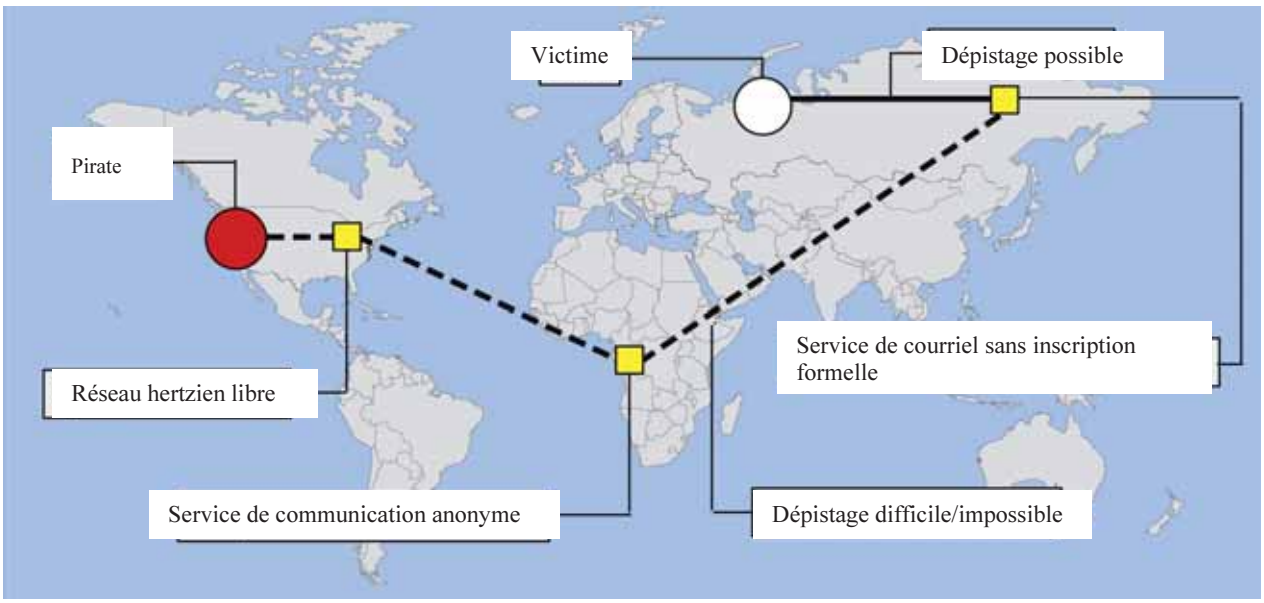
Union internationale des télécommunications

Ressources sur la législation relative à la cybercriminalité



COMPRENDRE LA CYBERCRIMINALITE: GUIDE POUR LES PAYS EN DEVELOPPEMENT

Division applications TIC et cybersécurité
Département des politiques et stratégies
Secteur du développement des télécommunications de l'UIT

Projet de document – avril 2009

Pour de plus amples informations, veuillez contacter la
Division applications TIC et cybersécurité de l'UIT-D à l'adresse cybmail@itu.int

Union internationale des télécommunications

Remerciements

Le présent rapport a été réalisé à la demande de la Division applications TIC et cybersécurité du Secteur du développement des télécommunications de l'UIT.

Comprendre la cybercriminalité: Guide pour les pays en développement a été élaboré par Marco Gercke. L'auteur remercie l'équipe du Secteur du développement des télécommunications de l'UIT pour son soutien et Gunhild Scheer pour les échanges de vues très productifs.

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, sous quelque forme et par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

Les dénominations et classifications employées dans le présent rapport n'impliquent l'expression d'aucune opinion de la part de l'Union internationale des télécommunications concernant le statut juridique ou autre de tel ou tel territoire, ni l'acceptation ou l'approbation d'une quelconque frontière. Le terme "pays" utilisé dans le présent rapport désigne un pays ou un territoire.

La publication Comprendre la cybercriminalité: Guide pour les pays en développement de l'UIT est disponible en ligne à l'adresse:

www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Le présent document est formaté pour une impression en recto-verso. Il n'a pas été revu par les services d'édition.

Pour de plus amples informations, veuillez contacter:

Division applications TIC et cybersécurité (CYB)
Département des politiques et stratégies
Bureau de développement des télécommunications
Union internationale des télécommunications
Place des Nations
1211 Genève 20
Suisse
Tél.: +41 22 730 5825/6052
Fax: +41 22 730 5484
Courriel: cybmail@itu.int
Site Internet: www.itu.int/ITU-D/cyb/

Déni de responsabilité

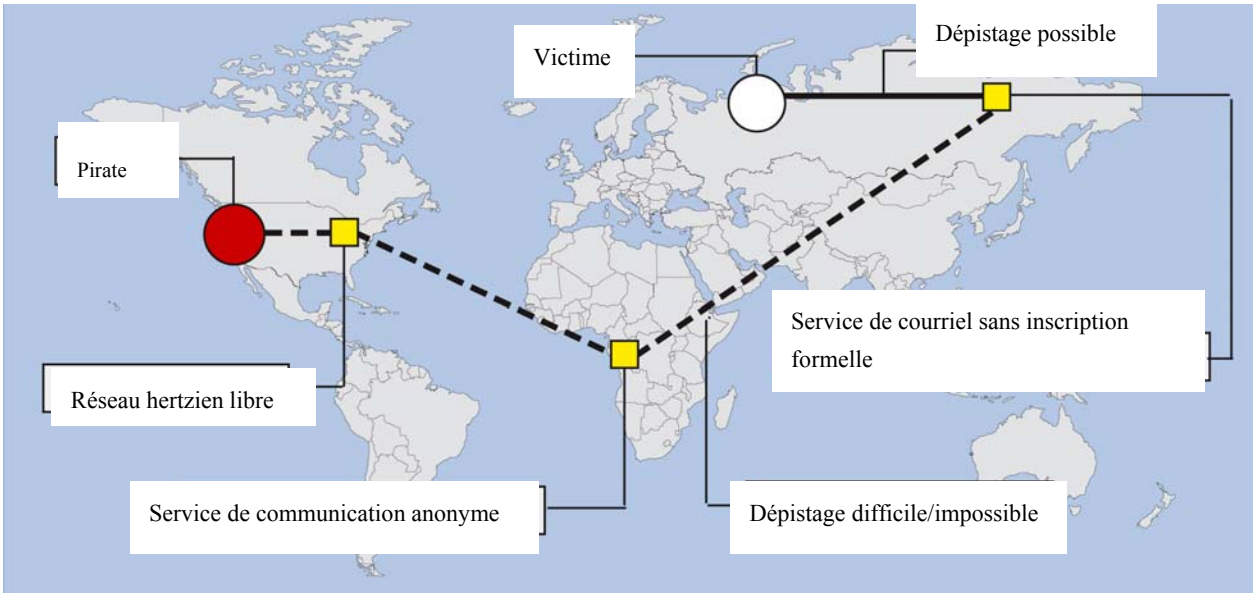
Les opinions exprimées dans cette publication sont celles de l'auteur ou des auteurs et ne représentent pas nécessairement les points de vue de l'Union internationale des télécommunications (UIT) ou de ses membres. Les désignations utilisées et la présentation des données, y compris des cartes, n'impliquent, de la part de l'UIT, aucune prise de position quant au statut juridique de tel ou tel pays, territoire, ville ou zone, ni quant au tracé de ses frontières ou limites. La mention de pays, de sociétés, de produits, d'initiatives ou de directives, ou la référence à ceux-ci, n'entraîne, de la part de l'UIT, aucune approbation ou recommandation de ces pays, sociétés, produits, initiatives ou directives de préférence à d'autres de nature analogue qui ne sont pas cités.

