

[1517] See Art. 10 (1)(a) HIPCAR Model Legislative Text on Cybercrime.

[1518] See below: § 6.2.6.

[1519] With regard to the liability of different types of provider see below: § 6.7.

[1520] Regarding the liability of search engines see below: § 6.7.10.

[1521] With regard to illegal interception, see below: § 6.2.4.

[1522] For more details related to the interference with computer data see below: § 6.2.5.

[1523] With regard to system interference see below: § 6.2.6.

[1524] See in this regard below: § 6.2.14.

[1525] See below: § 6.5.12.

[1526] Regarding the different legal approaches to seize evidence see below: § 6.5.6.

[1527] See in this regard Art. 19 (3) Council of Europe Convention on Cybercrime.

[1528] Sec. 3 Commonwealth Model Law on Computer and Computer-related Crime.

[1529] Sec. 3(17) HIPCAR Model Legislative Text on Cybercrime.

[1530] See below: § 6.5.9.

[1531] Art. 1 Council of Europe Convention on Cybercrime.

[1532] Sec. 3(18) HIPCAR Model Legislative Text on Cybercrime.

[1533] *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[1534] These range from the simple proof that technical protection measures can be circumvented, to the intent to obtain data stored on the victim computer. Even political motivations have been discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

[1535] Regarding the independence of place of action and the location of the victim, see above § 3.2.7.

[1536] These can, for example, be passwords or fingerprint authorization. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of potential tools, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[1537] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is also highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

[1538] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 729.

[1539] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "The need for protection reflects the interests of organizations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

[1540] With regard to data espionage, see above, § 2.5.2 and below, § 6.1.3.

[1541] With regard to data interference, see above, § 2.5.4 and below, § 6.1.5.

[1542] *Sieber*, Informationstechnologie und Strafrechtsreform, page 49 *et seq.*

[1543] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1544] Art. 2 of the Convention on Cybercrime enables the Member States to keep those existing limitations that are mentioned in Art. 2, sentence 2. Regarding the possibility of limiting criminalization, see also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

[1545] An example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). This provision was changed in 2007. The following text presents the old version:

> *Section 202a – Data Espionage*
>
> *(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.*
>
> *(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.*

[1546] This approach is not only found in national legislation, but was also recommended by Council of Europe Recommendation No. (89) 9.

[1547] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1548] Regarding the system of reservations and restrictions, see *Gercke*, The Convention on Cybercrime, Computer Law Review International, 2006, 144.

[1549] *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1550] With regard to software tools that are designed and used to carry out such attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf. With regard to Internet-related social engineering techniques, see the information offered by the anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1551] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1552] The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5 per cent of the respondents reported that 80-100 per cent of their losses were caused by insiders. Nearly 40 per cent of all respondents reported that between 1 per cent and 40 per cent of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: www.gocsi.com/.

[1553] Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

[1554] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1555] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1556] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39

[1557] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the* conduct *involved is done "without right". It reflects the insight that the conduct described is not always punishable*

per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1558] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

[1559] *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, page 7.

[1560] See for example: World Information Technology And Services Alliance (WITSA), Statement On The Council Of Europe Draft Convention On Cybercrime, 2000, available at: www.witsa.org/papers/COEstmt.pdf. Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1561] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62 (dealing with Article 4).

[1562] *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[1563] This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

[1564] *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1565] Article 42 – Reservations: By a written notification addressed to the Secretary-General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[1566] This limits the criminalization of illegal access to those cases where the victim used technical protection measures to protect its computer system. Access an unprotected computer system would therefore not be considered a criminal act.

[1567] The additional mental element/motivation enables Member States to undertake a more focused approach rather than implementing a criminalization of the mere act of hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

[1568] This enables Member States to avoid a criminalization of cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

[1569] Framework Decision on Attacks against Information Systems – 19 April 2002 – COM (2002) 173. For more details, see above: § 5.2.1.

[1570] Article 2 – Illegal access to information systems:

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

[1571] Model Law on Computer and Computer Related Crime, LMM(02)17, available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers

Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1572] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1573] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1574] EU Directive 2013/40/EU on attacks against information systems.

[1575] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1576] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1577] See *Sofaer/Goodman/Cuellar/Drozdova and others*. A Proposal for an International Convention on Cybercrime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1578] In this context, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

[1579] Standalone computer systems are covered by Art. 1, paragraph 3, of the Draft Convention because they "control programs". This does not require a network connection.

[1580] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1581] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1582] The Explanatory Report points out that the provision intends to criminalize violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1583] See below: § 6.1.4.

[1584] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

[1585] One key indication of the limitation of application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet, which do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights."* See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1586] See in this context especially a recent case from Hong Kong, People's Republic of China. See above: § 2.5.2.

[1587] ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1588 Regarding the challenges related to the use of encryption technology by offenders, see above: § 3.2.14; *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf; *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html. Regarding the underlying technology, see: *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

1589 One of the consequences related to this aspect is the fact that limitation of the criminalization of illegal access to those cases where the victim of the attack secured the target computer system with technical protection measures could limit the application of such a provision, insofar as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

1590 Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996). See in this context: *Chamblee*, Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 *et seq.*), 177 A.L.R. Fed. 609 (2002); *Fischer*, An Analysis of the Economic Espionage Act of 1996, 25 Seton Hall Legis. J. 239 (2001).

1591 *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 986, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

1592 For details, see: US CCIPS, Prosecuting Intellectual Property Crimes, 3rd Edition, 2006, page 138 *et seq.* available at: www.justice.gov/criminal/cybercrime/ipmanual/04ipma.pdf.

1593 *Loundy*, Computer Crime, Information Warfare, and Economic Espionage, 2009, page 55 *et seq.*; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.* available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

1594 *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 988, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

1595 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1596 The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1597 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1598 This provision has recently been modified and now even criminalizes illegal access to data. The previous version of the provision has been used here, because it is better suited for demonstrating the dogmatic structure.

1599 See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

1600 A similar approach of limiting criminalization to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention on Cybercrime: *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.* For more information, see above: § 6.1.1.

1601 This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement, self-protection measures.

1602 See in this context for example a recent case in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Herald, 14.02.2008, available at: www.smh.com.au/news/web/stolen-photos-from-laptop-tell-a-tawdry-tale/2008/02/14/1202760468956.html; *Pomfret*, Hong Kong's Edision
Chen quits after sex scandal, Reuters, 21.02.2008, available at: www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

1603 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1604 With regard to "phishing", see above: § 2.9.4 and below: § 6.1.15 and as well: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Phishing, Computer und Recht, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1605 Regarding the risks related to the use of wireless networks, see above: § 3.2.3. Regarding the difficulties in cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

1606 Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1607 Regarding the underlying technology and the security related issues, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx. With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

1608 The computer magazine ct reported in 2004 that field tests proved that more than 50 per cent of 1 000 wireless computer networks that were tested in Germany were not protected. See: www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182.

1609 Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx.

1610 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1611 Regarding identity theft, see above: § 2.8.3 and below: § 6.1.16 and also: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1612 In the United States, the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes. Regarding offences related to social-security numbers, see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

1613 See: *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1, page 112.

1614 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1615 The Explanatory Report describes the technical means more in detail: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalization." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

1616 Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering".

1617 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

1618 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1619 See above: § 6.1.3.

1620 "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 55.

1621 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

1622 Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue, see Explanatory Report, No. 57: *"The creation of an offence in relation to "electromagnetic emissions" will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as "data" according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision"*, Explanatory Report to the Council of Europe Convention on Cybercrime, No. 57.

1623 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1624 *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1625 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 54.

1626 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39

1627 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1628 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1629 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1630 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1631 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1632 Cookies are data sent by a server to a browser and then sent back each time the browser is used to access the server. Cookies are used for authentication, tracking and keeping user information. Regarding the functions of cookies and the controversial legal discussion, see: *Kesan/Shah*, Deconstruction Code, Yale Journal of Law & Technology, 2003-2004, Vol. 6, page 277 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

1633 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1634 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1635 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1636 Model Law on Computer and Computer Related Crime" LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-

86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1637 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1638 The difficulty with offences against the integrity of data is that identification of these violations is often difficult to prove. Therefore, the Expert Group which drafted the Convention on Cybercrime identified the possibility of prosecuting violations regarding data interference by means of criminal law as a necessary strategic element in the fight against cybercrime. Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

1639 The 2007 Computer Economics Malware Report focuses on computer crime and analyses the impact of malware on the worldwide economy by summing up the estimated costs caused by attacks. It identified peaks in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion). For more information, see: 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code. A summary of the report is available at: www.computereconomics.com/article.cfm?id=1225.

1640 A number of computer fraud scams are including the manipulation of data – e.g. the manipulation of bank-account files, transfer records or data on smart cards. Regarding computer related fraud scams, see above: § 2.8.1 and below: § 6.1.17.

1641 Regarding the problems related to these gaps, see for example the LOVEBUG case, where a designer of a computer worm could not be prosecuted due to the lack of criminal law provisions related to data interference. See above: § 2.5.4 and: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1642 A similar approach to Art. 4 of the Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 – Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

1643 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

1644 As pointed out in the Explanatory Report, the two terms overlap. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1645 Regarding the more conventional ways to delete files using Windows XP, see the information provided by Microsoft, available at: www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

1646 Regarding the consequences for forensic investigations, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq.*, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1647 See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/05hb003.pdf.

1648 The fact that the Explanatory Report mentions that the files are unrecognizable after the process does not give any further indication with regard to the interpretation of the term. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1649 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1650 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf. In 2000 a number of well-known US e-commerce businesses were targeted by DoS attacks. A full list is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1651 With regard to the criminalization of DoS attacks, see also below: § 6.1.6.