© UIT 2009

Avant d'imprimer ce rapport, pensez à l'environnement.

Union Internationale des Télécommunications

Ressources sur la législation relative à la cybercriminalité



COMPRENDRE LA CYBERCRIMINALITÉ: GUIDE POUR LES PAYS EN DÉVELOPPEMENT

Division applications TIC et cybersécurité
Département des politiques et stratégies
Secteur du développement des télécommunications de l'UIT

Projet de document – avril 2009

Pour de plus amples informations, veuillez contacter la
Division applications TIC et cybersécurité de l'UIT-D à l'adresse cybmail@itu.int

Union internationale des télécommunications

SIGLES ET ACRONYMES

ABA	Association du barreau américain
ANASE	Association des nnations de l'Asie du Sud-Est
APEC	Coopération économique pour l'Asie-Pacifique
APIG	*All Party Internet Group*
CdE	Conseil de l'Europe
CE	Commission européenne
CFAA	*Computer Fraud and Abuse Act* (Etats-Unis)/loi relative à la fraude informatique et à l'utilisation abusive de l'informatique
CMA	*Computer Misuse Act* (Royaume-Uni) *& Computer Misuse Act* (Singapour)/loi relative à l'utilisation abusive de l'informatique
DDoS	Attaque par refus de service
ECPA	*Electronic Communications Privacy Act* (Etats-Unis)/loi relative à la vie privée concernant les communications électroniques
G8	Groupe des huit
GCA	Programme mondial cybersécurité
GEE	Groupe d'entraide internationale (Canada)
IRG	*Gesetz über die Internationale Rechtshilfe in Strafsachen*
OCDE	Organisation de coopération et de développement économiques
OWig	*Gesetz über Ordnungswidrigkeiten* (Allemagne)
ONU	Organisation des Nations Unies
PACC	*ABA Privacy & Computer Crime Committee*/comité pour la défense de la vie privée et la lutte contre la criminalité de l'ABA
Réglementations CE	Réglementations relatives aux communications privées et électroniques 2003 (Royaume-Uni)
RIPA	*Regulation of Investigatory Powers Act* (Royaume-Uni)/loi sur la réglementation des pouvoirs d'enquête
RU	Royaume-Uni
SMSI	Sommet mondial sur la société de l'information
StGB	Code pénal allemand (*Strafgesetzbuch*)
StPO	Code de procédure pénale allemand (*Strafprozessordnung*)
TIC	Technologies de l'information et de la communication
TKG	Loi allemande relative aux télécommunications (*Telekommunikationgesetz*)
UE	Union européenne
UIT	Union internationale des télécommunications
UrhG	Loi allemande relative au droit à la propriété intellectuelle (*Urheberrechtsgesetz*)
USD	dollars américains

OBJECTIF

L'ouvrage **Comprendre la cybercriminalité: Guide pour les pays en développement** de l'UIT se propose d'aider les pays intéressés à comprendre les aspects juridiques de la cybercriminalité et de contribuer à l'harmonisation des cadres juridiques. Dès lors, il vise à aider les pays en développement 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 aider ces pays à construire un cadre juridique solide.

Ce guide propose une vue d'ensemble complète 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. Le guide fournit un grand nombre de ressources, qui 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 guide 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 guide 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.

Comprendre la cybercriminalité: **Guide pour les pays en développement** 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. 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.

TABLE DES MATIÈRES

1 Introduction

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 ..., 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), de nombreux pays en développement peuvent, plus facilement que jamais, 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

---

1 Related to 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: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to the ITU, there were 1,13 billion Internet users by the end of 2007, available at: http://www.itu.int/ITU-D/.

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 seqq., available at: http://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 computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. 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: http://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 Within the "One Laptop per Child» initiative, inexpensive laptop computers should be distributed to children, especially those in developing countries. The project is organised by the United States-based non-profit organisation OLPC. For more information, see the official OLPC website at http://www.laptop.org. Regarding the technology of the laptop, see Heise News, Test of the 100 dollar laptop, 09.05.2007, available at: http://www.heise.de/english/newsticker/news/89512.

6 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 http://www.wimaxforum.org; Andrews, Ghosh, Rias, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; Nuaymi, WiMAX, Technology for Broadband Wireless Access.

7 Current reports highlight that less than 4 per cent of the African population has access to the Internet. See Waters, Africa waiting for net revolution, BBC News, 29.10.2007, available at: http://news.bbc.co.uk/1/hi/technology/7063682.stm.

8 Regarding the impact of ICT on the 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 Defence had to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

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 tire des TIC et des nouveaux services en réseau un certain nombre d'avantages.

Les applications TIC (cybergouvernance, commerce électronique, cyberenseignement, cybersanté, cyberenvironnement, etc.), vecteurs efficaces de la fourniture d'une large gamme de services de base dans les régions éloignées et les 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 des 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[12].

Le coût des services en ligne est souvent très inférieur à celui des services comparables hors ligne[13]. Ainsi, contrairement aux services postaux traditionnels, les services de messagerie électronique sont souvent gratuits ou proposés pour une somme modique[14]. L'encyclopédie en ligne Wikipédia[15] est accessible gratuitement, de même que des centaines de services d'hébergement en ligne[16]. 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.

---

10 Regarding the ability to block Internet-based information services by denial-of-service attacks see below 2.4.e.

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

13 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.

14 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: http://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: http://www.email-marketing-reports.com/metrics/email-statistics.htm.

15 http://www.wikipedia.org

16 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: http://www.symantec.com/business/resources/articles/article.jsp?aid=20080513_symantec_reports_malicious_web_attacks_are_on_the_rise.

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"[17], modèle de société qui offre d'immenses possibilités[18]. 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)[19]. 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[20].

Cela étant, l'expansion de la société de l'information s'accompagne de nouveaux dangers et de graves menaces[21]. En effet, des services essentiels, tels que la distribution d'eau et d'électricité, s'appuient aujourd'hui sur les TIC[22]. De même, les voitures, la régulation du trafic, les ascenseurs, la climatisation et le téléphone reposent sur la bonne marche de ces nouvelles technologies[23]. 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[24].

On recense déjà de telles attaques[25]: fraude en ligne, diffusion de contenu pornographique mettant en scène des enfants, opérations de piratage, pour ne citer que quelques exemples d'infractions informatiques commises

---

17 Unlike in the Industrial Society, members of the Information Society are no longer connected by their participation in industrialisation, 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.

18 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.

19 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: http://www.jiti.com/v1n1/white.pdf.

20 Regarding the extend of integration of ICTs into the daily lives and the related threats see below 3.2.a 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.

21 See *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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

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

23 *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 seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf.

24 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: http://www.gao.gov/new.items/d08212t.pdf.

25 Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: http://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: http://www.projects.ncassr.org/hackback/ethics00.pdf.

chaque jour à grande échelle[26]. Les pertes financières dues à la cybercriminalité sont extrêmement élevées[27]. Pour la seule année 2003, les logiciels malveillants ont causé jusqu'à 17 milliards USD de pertes[28]. 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[29]. Presque 60% des entreprises aux Etats-Unis estiment que la cybercriminalité leur coûte plus que les infractions matérielles[30]. Ces estimations le montrent clairement, il est vital de protéger les infrastructures de l'information[31].

1.3 Cybersécurité et cybercriminalité

La cybersécurité[32] joue un rôle essentiel dans le développement des technologies de l'information et des services en ligne[33]. 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[34]. 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 lA d'une responsabilité commune, qui demande de la part des autorités, du secteur privé et de

---

26 The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in one month (August 2007). Source: http://www.hackerwatch.org.

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

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

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

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

31 *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: http://www.gao.gov/new.items/d08212t.pdf.For more information on the economic impact of Cybercrime see below 2.9.

32 The term "Cybersecurity» is used to summarise various activities such as 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 cyber environment 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 cyber environment. 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. Regarding the definition of cybersecurity, 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 cyber environment 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 cyber environment. 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: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc..

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

34 See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://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: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

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 exige donc une approche globale[35]. 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[36]. Il est donc primordial, pour lutter contre la cybercriminalité, de développer et de soutenir les stratégies de cybersécurité[37].

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[38]. A cet égard, le Sommet mondial sur la société de l'information (SMSI)[39] 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*[40], annexe comprise, exposent un plan pour la mise en oeuvre de multi-parties prenantes au niveau international du *Plan d'Action de Genève du SMSI*[41]. 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"[42].

En vertu de ce mandat, le Secrétaire général de l'UIT a lancé, le 17 mai 2007, le Programme mondial cybersécurité (GCA)[43], 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.

---

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

36 For more information see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

37 See: *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf; See as well Pillar One of the ITU Global Cybersecurity Agenda, available at: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html; With regard to the elements of an anti-cybercrime strategy see below: Chapter 4.

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

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

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

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

42 For more information on WSIS action line C5: Building confidence and security in the use of ICTs see: http://www.itu.int/wsis/c5/

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

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, 5) Coopération internationale[44].

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[45]. 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.[46] 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[47]. Il est donc essentiel d'analyser en détail les lois nationales en vigueur afin d'identifier les éventuelles lacunes[48]. Outre les dispositions de fond en droit pénal[49], les instances de répression doivent disposer des mécanismes et des instruments nécessaires pour instruire les affaires de cybercriminalité[50]. L'instruction de ce type d'affaire présente des difficultés[51], 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

---

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

45 For an overview about the most important instruments in the fight against Cybercrime see below: Chapter 6.2.

46 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

47 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 et. Seqq.

48 For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at: http://www.coe.int/cybercrime/. 48 See for example the following surveys on national Cybercrime legislation: 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; Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*. , available at: https://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: http://www.mosstingrett.no/info/legal.html.

49 See below: Chapter 6.1.

50 See below: Chapter 6.1.

51 For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.2.

identité[52]. En conséquence, ces mécanismes et instruments peuvent être assez différents de ceux utilisés pour enquêter sur les infractions classiques[53].

1.4 Dimensions internationales de la cybercriminalité

La cybercriminalité présente souvent une dimension internationale[54]. On notera par exemple que les contenus illicites transmis par courriel transitent souvent par plusieurs pays avant d'atteindre le destinataire. Parfois, ils ne sont pas stockés dans le pays mais à l'étranger[55]. Il est donc essentiel que les Etats concernés par un cyberdélit collaborent étroitement aux enquêtes diligentées[56], 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[57]. Il est donc crucial de réviser les procédures afin de pouvoir rapidement réagir aux incidents et répondre aux demandes de coopération internationale[58].

Dans de nombreux pays, le régime d'entraide judiciaire repose sur le principe de la "double incrimination"[59]. 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 qui peuvent faire l'objet de poursuites n'importe où dans le monde, mais, malgré tout, les différences régionales jouent un rôle important[60]. C'est le cas notamment des

---

52 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 seqq., available at: http://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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Design», 2005.

53 Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.11

54 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.

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

56 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 seqq., 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 seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

57 See below: Chapter 6.3.

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

59 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime», 2005, page 5, available at: http://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. seqq., available at: http://www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

60 See below: Chapter 5.5. See for example the following surveys on national Cybercrime legislation: 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; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: A*n Overview,* CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: http://www.mosstingrett.no/info/legal.html.

infractions pour contenu illicite, qui sont sanctionnées différemment selon les pays[61]: il n'est pas rare que certains contenus légalement autorisés par certains soient jugés illicites par d'autres[62].

Partout dans le monde, l'informatique repose fondamentalement sur la même technologie[63]. 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[64]. C'est aussi pour cette raison que les internautes du monde entier peuvent avoir accès aux mêmes services[65].

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 à la Convention du Conseil de l'Europe sur la cybercriminalité[66], le droit national évolue beaucoup plus lentement que les techniques[67].

Or, si Internet ne connaît pas les contrôles aux frontières, des moyens existent cependant de restreindre l'accès à certaines informations[68]. 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")[69]. Ces deux mesures, certes non sans failles, demeurent des instruments utiles pour préserver des différences territoriales dans un réseau mondial[70]. L'OpenNet Initiative[71] signale qu'une vingtaine de pays environ pratiquent ce type de censure[72].

---

61 The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Convention on Cybercrime, but addressed in an additional protocol. See below: Chapter 2.5.

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

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

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

65 Regarding the technical standardisation 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: http://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. seqq.

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

67 Since parties participating in the negotiation could not agree on a common position on the criminalisation 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.

68 See *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

69 This was for example discussed within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *http://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.*

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

71 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: http://www.opennet.net.