1652 In addition, criminalization of DoS attacks is provided by Art. 5 of the Convention on Cybercrime. See below: § 6.1.6.

1653 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

1654 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Regarding the different recognized functions of malicious software, see above: § 2.5.4. Regarding the economic impact of malicious software attacks, see above: § 2.5.4.

1655 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1656 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1657 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report states: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always* punishable *per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1658 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62: "The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g., encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right." Regarding the liability of Remailer, see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1659 For further information, see *du Pont*, The Time Has Come For Limited Liability For Operators Of True Anonymity Remailers In Cyberspace: An Examination Of The Possibilities And Perils, Journal Of Technology Law & Policy, Vol. 6, Issue 2, page 176 *et seq.*, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1660 With regard to the possible difficulties to identify offenders who have made use of anonymous or encrypted information, the Convention leaves the criminalization of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

1661 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1662 For further information, see: *Gercke*, The EU Framework Decision on Attacks against Information Systems, Computer und Recht 2005, page 468 *et seq.*

1663 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1664 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1665 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1666 Sec. 5 (Illegal access), Sec. 8 (Illegal interception) and Sec. 10 (Child pornography).

1667 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cybercrime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1668 ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1669 A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see above: § 2.5.4 and US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

1670 For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, Inferring Internet Denial-of-Service Activities, page 1, available at: www.caida.org/papers/2001/BackScatter/usenixsecurity01.pdf; CNN News, One year after DoS attacks, vulnerabilities remain, at: http://edition.cnn.com/2001/TECH/internet/02/08/ddos.anniversary.idg/index.html. *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1671 Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: Campbell/Gordon/Loeb/Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, pages 431-448.

1672 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding cyberterrorism, see above § 2.9.1 and *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyberterrorism and Cybersecurity, available at: www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeld*t, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: *Prados*, America Confronts Terrorism, 2002, 111 *et seq.*;

Lake, 6 Nightmares, 2000, page 33 et *seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.* OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf; *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, pages 221-249.

1673 The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 65.

1674 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1675 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1676 The Explanatory Report gives examples for implementation of restrictive criteria for serious hindering: "Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate "denial-of-service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)" – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 67.

1677 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Although the connotation of "serious" does limit the applicability, it is likely that even serious delays to operations resulting from attacks against a computer system can be covered by the provision.

1678 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1679 Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection.

1680 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61. Regarding the fact that the definition does not distinguish between the different ways how information can be deleted, see above: § 6.1.15. Regarding the impact of the different ways of deleting data on computer forensics, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq*., available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1681 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1682 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is therefore likely that the provision could cover unauthorized corrections of faulty information as well.

1683 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1684 "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam legislation worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: § 2.5.g.

1685 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1686 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1687 Regarding legal approaches in the fight against spam, see above: § 6.1.l3.

1688 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1689 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1690 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1691 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable*

per *se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1692 See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

1693 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 68: "The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized by this article, even if it causes serious hindering."

1694 Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

1695 Article 3 – Illegal system interference: "Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor".

1696 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf..

1697 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1698 Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), PC-CY (2000), 19, available at: www.iwar.org.uk/law/resources/eu/cybercrime.htm.

1699 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/ documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1700 For an overview on hate speech legislation, see for example: the database provided at: www.legislationline.org. For an overview on other cybercrime-related legislation, see: the database provided at: www.cybercrimelaw.net.

1701 Regarding the challenges of international investigation, see above: § 3.2.4 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1702 For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

1703 *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 5.

1704 Regarding the influence of pornography on minors, see: *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact, and Prevention, Youth & Society,

Vol. 34, 2003, page 330 *et seq.*, available at: www.unh.edu/ccrc/pdf/Exposure_risk.pdf; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002, available at: http://findarticles.com/p/articles/mi_m2372/is_1_39/ai_87080439.

1705 See Section 11 Subparagraph 3 Penal Code: "Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection".

1706 *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 28.

1707 The draft law was not in force by the time this publication was finalized.

1708 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1709 Regarding the challenges of international investigation, see above: § 3.2.4. See also: *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1710 *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Cox*, Litigating Child Pornography and Obscenity Cases, Journal of Technology Law and Policy, Vol. 4, Issue 2, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB.

1711 Regarding methods of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication, see above: § 3.2.14.

1712 It has been reported that some websites containing child pornography register up to a million hits per day. For more information, see: *Jenkins*, Beyond Tolerance: Child Pornography on the Internet, 2001, New York University Press; *Wortley/Smallbone*, Child Pornography on the Internet, page 12, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1713 Regarding the challenges related to investigations involving anonymous communication technology, see above: § 3.2.l.

1714 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

1715 *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 68..

1716 *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11, page 6, available at: http://jjlp.law.ucdavis.edu/archives/vol-11-no-1/07%20Liu%2011.1.pdf.

1717 *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 69.

1718 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

1719 *Akdeniz* in *Edwards/Waelde*, Law and the Internet: Regulating Cyberspace; *Williams* in *Miller*, Encyclopaedia of Criminology, page 7. Regarding the extent of criminalization, see: Child Pornography: Model Legislation & Global Review, 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalization of child pornography and freedom of speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws in terms of the criminalization of child pornography.

1720 Regarding differences in legislation, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 26, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1721 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91..

1722 *Walden*, Computer Crimes and Digital Investigations, 2006, page 144.

1723 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 94.

[1724] Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, ETS 201.

[1725] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 135.

[1726] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1727] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 95.

[1728] Regarding criminalization of the possession of child pornography in Australia, see: *Krone*, Does thinking make it so? Defining online child pornography possession offences, in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalization of child pornography.

[1729] See: Child Pornography: Model Legislation & Global Review, 2006, page 2, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[1730] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 98.

[1731] *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

[1732] Based on the National Juvenile Online Victimization Study, only 3 per cent of arrested Internet-related child-pornography possessors had morphed pictures. *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1733] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 102.

[1734] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1735] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1736] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1737] Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49. Article 1. For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

[1738] One example is the current German Penal Code. The term "child" is defined by law in Section 176 to which the provision related to child pornography refers: Section 176: "Whoever commits sexual acts on a person under fourteen years of age (a child)...".

[1739] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[1740] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, available at: http://conventions.coe.int.

[1741] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1742] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1743] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1744] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1745] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by*

established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1746 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1747 *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

1748 Regarding the challenges related to the use of encryption technology, see above: § 3.2.14. One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

1749 See Explanatory Report to the Convention on the Protection of Children, No. 140.

1750 The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or is just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

1751 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1752 Official Notes:

NOTE: The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.

NOTE: The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read: "commits an offence punishable, on conviction:

(a) in the case of an individual, by a fine not exceeding [amount] or imprisonment for a period not exceeding [period]; or

(b) in the case of a corporation, by a fine not exceeding [a greater amount].

1753 Official Note:

NOTE: Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.

1754 See the preface to the Optional Protocol.

1755 See Art. 2.

1756 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225,

available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1757 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1758 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1759 See in this regard: *Powell*, Paedophiles, Child Abuse and the Internet, 2007; *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010, available at: www.cse.dmu.ac.uk/~bstahl/index_html_files/2010_grooming_ICIS.pdf.

1760 See: Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

1761 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1762 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

1763 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 157.

1764 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 159.

1765 International Mechanisms for Promoting Freedom of Expression, Joint Declaration, Challenges to Freedom of Expression in the New Century, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2001.

1766 For an overview of hate speech legislation, see the database provided at: www.legislationline.org.

1767 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1768 Regarding the criminalization of hate speech in Europe, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 781 *et seq.* available at: http://law.wlu.edu/ deptimages/Law%20Review/62-2VanBlarcum.pdf. Regarding the situation in Australia, see: *Gelber/Stone*, Hate Speech and Freedom of Speech in Australia, 2007.

1769 Vienna Summit Declaration, 1993, available at: www.coe.int/t/dghl/monitoring/ecri/archives/other_texts/2-vienna/plan_of_action/plan_of_action_vienna_summit_EN.asp.

1770 Recommendation No. 1275 on the fight against racism, xenophobia, anti-Semitism and intolerance.

1771 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4: "The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

1772 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

1773 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf..

1774 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1775] Regarding the list of states that signed the Additional Protocol, see above: § 5.2.1.

[1776] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

[1777] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at: www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1778] Regarding the challenges of international investigation, see above: § 3.2.5 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1779] Regarding possible reservations, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 792

[1780] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1781] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1782] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1783] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 29.

[1784] Regarding the definition of "distributing" and "making available", see § 6.1.8 above.

[1785] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 34.

[1786] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1787] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 36.

[1788] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1789] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1790] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1791] Regarding legislation on blasphemy, as well as other religious offences, see: Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf.

[1792] International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2006.

1793 See above: § 6.1.9, as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

1794 The draft law was not in force at the time this publication was finalized.

1795 Prevention of Electronic Crimes Ordinance 2007, available at: www.upesh.edu.pk/net-infos/cyber-act08.pdf.

1796 Prevention of Electronic Crimes Ordinance, 2007, published in the Gazette of Pakistan, Extraordinary, Part-I, dated 31 December 2007, available at: www.na.gov.pk/ordinances/ord2008/elect_crimes_10042008.pdf.

1797 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1798 Regarding the difficulties related to jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

1799 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing
National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1800 Regarding the challenges of international investigation, see above: § 3.2.6 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1801 The 2005 e-gaming data report estimates total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm. Regarding the number of licensed Internet websites related to Internet gambling in selected countries, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 52, available at: www.gao.gov/new.items/d0389.pdf. Regarding the total numbers of Internet gambling websites, see: *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf.