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

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 – particulièrement coûteuses[73] – ainsi que des instruments juridiques[74], dont l'élaboration et la mise en œuvre demandent du temps. 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[75].

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[76]. 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[77].

2 Le phénomène de la cybercriminalité

2.1 Définitions du cyberdélit

La plupart des rapports, guides et publications sur la cybercriminalité commencent par une définition du terme "cyberdélit"[78]. Selon une acception courante, un cyberdélit désigne toute activité mettant en jeu des ordinateurs

---

73 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 http://www.oecd.org/dataoecd/5/47/34935342.pdf.

74 See below: Chapter 4.

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

76 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: http://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 industrialised countries. See OECD: "Spam Issue in Developing Countries», DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

77 For more details about the elements of an anti-cybercrime strategy see below: Chapter 4.

78 Regarding approaches to define and categorise cybercrime see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: http://www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the 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: http://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: http://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: http://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: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1.

ou des réseaux en tant qu'outil, cible ou lieu d'une infraction[79]. Exemple d'approche internationale, l'article 1.1 du projet de convention internationale visant à renforcer la protection contre la cybercriminalité et le terrorisme (CISAC, *Draft International Convention to Enhance Protection from Cyber Crime and Terrorism*)[80]. Cet article souligne que le terme "cybercriminalité" fait référence à des actes qui concernent des cybersystèmes[81]. Certains, tentant de prendre en compte les objectifs ou les intentions de l'auteur de l'infraction, donnent une définition plus précise du cyberdélit[82], à savoir "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*"[83].

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 Convention sur la cybercriminalité du Conseil de l'Europe[84]. Le fait, par exemple, de créer un dispositif USB[85] 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[86]. 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.

---

79 See for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: http://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. seqq.; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

80 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 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: http://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.

81 *Article 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;
[...]

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

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

84 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: Chapter 6.1.; *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 Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *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: http://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*.

85 Universal Serial Bus (USB)

86 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.

Il ressort de ce qui précède qu'il est extrêmement difficile de définir le terme "cyberdélit"[87]. Ce terme est en effet utilisé pour décrire des délits très variées, 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 seul critère, susceptible d'englober tous les actes mentionnés dans le projet de Convention de Stanford et la Convention sur la cybercriminalité, 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[88].

2.2 Typologie du cyberdélit

Le terme "cyberdélit" étant utilisé pour décrire une grande variété d'infractions[89], il est difficile d'élaborer une typologie ou un système de classification pour ce type de délit[90]. A noter cependant une tentative intéressante: le système proposé par la Convention du Conseil de l'Europe sur la cybercriminalité[91], qui distingue quatre types d'infractions[92]:

- les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques[93];
- les infractions informatiques[94];
- les infractions se rapportant au contenu[95];
- les infractions liées aux atteintes à la propriété intellectuelle[96].

---

87 For difficulties related to the application of 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: http://www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

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

89 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.

90 *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: http://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: http://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

91 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 Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *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: *http://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*.

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

93 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: Chapter 6.1.

94 Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences see below: Chapter 6.1.

95 Art. 9 (Offences related to child pornography). For more information about the offences see below: Chapter 6.1.

96 Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences see below: Chapter 6.1.

Cette typologie n'est pas totalement cohérente, car elle ne repose pas sur un critère unique, qui permettrait de différencier 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[97], infractions se rapportant au contenu[98] et infractions liées aux atteintes à la propriété intellectuelle[99]), alors que la quatrième (infractions informatiques[100]) vise la méthode. Du fait de cette incohérence, les catégories se chevauchent.

De plus, certains termes ("cyberterrorisme"[101], "hameçonnage"[102], etc.) recouvrent des infractions qui correspondent à plusieurs catégories. La classification proposée par la convention du Conseil de l'Europe reste toutefois une bonne base de travail pour étudier le phénomène de la cybercriminalité.

2.3 Indicateurs statistiques concernant les cyberdélits

Il est difficile de quantifier l'effet de la cybercriminalité sur la société[103]. Le nombre d'infractions et les pertes financières qu'elles entraînent sont très difficiles à estimer. Selon certaines sources, les pertes enregistrées par les entreprises et les institutions aux Etats-Unis[104] du fait de la cybercriminalité pourraient atteindre 67 milliards USD; il est cependant difficile de savoir si l'extrapolation des résultats des sondages donne des chiffres fiables[105]. Cette critique méthodologique s'applique aux pertes ainsi qu'au nombre d'infractions reconnues[106].

Le nombre de cyberdélits est difficilement mesurable, car les signalements, par les victimes, ne sont pas systématiques[107]. On peut toutefois, en réalisant des enquêtes, se faire une idée de l'impact de la cybercriminalité. A cet égard, la tendance est un paramètre plus pertinent que le nombre précis de cyberdélits dans une seule année. Elle peut être obtenue par comparaison des résultats sur plusieurs années.

On peut citer, à titre d'exemple, l'étude *Computer Crime and Security Survey 2007*, réalisée par l'institut américain CSI[108], qui analyse, entre autres tendances, le nombre d'infractions informatiques[109]. Cette étude repose sur les réponses fournies par 494 professionnels de la sécurité informatique travaillant dans des

---

97 See below: Chapter 2.4.

98 See below: Chapter 2.5

99 See below: Chapter 2.6

100 See below: Chapter 2.7

101 See below: Chapter 2.8.1

102 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 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. seqq.

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

104 See 2005 FBI Computer Crime Survey, page 10 As well as *Evers*, Computer crimes cost $ 67 billion, FBI says, ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

105 See below: Chapter 2.9.

106 Regarding the economic impact of Cybercrime see below: Chapter 2.9.

107 "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: http://www.heise-security.co.uk/news/80152.

108 Computer Security Institute (CSI), United States.

109 The CSI Computer Crime and Security Survey 2007 is available at: http://www.gocsi.com/

entreprises, des organismes publics et des établissements financiers américains aux Etats-Unis[110]. 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. Cette diminution du nombre d'infractions reconnues (dans les catégories mentionnées) est corroborée par des études menées par d'autres instituts (contrairement à ce que les médias laissent parfois entendre[111]). Une analyse des statistiques sur la criminalité conduit à des conclusions analogues. Des statistiques réalisées en Allemagne[112] montrent par exemple qu'après avoir atteint un pic en 2004, le nombre d'infractions informatiques a presque retrouvé son niveau de 2002.

Les statistiques sur la cybercriminalité ne peuvent pas fournir d'informations fiables sur le niveau ou l'ampleur des infractions[113]. L'incertitude concernant la proportion de victimes ayant signalé des infractions[114] 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.

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

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[115]. 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[116]. Cette section fournit une vue d'ensemble des infractions les plus courantes classées dans cette catégorie.