1802 For an overview of different national Internet gambling legislation, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

1803 Regarding the situation in the People's Republic of China, see for example: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

1804 Regarding addiction, see: *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: www.european-lotteries.org/data/info_130/Wood.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

1805 See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

1806 See *Thumm*, Strafbarkeit des Anbietens von Internetgluecksspielen gemaess § 284 StGB, 2004.

1807 Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which do not know that their services are abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

[1808] For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously, criminalization is limited to those cases where the offender is intentionally making the equipment available.

[1809] This is especially relevant with regard to the location of the server.

[1810] Avoiding the creation of safe havens is a major intention of harmonization processes. The issue of safe havens has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 states that: "*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "*There must be no safe havens for those who abuse information technologies*".

[1811] With regard to the principle of sovereignty, changing the location of a server can have a great impact on the ability of law-enforcement agencies to carry out an investigation. National Sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[1812] Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene, see above: §§ 3.2.6 and 3.2.7.

[1813] For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

[1814] Regarding the vulnerability of Internet gambling to money laundering, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 5, 34 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

[1815] Regarding other recent approaches in the United States, see: *Doyle*, Internet Gambling: A Sketch of Legislative Proposals in the 108th Congress, CRS Report for Congress No. RS21487, 2003, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-4047: *Doyle*, Internet Gambling: Two Approaches in the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

[1816] For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII, page 1183 *et seq.*, available at: http://law.fordham.edu/publications/articles/600flspub8956.pdf.

[1817] *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

[1818] *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm

[1819] Based on Sec. 5366, criminalization is limited to the acceptance of financial instruments for unlawful Internet gambling.

[1820] See: EU opens investigation into US Internet gambling laws, EU Commission press release, 10.03.2008, available at: http://ec.europa.eu/trade/issues/respectrules/tbr/pr100308_en.htm; *Hansen*, EU investigates DOJ internet gambling tactics, The Register, 11.03.2008, available at: www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

[1821] General Agreement on Trade in Services (GATS) – with regard to the United States Unlawful Internet Gambling Enforcement Act especially Articles XVI (dealing with Market Access) and XVII (dealing with National Treatment) could be relevant.

[1822] See above: § 3.2.l.

[1823] See above: § 3.2.2.

[1824] See, for example: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US delegation to OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; Lisby, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf; *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the

Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

1825 See, for example, the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information, see: www.osce.org/documents/rfm/2004/10/14893_en.pdf. See in addition the statement of the representative on Freedom of the Media, Mr Haraszti, at the fourth Winder Meeting of the OSCE Parliamentary Assembly on 25 February 2005.

1826 Regarding various regional approaches to criminalization of defamation, see: *Greene* (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf.

1827 For more details, see: the British Crime Survey 2006/2007 published in 2007, available at: www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

1828 See: Crime Statistic Germany (Polizeiliche Kriminalstatistik), 2006, available at: www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

1829 The full version of the Criminal Defamation Amendment Bill 2002 is available at: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02_P.pdf. For more information about the Criminal Defamation Amendment Bill 2002, see the Explanatory Notes, available at: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf.

1830 The full text of the Criminal Code of Queensland, Australia is available at: www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

1831 The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see: www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails are spam. See: http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

1832 For more information on the phenomenon, see above: § 2.6.7. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1833 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf

1834 See ITU Survey on Anti-Spam Legislation Worldwide, 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1835 Regarding the availability of filter technology, see: *Goodman,* Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam Consumer Perspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

1836 Spam Issues in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1837 See Spam Issues in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1838 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1839 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69: "The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law."

1840 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at:

www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1841 The document available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1842 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1843 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1844 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1845 Regarding the US legislation on spam, see: *Sorkin*, Spam Legislation in the United States, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Warner*, Spam and Beyond: Freedom, Efficiency, and the Regulation of E-mail Advertising, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Alongi*, Has the US conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 *et seq.*, available at: www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

1846 For more details about the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM act 2003), see: www.spamlaws.com/f/pdf/pl108-187.pdf.

1847 See: *Hamel,* Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?, New Eng. Law Review, 39, 2005, 196 *et seq*. 325, 327 (2001).

1848 For more details, see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1849 For more information, see: Wong, The Future Of Spam Litigation After Omega World Travel v. Mummagraphics, Harvard Journal of Law & Technology, Vol. 20, No. 2, 2007, page 459 et seq., available at: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech459.pdf.

1850 Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

1851 One example of this misuse is the publication of passwords used for access control. Once published, a single password can grant access to restricted information to hundreds of users.

1852 One example is the 2001 EU Framework Decision combating fraud and counterfeiting of non-cash means of payment.

1853 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 71: "To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries".

1854 With the definition of "distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report, No. 72), the drafters of the Convention restrict devices to software. Although the Explanatory Report is not definitive in this matter, it is likely that it covers not only software devices, but hardware tools as well.

1855 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1856 See, in this context: *Biancuzzi*, The Law of Full Disclosure, 2008, available at: www.securityfocus.com/print/columnists/466.

1857 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

[1858] See for example one approach in the US legislation:

18 USC. § 1029 (Fraud and related activity in connection with access devices)

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A) offering an access device; *or*

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; *or*

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; *shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.*

(b)

(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both. […]

[1859] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1860] This approach could lead to broad criminalization. Therefore Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

[1861] Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

[1862] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1863] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72: "*This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices*".

[1864] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society.

[1865] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 73: The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

[1866] Regarding the US approach to address the issue, see for example 18 USC. § 2512 (2):

(2) It shall not be unlawful under this section for –

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

[1867] *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1868] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76: "Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'."

[1869] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 731.

[1870] See, for example, the World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1871] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1872] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

[1873] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the* conduct *involved is done* "*without right*"*. It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression* '*without right*' *derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1874] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 77.

[1875] For more information, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 78.

[1876] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1877] Expert Group's suggestion for an amendment:

Paragraph 3: A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.

Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

[1878] Canada's suggestion for an amendment:

Paragraph 3:

(3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8, unless the person raises a reasonable doubt as to its purpose.

Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

[1879] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1880] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1881] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1882] "Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating." See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1883] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1884] See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

[1885] See for example: *Austria*, Forgery in Cyberspace: The Spoof could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, Vol. IV, 2004, available at: http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf.

[1886] See for example 18 USC. § 495:

> Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or

Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited –

Shall be fined under this title or imprisoned not more than ten years, or both.

Or Sec. 267 German Penal Code:

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:

1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;
2. causes an asset loss of great magnitude;
3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

[1887] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 82.

[1888] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

[1889] See Art. 1 (b) Convention on Cybercrime.

[1890] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

[1891] For example, by filling in a form or adding data to an existing document.

[1892] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

[1893] With regard the definition of "alteration" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1894] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1895] With regard the definition of "suppression" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1896] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1897] With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1898] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1899] If only part of a document is deleted the act might also be covered by the term "alteration".

[1900] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1901] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1902] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self*

defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1903] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 85.

[1904] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1905] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1906] See, for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: http://edition.cnn.com/2006/US/05/18/identity.theft/; Identity Fraud, NY Times Topics, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html; *Stone*, US Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

[1907] See, for example, the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1908] See, for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the US: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[1909] Regarding the phenomenon of identity theft, see above: § 2.8.3.

[1910] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1911] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1912] *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

[1913] *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[1914] This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data, see: *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007, available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1 ; ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

1915 The reason for the success is the fact that the provisions focus on the most relevant aspect of phase 1: transfer of the information from the victim to the offender.

1916 Examples of acts that are not covered include the illegal access to a computer system in order to obtain identity related information.

1917 One of the most common ways the information obtained is used is fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1918 Furthermore, it is uncertain whether the provisions criminalize possession if the offender does not intend to use the data but to sell them. Prosecution could in this case in general be based on fact that 18 USC. § 1028 not only criminalizes possession with the intent to use it to commit a crime, but also to aid or abet any unlawful activity.

1919 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1920 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1921 See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

1922 Similar provisions are included in the Commonwealth Model Law and the Stanford Draft International Convention. For more information about the Commonwealth model law, see: Model Law on Computer and Computer Related Crime, LMM(02)17. The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Stanford Draft International Convention, see: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1923 See above: § 6.1.1.

1924 See above: § 6.1.4.

1925 See above: § 6.1.5.

1926 *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1927 See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1928 See above: § 2.8.1.

1929 Regarding the criminalization of computer-related fraud in the UK, see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 *et seq.*

1930 One example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does not therefore cover the majority of computer-related fraud cases:

Section 263 Fraud

(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

1931 A national approach that is explicitly address computer-related fraud is 18 USC. § 1030:

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC. 1681 et seq.);

(B) information from any department or agency of the United States; *or*

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

[1932] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1933] The drafters highlighted that the four elements have the same meaning as in the previous articles: "To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer program or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1934] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1935] With regard to the definition of "alteration" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1936] With regard to the definition of "suppression" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1937] With regard to the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1938] As a result, not only data-related offences, but also hardware manipulations, are covered by the provision.

[1939] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 87.

[1940] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 88.

[1941] "The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another."

[1942] The drafters of the Convention point out that these acts are not meant to be included in the offence established by Article 8 – Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

[1943] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by*

established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1944] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

[1945] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1946] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1947] Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

[1948] For more information on the effects of digitization on the entertainment industry, see above: § 2.7.1.

[1949] The technology that is used is called digital rights management – DRM. The term digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies or other digital data. One of the key functions is copy protection, which aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[1950] Regarding the technical approach to copyright protection, see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

[1951] For details see above: § 2.7.1.

[1952] Examples are 17 USC. § 506 and 18 USC. § 2319:

Section 506. Criminal offenses

(a) Criminal Infringement. — Any person who infringes a copyright willfully either –

(1) for purposes of commercial advantage or private financial gain, or

(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.