---

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

111 See, for example, the 2005 FBI Computer Crime Survey, page 10.

112 See Polizeiliche Kriminalstatisik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

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

114 See below: Chapter 2.9.2.

115 Regarding the development of computer systems, see *Hashagen*, The first Computers – History and Architectures.

116 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.»

2.4.1 Accès illégal (piratage, craquage)[117]

Le "piratage" (*hacking*) désigne l'accès illégal à un ordinateur[118]. C'est l'une des infractions informatiques les plus anciennes[119]. vec le développement des réseaux informatiques (notamment d'Internet), cette infraction est devenue un phénomène de masse[120]. Certaines organisations bien connues ont été victimes de piratage. Ainsi 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[121]. Les exemples suivant illustrent quelques infractions entrant la catégorie du "piratage":

- craquage d'un mot de passe ou de sites Internet protégés par mot de passe[122];
- contournement d'une protection par mot de passe sur un ordinateur.

On peut citer quelques exemples d'actes préparatoires:

- exploitation d'une faille logicielle ou matérielle pour obtenir illégalement un mot de passe permettant d'entrer dans un système informatique[123];
- création de sites Internet d'"espionnage" (*spoofing*) conçus pour amener les utilisateurs à révéler leur mot de passe[124];
- 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[125].

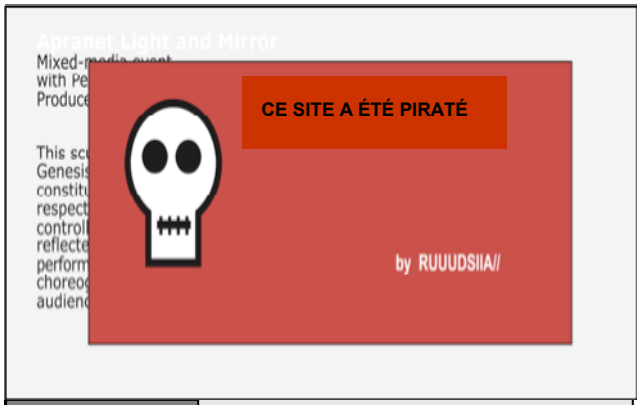


Figure 1

Le logo montre que le site Internet a été piraté. L'auteur a modifié la page d'accueil pour signaler aux visiteurs que son attaque a réussi.

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 (voir Figure 1)[126]. D'autres ont des motivations politiques

---

117 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.

118 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.

119 See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: http://www.aic.gov.au/publications/htcb/htcb005.pdf.; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61.

120 See the statistics provides 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: http://www.hackerwatch.org.

121 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 sq.; Regarding the impact see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et. seq.

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

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

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

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

126 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 Chapter 6.1.a and Chapter 6.1.d.

(c'est ce que l'on appelle l'"hactivisme" ou piratage militant[127]), à l'exemple des pirates qui ont récemment attaqué le site Internet principal des Nations-Unies[128]. 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[129]: espionnage ou manipulation de données, attaques par refus de service (DoS), etc. Ainsi, en règle générale, l'accès illicite au système n'est-il qu'une indispensable première étape[130].

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[131]. Trois facteurs principaux expliquent ce phénomène:

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[132]. 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[133]. 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[134].

Le développement d'outils logiciels d'automatisation des attaques:

Depuis peu, des outils logiciels sont utilisés pour automatiser les attaques[135]. Un même pirate peut, à l'aide de certains logiciels et grâce à des attaques dite "de préinstallation", attaquer des milliers de systèmes informatiques dans une même journée à partir d'un seul ordinateur[136]. Si, en plus, il a accès à d'autres

---

127 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: http://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: http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

128 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

129 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.

130 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;

131 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: http://www.hackerwatch.org.

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

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

134 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, No5 – page 825 et sqq.

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

136 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: http://www.212cafe.com/download/e-book/A.pdf.

ordinateurs – via un botnet[137] par exemple –, 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 cible. Il est très facile de se procurer sur Internet les outils permettant de réaliser ces attaques standard[138]; si certains sont gratuits, les plus efficaces se vendent couramment quelques milliers de dollars[139]. 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)[140].

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[141]. Les ordinateurs professionnels résistent mieux aux attaques utilisant des outils logiciels préconfigurés car ils sont généralement mieux protégés que les ordinateurs privés[142]. 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[143].

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[144]. L'analyse des différentes façons d'envisager la pénalisation des accès aux systèmes informatiques montre que certaines législations 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:

---

137 Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf; See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

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

139 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: http://www.212cafe.com/download/e-book/A.pdf.

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

141 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

142 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: http://www.212cafe.com/download/e-book/A.pdf; *Erickson*, Hacking: The Art of Exploitation, 2003.

143 Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: Chapter 3.2.i.

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

- le système violé est protégé par des mesures de sécurité[145]; et/ou
- l'auteur de l'infraction a l'intention de nuire[146]; et/ou
- des 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[147].

2.4.2 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)[148]. Ainsi Internet est-il de plus en plus utilisé pour dérober des données commerciales confidentielles[149]. 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 soviétiques[150].

Pour entrer dans les systèmes informatiques de leurs victimes, les pirates utilisent diverses techniques[151], notamment:

- l'utilisation de logiciels conçus pour rechercher les ports non protégés[152];
- l'utilisation de logiciels conçus pour contourner les mesures de protection[153];
- l'"ingénierie sociale"[154].

Cette dernière approche 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[155]. L'ingénierie sociale n'est jamais la méthode la moins efficace pour attaquer les systèmes informatiques bien protégés. Elle

---

145 See in this context Art. 2, sentence 2 Convention on Cybercrime.

146 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

147 One example of this is the German Criminal Code, that criminalised 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.

148 For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq. *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, No5 – page 825 et sqq.

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

150 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.

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

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

153 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.

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

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

désigne aussi la manipulation des personnes dans le but d'accéder à des systèmes informatiques[156]. 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[157]. 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.

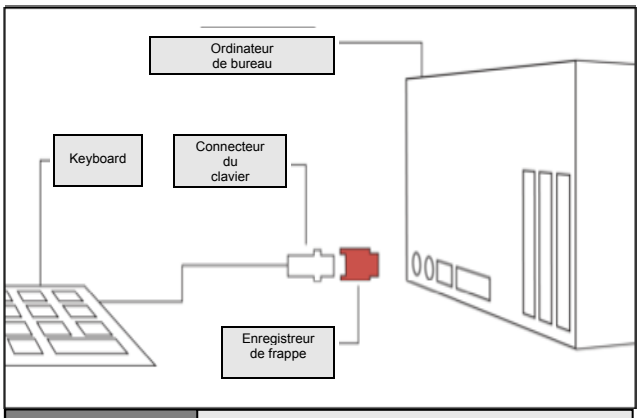


Figure 2

Ce schéma montre comment les enregistreurs de frappe matériels sont installés. La plupart de ces dispositifs – qui ressemblent à des adaptateurs – sont placés entre le connecteur du clavier et l'ordinateur. Les derniers modèles sont intégrés au clavier, de sorte qu'ils sont indécelables (à moins de démonter le matériel). Les logiciels antivirus ne peuvent pas détecter ce type d'enregistreur de frappe.