[...]

Section 2319. Criminal infringement of a copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506(a)(1) of title 17 –

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;

(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.

(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements shall include –

(A) producers and sellers of legitimate works affected by conduct involved in the offense;

(B) holders of intellectual property rights in such works; and

(C) the legal representatives of such producers, sellers, and holders.

(e) As used in this section –

(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and

(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.

Regarding the development of legislation in the United States, see: *Rayburn*, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

1953 Regarding the international instruments, see: *Sonoda*, Historical Overview of Formation of International Copyright Agreements in the Process of Development of International Copyright Law from the 1830s to 1960s, 2006, available at: www.iip.or.jp/e/summary/pdf/detail2006/e18_22.pdf; *Okediji*, The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, 2006, available at: www.unctad.org/en/docs/iteipc200610_en.pdf. Regarding international approaches to anti-circumvention laws, see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

1954 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 109.

1955 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 110: "With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

1956 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 111: "The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

1957 Explanatory Report to the Council of Europe Convention on Cybercrime, Nos. 16 and 108.

[1958] *Article 61:*

Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale

[1959] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 113.

[1960] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 114.

[1961] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression* 'without *right*' *derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1962] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 115. In addition, the drafters pointed out: The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

[1963] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1964] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1965] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1966] See, for example, Art. 5 of the Convention on Cybercrime.

[1967] Convention on Cybercrime, ETS 185.

[1968] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1969] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1970] EU Framework Decision on Combating Terrorism, COM (2007) 650.

[1971] EU Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[1972] EU Framework Decision 2008/919/JHA of 28 November 2008, No. 4.

[1973] The intention of the drafters to cover online and offline activities was highlighted several times. See, for example: EU Framework Decision 2008/919/JHA of 28 November 2008, No. 11. "These forms of behavior should be equally punishable in all Member States irrespective of whether they are committed through the Internet or not."

[1974] Regarding the motivation, see: *Russell*, A History of the United Nations Charter, 1958.

1975 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

1976 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 59.

1977 *Mani*, Basic Principles of Modern International Law: A Study of the United Nations Debates on the Principles of International Law Concerning Friendly Relations and Co-operation among States, 1993, page 263 *et seq.*

1978 *Bond*, Peacetime foreign Data Manipulations as one Aspect of Offensive Information Warfare, 1996.

1979 *Brownlie*, International Law and the Use of Force, 1993, page 362.

1980 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 80.

1981 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyber force, Alb. Law Journal of Science and Technology, Vol. 18, page 304.

1982 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57..

1983 *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1 000 Centrifuges at the Nataz Enrichment Plant?, Preliminary Assessment, Institute for Science and International Security, 2010.

1984 Regarding proliferation concerns, see: *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 58.

1985 With regard to the development, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

1986 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5.

1987 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 6.

1988 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

1989 Regarding the admissibility and reliability of digital images, see: *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy, page 267 *et seq.*

1990 *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7, page 71 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 14. Regarding the legal frameworks in different countries, see: *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 76; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213.

1991 See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

1992 For a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206..

1993 The Council of Europe Convention on Cybercrime therefore contains a provision that clarifies that the procedural instruments in the Convention shall not only be applicable with regard to cybercrime-related offences, but also to "other criminal offences committed by means of a computer system" and "the collection of evidence in electronic form of a criminal offence" (Art. 14).

[1994] *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

[1995] Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

[1996] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

[1997] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq*

[1998] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 1.

[1999] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[2000] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286. With more reference to national law: *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213; *Vaciago*, Digital Evidence, 2012, Chapter I.1 (with an overview about the discussion about digital evidence in different jurisdictions).

[2001] Police and Criminal Evidence Code (PACE).

[2002] *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

[2003] Regarding the different models of cybercrime investigation, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[2004] This includes the development of investigation strategies.

[2005] The second phase covers, in particular, the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2006] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[2007] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

[2008] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2009] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[2010] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2011] This includes, for example, the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[2012] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2013] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see:

Gordon/Hosmer/Siedsma/Rebovich, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59

2014 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

2015 *Vaciago*, Digital Evidence, 2012, Chapter II.

2016 *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

2017 Regarding geo-recognition, see: *Friedland/Sommer*; Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, available at: www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf; *Strawn*, Expanding the Potential for GPS Evidence Acquisition, Small Scale Digital Device Forensics Journal, 2009, Vol. 3, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V3_1_Strawn.pdf; *Zdziarski*, iPhone Forensics, 2008, available at:www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

2018 See *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010, page 95 *et seq.*, available at: www.dfrws.org/2010/proceedings/2010-311.pdf.

2019 Regarding the use of metadata for investigations, see: *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf.

2020 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

2021 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217. Regarding the challenges of witnesses as a source of evidence, see: *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002.

2022 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2023 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.

2024 Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

2025 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161.

2026 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2027 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2028 Daubert v. Merrell Dow Pharmaceutical, Inc. (1993) 113 S. Ct. 2786, available at: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=509&invol=579.

2029 *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3, page 1.

2030 The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

2031 Regarding the status of national legislation, see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

2032 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

2033 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

2034 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

2035 *Casey*, Digital Evidence and Computer Crime, 2004, page 15.

2036 *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2Dpage 38F31AF079F9.pdf; With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2037 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf. Criteria for Admissibility of Expert Opinion, Utah Law Review, 1978, page 546 *et seq.*

2038 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

2039 See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39

2040 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

2041 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2042 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2043 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

2044 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 92.

2045 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

2046 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2047 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2048 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

2049 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2050 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2051 For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

2052 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[2053] *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

[2054] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[2055] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2056] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[2057] Regarding the design of courtrooms, see: *Youngblood*, Courtroom Design, 1976; *Smith/Larson*, Courtroom design, 1976.

[2058] Scientific Evidence Review: Admissibility of Expert Evidence, ABA, 2003, page 159 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 169; *Nilsson*, Digital Evidence in the Courtroom, 2010; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12, Issue 1.

[2059] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2060] See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 538.

[2061] Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

[2062] *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

[2063] *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq*.

[2064] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 218

[2065] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

[2066] See in this context: *Nikali*, The Substitution of Letter Mail in Targeted Communication, 2007, available at: http://hsepubl.lib.hse.fi/pdf/diss/a136.pdf.

[2067] See in this context *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Hayes*, Forensic Handwriting Examination, 2006.

[2068] *Houck/Siegel*, Fundamentals of Forensic Science, 2010, page 512 *et seq.*; FBI Handbook of Crime Scene Forensics, 2008, page 111 *et seq.*; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962, Vol. 7, Issue 3, page 286 *et seq.*; *Miller*, An Analysis of the Identification Value of Defects in IBM Selectric Typewriters, American Academy of Forensic Science annual meeting, presented paper, Ohio, 1983; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007, page 207 *et seq*.

[2069] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[2070] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[2071] *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No. 1, page 16 *et seq.*, available at: http://airccse.org/journal/nsa/0409s2.pdf.

[2072] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2073] Regarding approaches to link a suspect to stored computer records, see for example: *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 165.

[2074] Regarding the obligation to register prior to the use of public Internet terminals in Italy, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, page 94.

2075 See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

2076 Regarding a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

2077 Regarding the extent of commercial child pornography, see: IWF 2007 Annual and Charity Report, page 7.

2078 See *Schnabel,* The Mikado Principle, Datenschutz und Datensicherheit, 2006, page 426 *et seq.*

2079 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 206.

2080 Regarding the legitimacy principle, see: *Grans/Palmer*, Australian Principles of Evidence, 2005, page 10.

2081 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 219.

2082 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.

2083 *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

2084 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

2085 Regarding necessary procedures, see: *Chawki*, The Digital Evidence in the Information Era, available at: www.droit-tic.com/pdf/digital_evid.pdf; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2086 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2087 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

2088 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2089 See in this context also: *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

2090 Regarding the consequences of the fruit of the poisonous tree doctrine for computer-crime investigations, see: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 563.

2091 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

2092 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.

2093 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332.

2094 *Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563, [2001] EMLR 654. The primary evidence rule was in any event inapplicable to recordings on film or tape, which may be proven by copies under common law (*Kajala v Noble* (1982) 75 Cr App Rep 149, DC; R v. Wayte (1982) 76 Cr App Rep 110, CA) and if lost or destroyed their contents may be proven by oral evidence from persons who have previously viewed or heard them (*Taylor v Chief Constable of Cheshire* [1987] 1 All ER 225, 84 Cr App Rep 191, DC). Also, see now the Criminal Justice Act 2003 s 133; and para 1464 post.

2095 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; *Permanent Trustee Co of New South Wales v Fels* [1918] AC 879, PC.

2096 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; The admission of documentary copies is subject to the Civil Evidence Act 1995: see PARA 808 *et seq.*

2097 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2098 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2099 With regard to different exemptions, see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 *et seq.*; Best Evidence Rule, California Law Review Commission, 1996, available at: www.clrc.ca.gov/pub/Printed-Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2100 For further reference, see: *Eltgroth*, Best Evidence and the Wayback Machine, Fordham Law Review, 2009, 193, available at: http://law.fordham.edu/assets/LawReview/Eltgroth_October_2009.pdf

2101 With regard to European common law countries (UK, Ireland), this development was especially supported by EU Directive 1999/93/EC. See also Sec. 4 and 6 of the Commonwealth model law on electronic evidence.

2102 *Munday*, Evidence, 2007, page 380; *Allen*, Practical Guide to Evidence, 2008, page 189.

2103 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567.

2104 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567 and *R v Sharp* [1988] 1WLR 7, HL; *R v Kearley* [1992] 2 AC 228, [1992] 2 All ER 345. HL. See also Civil Evidence Act 1995 ss1-7.