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[158]. 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[159]. 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[160]. Le succès des attaques visant à dérober des données sensibles s'explique souvent par l'absence de mesures de protection.

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[161]. En effet, les particuliers stockent souvent leurs coordonnées bancaires et leurs numéros de carte de crédit sur leur ordinateur[162], 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[163]. Les données relatives à des cartes de crédit peuvent ainsi se vendre

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

157 See the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: http://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 "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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

158 Regarding the elements of an Anti-Cybercrime Strategy, see below: Chapter 4.

159 "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: http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

160 Physical researches prove 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: Chapter 3.2.m.

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

162 Regarding the impact of this behaviour for identity-theft see *Gercke*, Internet-related Identity Theft, 2007, available at: http://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

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

jusqu'à 60 USD[164]. 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[165]. Plusieurs types de logiciels espions ont été découverts ces dernières années, parmi lesquels les enregistreurs de frappe[166]. Il s'agit de programmes conçus pour enregistrer toutes les frappes effectuées sur le clavier d'un ordinateur[167]. 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[168]) 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 (voir Figure 2). Ce type d'enregistreur de frappe est plus difficile à installer et à détecter, car il requiert un accès physique à l'ordinateur[169]. De plus, les logiciels anti-virus et anti-logiciels espions traditionnels sont, pour l'essentiel, incapables de les détecter[170].

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[171]. Le "hameçonnage" est récemment devenu une infraction majeure dans le cyberespace[172]. Il désigne un type d'infraction caractérisé par la tentative de s'approprier frauduleusement des données sensibles (mots de passe par exemple) en se faisant

---

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

165 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.

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

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

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

169 One approach to gain access to a computer system to install a key-logger 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.

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

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

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

passer pour une personne ou une entreprise digne de confiance (un établissement financier par exemple) dans une communication électronique d'apparence officielle[173].

L'espionnage de données est donc un autre type d'infraction, qui, très intelligemment, vise l'un des maillons les plus faibles de la sécurité informatique, à savoir l'utilisateur. La mise en lumière de l'exploitation du facteur humain fait clairement apparaître les dangers associés à ce type d'escroquerie. Mais il ouvre aussi la voie à des solutions. En effet, les utilisateurs bien formés ne sont pas des victimes faciles. La formation des utilisateurs est donc un élément essentiel de toute stratégie de lutte contre [174]

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[175].

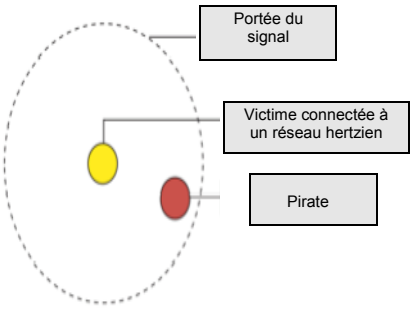


Figure 3

Ce schéma illustre un scénario dans lequel une attaque prend pour cible un ordinateur connecté à un réseau hertzien. Un pirate souhaitant intercepter des données envoyées ou reçues par la victime peut agir en tout point de l'intérieur du cercle défini par la portée du signal. Les signaux peuvent être interceptés dans un rayon maximal de 100 m, en fonction du routeur hertzien et de sa position.

2.4.3 Interception illégale

Pour obtenir des informations, les pirates peuvent également intercepter des communications[176] (messagerie électronique par exemple) ou des transferts de données (transfert vers un serveur ou accès à un support de stockage externe par le Web[177]). Les pirates sont susceptibles de viser tous les types d'infrastructures de communication (lignes fixes, communications hertziennes, etc.) et tous les types de service Internet (messagerie électronique, discussion en ligne, voix sur IP[178], etc.).

La plupart des transferts de données entre fournisseurs d'infrastructures Internet ou fournisseurs de services Internet sont bien protégés et difficiles à intercepter[179]. 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[180]. Aujourd'hui, les hôtels, les restaurants et les bars proposent à leurs clients des accès à Internet via des points d'accès hertzien. Or les signaux utilisés pour l'échange de données entre un ordinateur et un point

---

173 For more information on the phenomenon of phishing see below: Chapter 2.8.4.

174 Regarding the elements of an Anti-Cybercrime Strategy see below: Chapter 4.

175 The Council of Europe Convention on Cybercrime contains no provision criminalising data espionage.

176 *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.

177 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.

178 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 http://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: http://www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

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

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

d'accès peuvent être captés dans un rayon maximal de 100 m[181]. Les pirates souhaitant intercepter un processus d'échanges de données peuvent donc se placer n'importe où dans le cercle défini par ce rayon (Figure 3). Même lorsque les communications hertziennes sont chiffrées, ils parviennent parfois à décrypter les données interceptées[182].

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[183] (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.

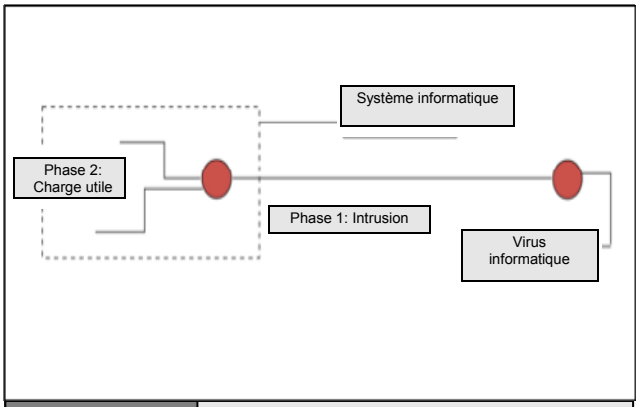


Figure 4

Ce schéma illustre le mode opératoire d'un virus informatique. Après avoir infecté le système (phase 1), le virus exécute la charge utile, c'est-à-dire la fonction pour laquelle il a été programmé (phase 2), à savoir, par exemple, l'effacement ou le chiffrement de certains fichiers.

L'utilisation de lignes fixes n'empêche pas les pirates d'intercepter les communications[184]. En effet, la transmission de données sur une ligne crée un champ électromagnétique[185], que les pirates peuvent détecter et enregistrer à l'aide d'un équipement approprié[186]. 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[187].

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 ou non bénéficier d'une protection analogue[188].

2.4.4 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[189]. Tout problème d'accès aux données peut ainsi causer des dommages (financiers) considérables. Les pirates peuvent violer l'intégrité des données de différentes façons[190]:

- par effacement;
- par suppression;
- par altération;

---

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

182 With regard to the time necessary for decryption see below: Chapter 3.2.13.

183 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: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

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

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

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

187 E.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

188 For more details on legal solutions see below: Chapter 6.1.3.

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

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

- par limitation de l'accès.

Le virus informatique est un exemple de programme malveillant qui opère par effacement des données[191]. Depuis les débuts de l'informatique, les virus menacent les utilisateurs qui ne protègent pas suffisamment leur ordinateur[192]. Le nombre de virus informatiques a en outre considérablement augmenté[193]. On notera deux évolutions récentes majeures, qui concernent:

- la méthode de diffusion des virus;
- leur charge active[194].

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[195]. 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[196] a infecté 90% des ordinateurs vulnérables dans les dix premières minutes de sa diffusion[197]. Les pertes financières dues aux attaques par virus dans la seule année 2000 sont estimées à quelque 17 milliards USD[198]. En 2003, ces pertes s'élevaient encore à plus de 12 milliards USD[199].

La plupart des virus informatiques de première génération étaient conçus pour effacer des données ou afficher des messages (voir Figure 4). Leur charge utile s'est récemment diversifiée[200]. 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 (la victime doit alors payer pour obtenir la clé de chiffrement)[201].

---

191 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. *Cohen*, "Computer Viruses»; *Adleman*, "An Abstract Theory of Computer Viruses». 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/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

192 One of the first computer virus was called (c)Brain and was created by *Basit* and *Amjad Farooq Alvi*. For further details, see: http://en.wikipedia.org/wiki/Computer_virus.

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

194 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.

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

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

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

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

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

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

201 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 license' 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.

2.4.5 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 leurs processus de production, bénéficiant ainsi d'une disponibilité sur vingt-quatre heures et d'une accessibilité dans le monde entier. Les pirates qui parviennent à déstabiliser le fonctionnement des systèmes informatiques peuvent donc [202]causer de très lourdes pertes financières[203].

Une façon de mener une attaque est de s'en prendre physiquement au système informatique[204], par destruction du matériel par exemple (A condition que les pirates peuvent 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[205].

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[206];
- les attaques par refus de service (DoS)[207].

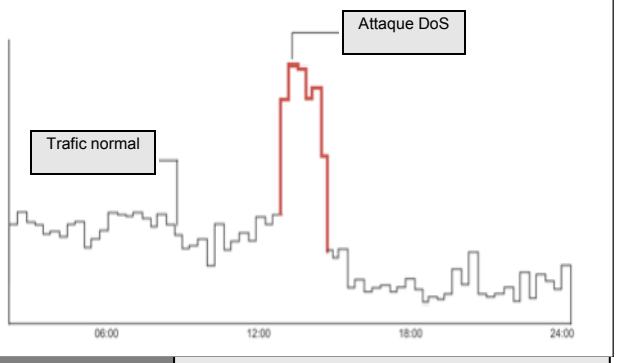


Figure 5

Ce graphique montre le nombre de demandes d'accès à un site Internet en fonctionnement normal (tracé noir) et pendant une attaque par refus de service (DoS). Si le serveur victime n'est pas en mesure de gérer l'augmentation du nombre de requêtes, le temps de réponse du site peut diminuer ou certains services devenir totalement inopérants.

---

202 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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

203 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.

204 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.

205 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.

206 *Sieber*, "Council of Europe Organised Crime Report 2004», page 107.

207 A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications 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: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

Comme les virus, les vers informatiques[208] 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 de deux façons:

- en fonction de la charge utile du ver, l'infection peut perturber le bon fonctionnement de l'ordinateur et le ver peut utiliser les ressources système afin de s'autoreproduire sur Internet;
- l'augmentation du trafic sur le réseau 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[209]. En envoyant à un système informatique plus de requêtes qu'il ne peut en gérer (voir Figure 5), 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[210], rendant certains services indisponibles pendant plusieurs heures, voire plusieurs jours[211].

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[212], la question se pose de savoir si la prévention et la poursuite des attaques visant des infrastructures essentielles requiert une approche législative distincte. Cette question est en cours d'examen.

2.5 Infractions se rapportant au contenu

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[213]. 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.

---

208 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 programme running loose through a computer network.

209 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: http://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».

210 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: http://www.projects.ncassr.org/hackback/ethics00.pdf.

211 *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;

212 Regarding the different approaches see below: Chapter 6.1.5.

213 For reports on cases involving illegal content, see *Sieber*, "Council of Europe Organised Crime Report 2004», page 137 et seqq.

Ainsi, la diffusion de contenus xénophobes est illégale dans de nombreux pays européens[214], alors qu'elle peut relever de la liberté d'expression[215] aux Etats-Unis[216]. De même, les remarques désobligeantes à l'égard du prophète Mahomet sont érigées en infraction pénale dans de nombreux pays arabes[217], mais pas dans certains pays européens.

Les problèmes juridiques qui se posent sont complexes, car toute information, une fois mise en ligne par un internaute dans un pays donné, devient accessible de tout point du globe (ou presque)[218]. Or, si un "délinquant" crée du contenu jugé illicite dans certains pays, mais pas dans le pays à partir duquel il opère, il est difficile, voire impossible, d'engager des poursuites à son encontre[219].

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[220].

---

214 One example of the wide criminalisation of illegal content is Sec. 86a German Penal Code. The provision criminalises 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.

215 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

216 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 criminalisation was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

217 See e.g. Sec. 295C 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 Muhammad (peace be upon him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

218 See below: Chapter 3.2.6 and Chapter 3.2.7.

219 In many cases, the principle of dual criminality hinders international cooperation.

220 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: http://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: http://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: http://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: http://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.

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[221]. 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)[222].

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. L'OpenNet Initiative[223] signale, à cet égard, qu'une vingtaine de pays environ pratiquent la censure[224].

2.5.1 Contenus érotiques ou pornographiques (A 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 des frais de port élevés[225];
- accès mondial[226] permettant d'atteindre un nombre de clients très supérieur à ce que peuvent réaliser des magasins de détail;
- Internet est souvent (A tort[227]) considéré comme un médium anonyme, caractéristique que les consommateurs de pornographie apprécient compte tenu des opinions sociales prédominantes.

---

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

222 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.

223 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: http://www.opennet.net.

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

225 Depending on the availability of broadband access.

226 Access is in some countries is limited by filter technology. 226 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: http://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: http://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: http://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: http://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.

227 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: Chapter 6.2.