2105 Per Lord Havers in *R v Sharp* [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion.

2106 *Keane*, Modern Law of Evidence, 2005, pages 246-266.

2107 *Dennis*, The Law of Evidence, 2002, Chapters 16-17.

2108 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

2109 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006.

2110 See in this context, for example, Part II of the Irish Criminal Evidence Act 1992.

2111 R v Dodson [1984] 1 WLR 971, 79 CrApp Rep 220, CA (photographic evidence); R v Maqsud Ali [1966] 1 QB 688, 49 Cr App Rep 230, CCA (tape recorded conversation); R v Wood (1982) 76 Cr App Rep 23, CA; Castle v Cross [1984] 1 WLR 1372, DPP v McKeown [1997] 1 All ER 737, 2 Cr App Rep 155, HL (computer evidence).

2112 A "statement" is now defined as any representation of fact or opinion made by a person by whatever means; and it includes a representation made in a sketch, photo or other pictorial form: Criminal Justice Act 2003 ss 115(2), 134 (2).

2113 See in this context, for example, the Statue of Liberty case, [1968] 1 W.L.R. 739.

2114 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

2115 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

2116 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

2117 *Insa/Lazaro*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 214; *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 205.

2118 Model Law on Electronic Evidence (LMM(02)12.

2119 Singapore Evidence Act, Section 35.

2120 Canada Uniform Electronic Evidence Act.

2121 See above.

2122 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. For more information, see: *Dumortier*, The European Directive 1999/93/EC on a Community Framework for Electronic Signatures, in Lodder/Kaspersen, eDirectives, 2000, page 33 *et seq.*, available at: www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf.

2123 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

2124 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2125 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2126 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2127 United Nations Report oft he International Law Commission, Fifty-eigth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm

2128 *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

2129 For a general overview see: *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

2130 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm..

2131 National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2132 *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

2133 *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 6; *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

2134 *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

2135 International Court of Justice, Case of S.S."Lotus", Series A – No. 10, 1927, available at: www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

2136 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.html; Dunn/Krishna-Hensel/Mauer (eds), The Resurgence of the State, Trends and Progress in Cyberspace Governance, 2007, page 69.

2137 *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 8, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

2138 For an overview about relevant case examples for conflicts see: *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 10 et seq.

2139 *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 21.

2140 See in this regard for example: *Ali/Ragothaman/Bhagavathula/Pendse*, Security Issues in Airplane Data Networks, available at: http://soar.wichita.edu/dspace/bitstream/handle/10057/398/GRASP-4.pdf?sequence=1; The Developments in Satellite Hardware, Satellite Executive Briefing, Vol. 3, No. 12, 2010, available at: www.satellitemarkets.com/pdf/aug10.pdf.

2141 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2142 See *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Cameron*, Protective Principle of International Criminal Jurisdiction, 1994.

2143 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2144 *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72. Regarding the use of the principle within the US see for example United States v. Gallaxy Sports.

2145 See in this regard below: § 6.2.8.

2146 *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72.

2147 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2148 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2149 See: *Kobrick*, The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes, Columbia Law Review, Vol 87, 1987, page 1523 et seq; Regarding the discussion about scope and application of the principle of universal jurisdiction within the UN see the information provided by the Sixth Committee, available at: www.un.org/en/ga/sixth/64/UnivJur.shtml.

2150 For an overview about the implementation of the principle in European countries see: Universal Jurisdiction in Europe – The State of the Art, Human Rights Watch, 2006, available at: www.hrw.org/sites/default/files/reports/ij0606web.pdf.

2151 See above: §§ 4.5.4 and 6.1.

2152 This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132. Regarding the substantive criminal law provisions related to cybercrime, see above: § 6.1.

2153 Regarding the elements of an anti-cybercrime strategy, see above: § 4. Regarding user-based approaches in the fight against cybercrime, see: *Görling*, The Myth Of User Education, 2006, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

2154 Due to the protocols used in Internet communication and worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence, see above: § 3.2.7.

2155 Regarding the challenges of fighting cybercrime, see above: § 3.2.

2156 The pure fact that the offender is acting from a different country can result in additional challenges for law-enforcement agencies' investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases, the investigation nevertheless requires international cooperation between the authorities in both countries, which in general is more time consuming compared to investigations concentrating on a single country.

2157 See in this context also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 134.

2158 For an overview of the current status of the implementation of the Convention on Cybercrime and its procedural law provisions in selected countries, see the country profiles made available on the Council of Europe website: www.coe.int/cybercrime/.

2159 See Articles 15-21 of the Council of Europe Convention on Cybercrime.

2160 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework,

International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

2161 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21.

2162 *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding
the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

2163 *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

2164 For an overview of different kinds of evidence that can be collected by computer forensic experts, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2165 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

2166 For an overview of different forensic investigation techniques related to the most common technologies, see: *Carney/Rogers*, The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Vol. 2, Issue 4; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Urnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, Vol. 5, Issue 1; *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2; *Gupta/Mazumdar*; Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4; Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Vol. 5, Issue 1; *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary
Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233; *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

2167 *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

2168 Regarding the different models of Cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

2169 This includes the development of investigation strategies.

2170 The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2171 With regard to developments, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive,
50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

2172 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2173] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2174] *Vaciago*, Digital Evidence, 2012, Chapter II.1; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

[2175] For guidelines on how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2176] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[2177] Regarding investigation techniques, see: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, page 283 *et seq*.

[2178] *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No. 1.

[2179] *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, Vol. 19, page 1227 *et seq.*; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 54.

[2180] See below: § 6.3.8.

[2181] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 171.

[2182] Regarding the challenges of encryption, see § 3.2.14 as well as *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, Issue 3.

[2183] Regarding possible counter strategies for law enforcement, see: *Haldeman/Schoen/Heninger* and other, Lest we Remember: Cold Boot Attacks on Encryption keys, 2008, available at: http://citp.princeton.edu/memory.

[2184] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2185] *Vaciago*, Digital Evidence, 2012, Chapter II.1.

[2186] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 59.

[2187] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2188] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2189] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2190] *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

[2191] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, page 297.

[2192] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process in forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[2193] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the forensic software magic lantern, developed as a keylogger used by law enforcement in the US, see: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001, available at:

www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

2194 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2195 *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2.

2196 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 52.

2197 For an overview of the debate, see: *Gercke*, The Role of Internet Service Providers in the Fight Against Child Pornography Computer Law Review International, 2009, page 65 *et seq.*

2198 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 15.

2199 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 24.

2200 See *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime – Toward common best-of-breed guidelines?, 2008, available at: www.coe.int/cybercrime/.

2201 For more information about the Guidelines, see: *Gercke,* The Council of Europe Guidelines for the Cooperation between LEAs and ISPs against Cybercrime, Computer Law Review International, 2008, page 97 *et seq.*

2202 See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 29.

2203 See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 30.

2204 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

2205 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

2206 Regarding the impact on tracing offenders, see: *Nicoll*, Concealing and Revealing Identity on the Internet in *Nicoll/Prins/Dellen*, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 *et seq.*

2207 *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

2208 For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2209 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, No. 4.

2210 For more information, see: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, § 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, page 149.

2211 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, The criminalization of Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide: Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

2212 *Casey*, Digital Evidence and Computer Crime, 2004, page 19.

2213 For more information, see: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten, 08.01.2007, available at: www.spiegel.de/panorama/justiz/0,1518,457844,00.html.

2214 *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 472.

2215 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2216 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 90, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2217 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

2218 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

2219 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2220 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

2221 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 64, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2222 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

2223 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.

2224 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

2225 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

2226 With regard to the criminalization of illegal devices, see below: § 6.1.15.

2227 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

2228 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

2229 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 29.

2230 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

2231 Regarding the ability to manipulate the time information and the response in forensic investigations, see: *Gladyshev/Patel*, Formalizing Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1. Regarding dynamic time analysis, see: *Weil*, Dynamic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

2232 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

2233 *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2234 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

2235 See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

2236 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2237 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2238 For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

2239 Regarding the related procedural instrument, see: Art. 19, paragraph 3 Convention on Cybercrime.

2240 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 12.

2241 *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf. With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2242 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2243 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 62.

2244 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

2245 See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801, for further reference

2246 Taylor, The Council of Europe Cybercrime Convention – A civil liberties perspective, available at http://crime-research.org/library/CoE_Cybercrime.html; Cybercrime: Lizenz zum Schnueffeln Financial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at www.ccc.de.

2247 See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 *et seq.*

2248 Regarding the possibilities of making reservations, see Article 42 of the Convention on Cybercrime:
Article 42
By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

2249 See above: § 5.2.1.

2250 "Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

2251 "There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under

applicable international human rights instruments." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

2252 For the transformation of safeguards for Internet-related investigation techniques, see: *Taylor*, The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/taylor.pdf.

2253 This is especially relevant with regard to the protection of the suspect of an investigation.

2254 See: Article 37 – Accession to the Convention.

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2255 ABA International Guide to Combating Cybercrime, page 139.

2256 "Interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" – Case of Kruslin v. France, Application No. 11801/85.

2257 "The requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly", Case of Malone v. United Kingdom, Application No. 8691/79.

2258 "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

2259 "The expression "in accordance with the law", within the meaning of Article 8 § 2 (Art. 8-2), requires firstly that the impugned measure should have some basis in domestic law", Case of Kruslin v. France, Application No. 11801/85.

2260 "Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject", Case of Doerga v. The Netherlands, Application No. 50210/99.

2261 "It also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law", Case of Kruslin v. France, Application No. 11801/85.

"Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence." Case of Malone v. United Kingdom, Application No. 8691/79.

2262 "The cardinal issue arising under Article 8 (Art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (Art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

2263 "Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

2264 The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

2265 "National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of

particular conditions and safeguards." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 147.

2266 See below: § 6.2.9.

2267 See below: § 6.2.10.

2268 "Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 230.

2269 See below: § 6.3.4.

2270 See below: § 6.3.7.

2271 As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorizes the law-enforcement agencies to prevent the deletion of the relevant data. The advantage of separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application.

2272 A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 of the Convention on Cybercrime.

2273 A definition of the term "computer data" is provided in Art. 1 of the Convention on Cybercrime.

2274 As described more in detail below, the differentiation between "computer data" and "subscriber information" in Art. 18 of the Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.

2275 "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 155. Regarding the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*

2276 *Gercke*, Preservation of User Data, DUD 2002, 578.

2277 The cost issue was especially raised within the discussion on data retention legislation in the EU. See, for example: E-communications service providers remain seriously concerned with the agreement reached by European Union Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005, available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

2278 Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2279 The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report of the Workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001. A similar discussion took place during the negotiation of the Convention on Cybercrime. The drafters explicitly pointed out that the Convention does not establish a data retention obligation. See Explanatory Report to the Convention on Cybercrime, No. 151, available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

2280 Regarding The Data Retention Directive in the European Union, see: *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1, available at: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

2281 Art. 6 Periods of Retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.
Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2282 See: Preface 11 of the European Union Data Retention Directive: "Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."

2283 Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2284 See, for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes – Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US, see: ABA International Guide to Combating Cybercrime, page 59.

2285 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2286 However, it is recommended that states consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

2287 *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2288 See: *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

2289 "Preservation" requires that data which already exists in a stored form be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

2290 Explanatory Report, No. 152.

2291 Regarding the advantages of a system of graded safeguards, see above: § 6.3.3.

2292 "The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)". See Explanatory Report to the Convention on Cybercrime, No. 160.

2293 The drafters of the Convention on Cybercrime tried to approach the problems related to the need for immediate action from law-enforcement agencies on the one hand and the importance of ensuring safeguards on the other in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law-enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime, No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

2294 *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2295 An IP address does not necessary immediately identify the offender. If law-enforcement agencies know the IP address an offender used to commit an offence, this information only enables them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café), further investigations are necessary to identify the offender.

2296 If the offender is using services that do not require a registration or if the subscriber information provided by the user is not verified, Art. 18 Subparagraph 1b) will not enable the law-enforcement agencies to immediately identify the offender. Art. 18 Subparagraph 1b) is therefore especially relevant with regard to commercial services (like providing Internet access, commercial e-mail or hosting services).

2297 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2298 "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

2299 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2300 Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.
Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

2301 The Commonwealth Model Law contains an alternative provision:

"Sec. 16: If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:
(a) the service providers; and
(b) the path through which the communication was transmitted."

2302 For an introduction to data retention, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*; *Blanchette/Johnson*, Data retention and the panoptic society: The social benefits of forgetfulness, available at: http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

2303 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

2304 Judgement in Joined Cases C-293/12 and C-594/12.

2305 See, for example: Briefing for the Members of the European Parliament on Data Retention, available at: www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: www.vibe.at/aktionen/200205/data_retention_30may2002.pdf. Regarding the concerns relating to violation of the European Convention on Human Rights, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

2306 See: Heise News, 13 000 determined to file suit against data retention legislation, 17.11.2007, available at: www.heise.de/english/newsticker/news/99161/from/rss09.

2307 Case C-275/06.

2308 See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

2309 In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

2310 Regarding the challenges for law-enforcement agencies related to the use of means of anonymous communication, see above: § 3.2.12.

2311 Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

2312 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2313 See: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

2314 Regarding the impact of use of anonymous communication technology on the work of law-enforcement agencies, see above: § 3.2.12.

2315 Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2316 Regarding protection of the use of anonymous means of communication by the United States constitution, see: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 82, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

2317 Judgement in Joined Cases C-293/12 and C-594/12.

2318 A detailed overview of the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.* Regarding remote live search and possible difficulties with regard to the principle of chain of custody, see: *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law and Technology Vol. 9, Issue 2, 2005, available at: www.lawtechjournal.com/articles/2005/05_051201_Kenneally.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2319 Regarding the involvement of computer forensic experts in investigations, see above: § 6.3.2.

2320 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2321 See below: § 6.3.12.

2322 Apart from the fact that direct access enables the law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2323 See Explanatory Report to the Convention on Cybercrime, No. 184.

2324 "However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data." Explanatory Report to the Convention on Cybercrime, No. 184.

Regarding the special demands with regard to computer-related search and seizure procedures, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2325 Explanatory Report, No. 184.

2326 Regarding the difficulties of online search procedures, see below: § 6.3.12.

2327 See in this context: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

2328 Regarding the requirements in the US, see for example: *Brenner*, Michigan Telecommunications and Technology Law Review, 2001-2002, Vol. 8, page 41 *et seq.*; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2329 "However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record." Explanatory Report to the Convention on Cybercrime, No. 187.

2330 *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2331 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2332 The importance of being able to extend the search to connected computer systems was already addressed by Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the recommendation is available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf.

2333 In this context, it is important to keep in mind the principle of national sovereignty. If the information is stored on a computer system outside the territory, an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be in its territory"– Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue, see also: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2334 For guidelines how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2335 Regarding the classification of the act of copying the data, see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*

2336 "Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data". Explanatory Report to the Convention on Cybercrime, No. 197.

2337 This principle also applies with regard to the seizure of hardware. Compared to maintaining the integrity of copied data it is often easier to maintain the integrity of data on a storage device.

2338 See above: § 2.6.

2339 One possibility to prevent access to the information without deleting it is the use of encryption technology.

2340 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

2341 The fact that law-enforcement agencies are able to access certain data stored outside the country through a computer system in their territory does not automatically legalize the access. See Explanatory Report to the Convention on Cybercrime, No. 195. "This article does not address 'transborder search and seizure', whereby States

could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation." Two cases of transborder access to stored computer data are regulated in Art. 32 Convention on Cybercrime:
Article 32 – Trans-border access to stored computer data with consent or where publicly available
A Party may, without the authorisation of another Party:
a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

2342 "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of com puter operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

2343 "A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data." Explanatory Report to the Convention on Cybercrime, No. 201.

2344 Explanatory Report to the Convention on Cybercrime, No. 202.

2345 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2346 Official Note: If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.

2347 Official Note: A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self-incrimination.

2348 Regarding the motivation of the drafters, see Explanatory Report to the Convention on Cybercrime, No. 171.

2349 "A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability." Explanatory Report to the Convention on Cybercrime, No. 171.

2350 Explanatory Report to the Convention on Cybercrime, No. 173.

2351 "At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement." Explanatory Report to the Convention on Cybercrime, No. 173.

2352 Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication, see above: § 3.2.12.

2353 If the providers offer their service free of charge, they do often either require an identification of the user nor do at least not verify the registration information.

2354 See above: § 6.3.5.

2355 Explanatory Report to the Convention on Cybercrime, No. 172.

2356 This can be, for example, information that was provided on a classic registration form and kept by the provider as paper records.

2357 The Explanatory Report even points out that the parties to the Convention can adjust their safeguards with regard to specific data within each of the categories. See Explanatory Report to the Convention on Cybercrime, No. 174: "Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

2358 For example, the requirement of a court order.

2359 The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 21) shows that the drafters of the Convention realized the importance of separating instruments with different impact.

2360 See below: § 6.3.9.

2361 See below: § 6.3.10.

2362 Art. 21 of the Convention on Cybercrime obliges the signatory states to implement the possibility to intercept content data only with regard to serious offences ("Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law"). On the contrary, Art. 20 of the Convention on Cybercrime is not limited to serious offences. "Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

2363 Regarding the advantages of a graded system of safeguards, see above: § 6.3.3.

2364 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2365 Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

2366 Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel, see: Legal Opinion on Intercept Communication, 2006, available at: www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

2367 In these cases, other technical solutions for surveillance need to be evaluated. Regarding possible physical surveillance techniques, see: *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997, page 384 *et seq.*

2368 Regarding the interception of VoIP to assist law-enforcement agencies, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2369 Regarding the interception of VoIP to assist law-enforcement agencies, see: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 48, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.htm; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006,

available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2370 In particular, lack of technical preparation of Internet providers to collect the relevant data in real time.

2371 Explanatory Report to the Convention on Cybercrime, No. 205.

2372 ABA International Guide to Combating Cybercrime, page 125.

2373 ABA International Guide to Combating Cybercrime, page 125.

2374 The "origin" refers to a telephone number, Internet protocol (IP) address or similar identification of a communications facility to which a service provider renders services. Explanatory Report to the Convention on Cybercrime, No. 30.

2375 "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in cybercrime investigations, see also: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 *et seq.*

2376 "In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a))." Explanatory Report to the Convention on Cybercrime, No. 223.

2377 The Convention does not define technical standards regarding the design of such an interface. Explanatory Report to the Convention on Cybercrime, No. 220.

2378 Explanatory Report to the Convention on Cybercrime, No. 223.

2379 "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Explanatory Report to the Convention on Cybercrime, No. 221.

2380 See above: § 3.2.12.

2381 Tor is a software that enables users to protect against traffic analysis. For more information about the software, see: http://tor.eff.org/.

2382 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request an identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2383 This advantage is also relevant for remote forensic investigations. See below: § 6.3.12.

2384 Such obligation might be legal or contractual.

2385 Explanatory Report to the Convention on Cybercrime, No. 226.

2386 Regarding the key intention, see Explanatory Report on the Convention on Cybercrime No. 16: "The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation."

2387 The drafters of the Convention point out that the signatory states should limit the use of the right to make reservations in this context: Explanatory Report to the Convention on Cybercrime, No. 213.

Regarding the possibilities of making reservations, see Art. 42 Convention on Cybercrime:
Article 42
By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails

itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No. other reservation may be made.

2388 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at:

www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers,* Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2389 One possibility to prevent law-enforcement agencies from analysing the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures, see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

2390 Regarding the impact of encryption technology on computer forensic and criminal investigations, see: *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge, see below: § 6.3.11.

2391 *Schneier*, Applied Cryptography, page 185.

2392 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2393 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

2394 *Schneier*, Applied Cryptography, page 185.

2395 Regarding practical approaches to recover encrypted evidence, see: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at:

2396 The issue is, for example, addressed by Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with information, 11 September 1995: "14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary" and the G8 in the 1997 Meeting in Denver: "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines. Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies."

2397 For more information, see: *Koops*, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

2398 The need for such authorization is mentioned, for example, in principle 6 of the 1997 Guidelines for Cryptography Policy: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

2399 This topic was discussed in the deliberations of the US District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow law-enforcement agencies to make use of a software to record keystrokes on a suspect's computer (keylogger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers). See: www.epic.org/crypto/scarfo/opinion.html.

2400 Export limitations on encryption software capable of processing strong keys are not designed to facilitate the work of law-enforcement agencies in the country. The intention of such regulations is to prevent the availability of the technology outside the country. For detailed information on import and export restrictions with regard to encryption technology, see: http://rechten.uvt.nl/koops/cryptolaw/index.htm.

2401 The limitation of the import of such powerful software is even characterized as "misguided and harsh to the privacy rights of all citizens". See, for example: The Walsh Report – Review of Policy relating to Encryption Technologies 1.1.16 available at: www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

2402 See: *Lewis*, Encryption Again, available at: www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

2403 The key escrow system was promoted by the United States Government and implemented in France for a period in 1996. For more information, see: Cryptography and Liberty 2000 – An International Survey of Encryption Policy, available at: http://www2.epic.org/reports/crypto2000/overview.html#Heading9.

2404 See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 *et seq.*

2405 "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management. which may allow, consistent with these guidelines. lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies", www.g7.utoronto.ca/summit/1997denver/formin.htm.

2406 See, for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf; Australia, Cybercrime Act, Art. 12, available at: http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf; Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at: http://staatsbladclip.zita.be/staatsblad/wetten/2001/02/03/wet-2001009035.html; France, Loi pour la confiance dans l'économie numérique, Section 4, Art. 37, available at: www.legifrance.gouv.fr/affichTexte.do;jsessionid=B78A2A8ED919529E3B420C082708C031.tpdjo12v_3?cidTexte=JORFTEXT000000801164&dateTexte=20080823; United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at: www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative à l'échange électronique de données juridiques, Chapter III, available at: http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/; Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: www.info.gov.za/gazette/acts/2002/a70-02.pdf; Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

2407 An example can be found in Sec. 69 of the Indian Information Technology Act 2000: "Directions of Controller to a subscriber to extend facilities to decrypt information.(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." For more information about the Indian Information Technology Act 2000, see: *Duggal*, India's Information Technology Act 2000, available under: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf.

2408 For general information on the Act, see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses, available at: www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

2409 For an overview of the regulation, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2410 Regarding the discussion of protection against self-incrimination under United States law, see for example: *Clemens*, No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private key, UCLA Journal of Law and Technology, Vol. 8, Issue 1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: www.richmond.edu/jolt/v2i1/sergienko.html; *O'Neil*, Encryption and the First Amendment, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art1.pdf; *Fraser*, The Use of Encrypted, Coded and Secret Communication is an "Ancient Liberty" Protected by the United States Constitution, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art2.pdf; *Park*, Protecting the Core

Values of the First Amendment in an age of New Technology: Scientific Expression vs. National Security, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art3.pdf; Hearing before the Subcommittee
on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary, United States Senate, 150 Congress, Second Session on Examining the Use of Encryption, available at: www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe on self-incrimination, in particular with regard to the European Convention on Human Rights (ECHR), see: *Moules*, The Privilege against self-incrimination and the real evidence, The Cambridge Law Journal, 66, page 528 *et seq.*; *Mahoney*, The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR, Judicial Studies Institute Journal, 2004, page 107 *et seq.*; *Birdling*, Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom, International Journal of Evidence and Proof, Vol. 12, Issue 1, 2008, page 58 *et seq.*; Commission of the European Communities, Green Paper on the Presumption of Innocence, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:pdf.

2411 Regarding the situation in the US, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

2412 In this context, see also: *Walker*, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: www.bileta.ac.uk/01papers/walker.html.

2413 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2414 Regarding possibilities to circumvent the obligations, see: *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm.

2415 A detailed overview of the elements of search procedures as well as the challenges of carrying them out is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.*

2416 Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an ongoing investigation based on Art. 20 confidential, see above: § 6.3.9.

2417 There are disadvantages related to remote investigations. Apart from the fact that direct access enables law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system it is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2418 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2419 See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.200, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm;

Abreu, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

2420 See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: www.heise-security.co.uk/news/92950.

2421 Computer and Internet protocol address verifier.

2422 A copy of the search warrant is available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search, see: www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf. For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2423 Regarding the discussion in Germany, see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware "specialists" to bug terrorists, The Register, 21.11.2007, available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: www.spiegel.de/international/germany/0,1518,502955,00.html.

2424 See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: www.tagesspiegel.de/politik/;art771,1989104.

2425 For an overview, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

2426 The search function was the focus of the decision of the German Supreme Court in 2007. See: Online police searches found illegal in Germany, 14.02.2007, available at: www.edri.org/edrigram/number5.3/online-searches.

2427 Regarding investigations involving VoIP, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2428 See: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf. Keylogging is the focus of the FBI software "magic lantern". See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf. See also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

2429 This is the focus of the US investigation software CIPAV. Regarding the functions of the software, see the search warrant, available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf.

2430 Regarding these functions, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

2431 Regarding the possible ways of infecting a computer system by spyware, see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

2432 With regard to the efficiency of virus scanners and protection measures implemented in the operating systems, it is likely that the functioning of a remote forensic software would require the cooperation of software companies. If

software companies agree to prevent detection of remote forensic software, this could result in serious risks for computer security. For more information, see: *Gercke*, Computer und Recht 2007, page 249.

2433 If the offender stores illegal content on an external storage device that is not connected to a computer system, the investigators will in general not be able to identify the content if they only have access to the computer system via remote forensic software.

2434 Regarding the importance of maintaining integrity during a forensic investigation, see: *Hosmer*, Providing the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2435 National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2436 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2437 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2438 See above: § 3.2.12.

2439 Based on Art. 7, "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electrnic data transmission or other communications, are made available to the public, to customers or members" is obliged to require a licence from local authorities and identify persons using the service. For more information, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

2440 Decree 144/2005, 27 July 2005 ("Decreto-legge"). Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article, Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2441 For more details, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

2442 *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

2443 Regarding the related challenges, see: *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

2444 International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005.

2445 *Büllingen/Gillet/Gries/Hillebrand/Stamm*, Situation and Perspectives of Data Retention in an international comparison (Stand und Perspectiven der Vorratsdatenspeichung im internationalen Vergleich), 2004, page 10, available at: www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

2446 *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

2447 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

2448 See above: § 3.2.7.

2449 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2450 See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2451 *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

2452 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

2453 The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

2454 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

2455 The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

2456 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

2457 European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

2458 Council of Europe Convention on Cybercrime, ETS 185.

2459 See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2460 A full list of agreements is available at: www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

2461 Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

2462 See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, page 119.

2463 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.

2464 *Choo,* Trends in Organized Crime, 2008, page 273.

2465 *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4, page 27.

2466 See, for example: Great Britain Crown Prosecution Service, Convictions for internet rape plan, Media release, 01.12.2006.

2467 *Choo,* Trends in Organized Crime, 2008, page 273.

2468 For further details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2469 According to the report of the expert meeting held between 8 and 10 October 2008, there are certain states which require special provisions in their internal law to allow such spontaneous information, while others can transmit information spontaneously without such internal provisions in force: see CTOC/COP/2008/18 page 5.

2470 For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 226, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2471 For details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 225, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2472 See, for example, Art. 29 and Art. 35 Convention on Cybercrime.

2473 The directory is available at: www.unodc.org/compauth/en/index.html. Access requires registration and is reserved for competent national authorities.

2474 The directory indicates the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific requests of the receiving states and sometimes even extracts from domestic legislation of that state.

2475 See CTOC/COP/2008/18, paragraph 27.

2476 See Art. 25, paragraph 3 of the Convention on Cybercrime.

2477 The software is available at: www.unodc.org/mla/index.html.

2478 See Explanatory Report to the Convention on Cybercrime, No. 243. The Member States have the possibility to limit the international cooperation with regard to certain measures (extradition, real time collection of traffic data and the interception of content data).

2479 If, for example, two countries involved in a cybercrime investigation already have bilateral agreements in place that contain the relevant instruments, those agreements will remain a valid basis for the international cooperation.

2480 Regarding the difficulties with the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

2481 The Explanatory Report clarifies that the determination of the covered offences does not depend on the actual penalty imposed in the particular cases. See: Explanatory Report to the Convention on Cybercrime, No. 245.

2482 Regarding the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

2483 See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

2484 See above: § 3.2.10.

2485 See Explanatory Report to the Convention on Cybercrime, No. 256.

2486 This information often leads to successful international investigations. For an overview of large-scale international investigations related to child pornography, see: *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296, page 4, available at: www.ecpat.se/upl/files/279.pdf.

2487 Similar instruments can be found in other Council of Europe conventions. For example, Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 28 of the Criminal Law Convention on Corruption. Council of Europe conventions are available at: www.coe.int.

2488 See Explanatory Report to the Convention on Cybercrime, No. 262.

2489 Regarding the 24/7 network points of contact, see below: § 6.4.12.

2490 See Explanatory Report to the Convention on Cybercrime, No. 265: "Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to

satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly."

2491 See Explanatory Report to the Convention on Cybercrime, No. 268.

2492 See Explanatory Report to the Convention on Cybercrime, No. 269. "Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal."

2493 See Explanatory Report to the Convention on Cybercrime, No. 269.

2494 See above: § 6.3.

2495 The most important instruments established by the Convention on Cybercrime are: Expedited preservation of stored computer data (Art. 16), Expedited preservation and partial disclosure of traffic data (Art. 17), Production order (Art. 18), Search and seizure of stored computer data (Art. 19), Real-time collection of traffic data (Art. 20), Interception of content data (Art. 21).

2496 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2497 An exemption is Art. 32 of the Convention on Cybercrime – See below. Regarding the concerns related to this instrument, see: Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: " […] Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32b in particular in the light of experience gained from the use of this Article).

2498 See above: § 6.3.4.

2499 See above: § 6.3.4.

2500 See above: § 6.3.7.

2501 See above: § 6.3.6.

2502 See above: § 6.3.9.

2503 See above: § 6.3.10.

2504 See Explanatory Report to the Convention on Cybercrime, No. 293.

2505 "The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules." See Explanatory Report to the Convention on Cybercrime, No. 293.

2506 See below in this chapter.

2507 See Explanatory Report to the Convention on Cybercrime, No. 293.

2508 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

2509 See: Challenges and Best Practices in Cybercrime Investigation, 2008, available at: www.unafei.or.jp/english/pdf/PDF_rms/no79/15_P107-112.pdf.

2510 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2511 For more information, see: A Draft Commentary on the Council of Europe Convention, October 2000, available at: www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf.

2512 In this context, it is necessary to point out a difference between Art. 32 and Art. 18. Unlike Art. 18, Art. 32 does not enable a foreign law-enforcement agency to order the submission of the relevant data. It can only seek permission.

2513 Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, 19-20 October 1999.

2514 Principles on Transborder Access to Stored Computer Data, available at: www.justice.gov/criminal/cybercrime/g82004/99TransborderAccessPrinciples.pdf.

2515 The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator

or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

2516 See above: § 6.3.4.

2517 Availability 24 hours a day and 7 days a week is especially important with regard to the international dimension of cybercrime, as requests can potentially come from any time zone in the world. Regarding the international dimension of cybercrime and the related challenges, see above: § 3.2.6.

2518 See Explanatory Report to the Convention on Cybercrime, No. 298.

2519 Regarding the activities of the G8 in the fight against cybercrime, see above: § 5.1.1. For more information on the 24/7 Network, see: *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 484, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.

2520 See above: § 3.2.10.

2521 See above: § 3.2.6.

2522 Regarding the question of which authorities should be authorized to order the preservation of data, see above: § 6.3.4.

2523 Explanatory Report to the Convention on Cybercrime, No. 301.

2524 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

2525 *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf.

2526 The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

2527 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

2528 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

2529 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

2530 Regarding the network architecture and the consequences with regard to the involvement of service providers, see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003, available at: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

2531 See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

2532 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2533 For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2534 In the decision Recording Industry Association Of America v. Charter Communications, Inc., the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the United States DMCA by pointing out the balance. In the opinion of the court, DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

2535 Regarding the history of DMCA and pre-DMCA case law in the United States, see: *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Salow*, Liability Immunity for Internet Service Providers – How is it working?, Journal of Technology Law and Policy, Vol. 6, Issue 1, 2001, available at: http://grove.ufl.edu/~techlaw/vol6/issue1/pearlman.html.

2536 Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html.

2537 Regarding the application of DMCA to search engines, see: *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

2538 17 USC. § 512(a)

2539 17 USC. § 512(b)

2540 Regarding the Communications Decency Act, see: *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf;

2541 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union e-commerce regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*, available at: www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

2542 See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

2543 Art. 12 – Art. 15 EU of the E-Commerce Directive.

2544 With the number of different services covered, the E-Commerce Directive aims for a broader regulation than 17 USC. § 517(a). Regarding 17 USC. § 517(a).

2545 See Art. 12 paragraph 3 of the E-Commerce Directive.

2546 The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2547 Regarding traditional caching as well as active caching, see: *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

2548 For more information on proxy servers, see: *Luotonen*, Web Proxy Servers, 1997.

[2549] The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2550] See above: § 6.5.4.

[2551] Regarding the impact of free webspace on criminal investigations, see: *Evers*, Blogging sites harbouring cybercriminals, CNET News, 26.07.2005, available at: http://news.zdnet.co.uk/security/0,1000000189,39210633,00.htm.

[2552] This procedure is called "notice and takedown".

[2553] The hosting provider is quite often in a difficult situation. On the one hand, it needs to react immediately to avoid liability; on the other hand, it has certain obligations to its customers. If it removes legal information that was just at first sight illegal, this could lead to claims for indemnity.

[2554] By enabling their customers to offer products, they provide the necessary storage capacity for the required information.

[2555] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2556] See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2557] See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2558] *Spindler*, Multimedia und Recht 1999, page 204.

[2559] Art. 21 – Re-examination

1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.
2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, 'notice and take down' procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

[2560] *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

[2561] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[2562] See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[2563] § 17 – Ausschluss der Verantwortlichkeit bei Links

(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

[2564] *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, page 5, available at: www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

[2565] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[2566] See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[2567] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) – Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (Spain)

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No. tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

[2568] Ausschluss der Verantwortlichkeit bei Suchmaschinen

§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er

1. die Übermittlung der abgefragten Informationen nicht veranlasst,
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Union internationale des telecommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau du Directeur
Place des Nations
CH-1211 Genève 20 – Suisse
Courriel: bdtdirector@itu.int
Tél.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Adjoint au directeur et
Chef du Département de
l'administration et de la
coordination des opérations (DDR)
Courriel: bdtdeputydir@itu.int
Tél.: +41 22 730 5784
Fax: +41 22 730 5484

Département de l'environnement
propice aux infrastructures et
aux cyberapplications (IEE)
Courriel: bdtiee@itu.int
Tél.: +41 22 730 5421
Fax: +41 22 730 5484

Département de l'innovation et des
partenariats (IP)
Courriel: bdtip@itu.int
Tél.: +41 22 730 5900
Fax: +41 22 730 5484

Département de l'appui aux projets et
de la gestion des connaissances (PKM)
Courriel: bdtpkm@itu.int
Tél.: +41 22 730 5447
Fax: +41 22 730 5484

Afrique

Ethiopie

International Telecommunication
Union (ITU)
Bureau régional
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopie

Courriel: itu-addis@itu.int
Tél.: +251 11 551 4977
Tél.: +251 11 551 4855
Tél.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroun

Union internationale des
telecommunications (UIT)
Bureau de zone de l'UIT
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Courriel: itu-yaounde@itu.int
Tél.: + 237 22 22 9292
Tél.: + 237 22 22 9291
Fax: + 237 22 22 9297

Sénégal

Union internationale des
telecommunications (UIT)
Bureau de zone de l'UIT
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

Courriel: itu-dakar@itu.int
Tél.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication
Union (ITU)
Bureau de zone
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 4 77 5939
Tél.: +263 4 77 5941
Fax: +263 4 77 1257

Amériques

Brésil

União Internacional de
Telecomunicações (UIT)
Bureau régional
SAUS Quadra 06, Bloco "E"
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Courriel: itubrasilia@itu.int
Tél.: +55 61 2312 2730-1
Tél.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

La Barbade

International Telecommunication
Union (ITU)
Bureau de zone
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Courriel: itubridgetown@itu.int
Tél.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chili

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chili

Courriel: itusantiago@itu.int
Tél.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Courriel: ituteguciglapa@itu.int
Tél.: +504 22 201 074
Fax: +504 22 201 075

Etats arabes

Egypte

International Telecommunication
Union (ITU)
Bureau régional
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypte

Courriel: itucairo@itu.int
Tél.: +202 3537 1777
Fax: +202 3537 1888

Asie-Pacifique

Thaïlande

International Telecommunication
Union (ITU)
Bureau régional
Thailand Post Training
Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thaïlande

Adresse postale:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thaïlande

Courriel: itubangkok@itu.int
Tél.: +66 2 575 0055
Fax: +66 2 575 3507

Indonésie

International Telecommunication
Union (ITU)
Bureau de zone
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonésie

Adresse postale:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonésie

Courriel: itujakarta@itu.int
Tél.: +62 21 381 3572
Tél.: +62 21 380 2322
Tél.: +62 21 380 2324
Fax: +62 21 389 05521

Pays de la CEI

Fédération de Russie

International Telecommunication
Union (ITU)
Bureau de zone
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie

Adresse postale:
P.O. Box 25 – Moscow 105120
Fédération de Russie

Courriel: itumoskow@itu.int
Tél.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Suisse

Union internationale des
télécommunications (UIT)
Bureau de développement des
télécommunications (BDT)
Unité Europe (EUR)
Place des Nations
CH-1211 Genève 20 – Suisse
Courriel: eurregion@itu.int
Tél.: +41 22 730 5111

Union internationale des télécommunications
Bureau de Développement des Télécommunications
Place des Nations
CH-1211 Genève 20
Suisse
www.itu.int

ISBN 978-92-61-15642-8 SAP id 39678

Imprimé en Suisse
Genève, 2014

11/2014