De récentes études ont recensé pas moins de 4,2 millions de sites pornographiques potentiellement disponibles à tout moment sur Internet[228]. Outre les sites Internet, d'autres supports permettent de diffuser du contenu pornographique:

- les systèmes de partage de fichiers[229];
- 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[230], 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[231]. Selon certaines études, l'accès, par des enfants, à du contenu pornographique pourrait avoir sur leur développement des effets indésirables[232]. Pour se conformer aux diverses législations, les sites Internet ont mis en place des "systèmes de vérification de l'âge" (Figure 6)[233]. D'autres pays sanctionnent pénalement tout échange de contenu pornographique, même entre adultes[234], sans viser spécifiquement certains groupes (les mineurs par exemple).

Figure 6

Cette figure présente une approche possible pour empêcher l'accès par des mineurs à des sites Internet hébergeant du contenu pornographique. Plusieurs pays jugent cette solution insuffisante car elle ne permet pas de vérifier la réponse donnée par l'utilisateur.

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.

---

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

229 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.

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

231 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; […]

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

233 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: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

234 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.

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[235]. De plus, le principe de "double incrimination"[236] 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[237] par exemple)[238].

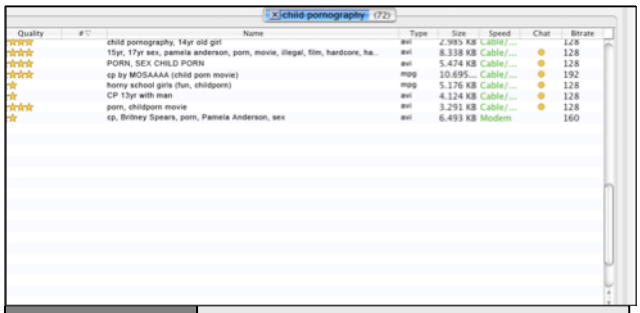


Figure 7

Cette image correspond à l'interface utilisateur d'un logiciel de partage de fichiers. La recherche de l'expression "child pornography» renvoie la liste de tous les fichiers mis à disposition par les utilisateurs du système dont le nom contient cette expression.

2.5.2 Pornographie mettant en scène des enfants (pédopornographie)

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[239]. Plusieurs organisations internationales sont engagées dans la lutte contre la diffusion en ligne de ce type de pornographie[240]. A noter, entre autres, plusieurs initiatives juridiques internationales: la Convention des Nations Unies relative aux droits de l'enfant de 1989[241], la Décision-cadre du Conseil de l'Union européenne relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie[242], et la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels[243].

---

235 National Sovereignty is a fundamental principle in International Law. See Roth, "State Sovereignty, International Legality, and Moral Disagreement», 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

236 Regarding the principle of "dual criminality», see below: Chapter 6.3.2.

237 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: http://www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

238 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: http://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: http://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: http://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: http://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.

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

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

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

242 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.

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

Malheureusement, s'agissant du contrôle de la pornographie 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 (Figure 7)[244]. 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[245], 19% des images d'enfants âgés de moins de trois ans[246] et 21% des images d'actes de violence[247].

La vente de contenu pédopornographique est très rentable[248], les personnes intéressées étant prêtes à payer de fortes sommes pour des films et des images montrant des enfants dans un contexte sexuel[249]. Les moteurs de recherche permettent de trouver ce type de contenu très rapidement[250]. 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[251].

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[252]

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[253]. 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[254]. Il n'en reste pas moins que les personnes qui effectuent des paiements anonymes sont difficiles à dépister.

---

244 *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: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

245 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

246 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

247 For more information, see "Child Pornography: Model Legislation & Global Review», 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

248 See *Walden*, "Computer Crimes and Digital Investigations», page 66.

249 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.

250 "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: http://www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

251 See ABA "International Guide to Combating Cybercrime», page 73.

252 Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, "Harvard Journal of Law & Technology», Volume 11, page 840 et seqq.

253 For more information, see *Wilson*, "Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond».

254 *Smith*, "Child pornography operation occasions scrutiny of millions of credit card transactions»,, available at: http://www.heise.de/english/newsticker/news/print/83427.

2) L'utilisation de techniques de chiffrement[255]

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[256], ce qui complique considérablement les enquêtes[257].

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[258].

2.5.3 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 (Figure 8)[259]. On observe depuis peu une augmentation du nombre de sites Web présentant un contenu raciste et des discours de haine[260]. 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[261]. On dénombrait, en 2006, plus de 6 000 sites de ce type sur Internet[262].

Figure 8

Cette figure présente un site Internet édité par un groupement radical. Ce type de groupement a largement recours à Internet pour expliquer ses objectifs et recruter de nouveaux membres.

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[263]. 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[264]. Internet est aussi utilisé pour transmettre du courrier électronique, envoyer des bulletins d'information et diffuser des clips vidéo et des

255 See below: Chapter 3.2.13.

256 Based on the "National Juvenile Online Victimisation Study», 12% 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

257 See below: Chapter 3.2.13.

258 For an overview about 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.

259 Radical groups in the United States recognised 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.

260 *Sieber*, "Council of Europe Organised Crime Report 2004», page 138.

261 *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: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

262 See "Digital Terrorism & Hate 2006», available at: http://www.wiesenthal.com.

263 *Whine*, "Online Propaganda and the Commission of Hate Crime», available at: http://www.osce.org/documents/cio/2004/06/3162_en.pdf

264 See "ABA International Guide to Combating Cybercrime», page 53.

programmes télévisés via des sites d'archivage bien connus (YouTube, etc.).

Tous les pays ne sanctionnent pas ces infractions[265], ce type de contenu étant parfois protégé au nom de la liberté d'expression[266]. 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[267]. 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[268].

Figure 9

Cette figure présente un site Internet mettant à disposition un contenu à caractère religieux, qui peut être vu dans le monde entier.

Ces divergences 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 des conflits de lois[269]. 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[270]. Certains pays, notamment les Etats-Unis, auraient pu, sans cela, se trouver dans l'incapacité de signer la convention.

2.5.4 Infractions à motivation religieuse

Un nombre grandissant[271] 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

---

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

266 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

267 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, page1041.

268 See"Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme», 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: http://www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=213138298941949941944938934938937961519199 1.

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

270 See "Explanatory Report to the First Additional Protocol», No. 4.

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

figurent les déclarations écrites contre la religion[272]. 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 (Figure 9).

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 le principe de la liberté d'expression[273], facteur fondamental de la réussite d'Internet[274]. 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. Cette "affaire des caricatures de Mahomet"[275] est une bonne illustration des risques de conflit, au niveau international, liés à la disparité des réglementations.

La diffusion de certaines informations ou matériels – religieux notamment – 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[276] ou la profanation du Coran[277], alors que d'autres, adoptant une approche plus libérale, ne sanctionnent pas de tels actes.

---

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

273 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

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

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

276 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.

277 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.

2.5.5 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[278]. Selon la société Linden Labs, le nombre d'inscriptions au jeu en ligne *Second Life*[279], dont elle est l'inventeur, atteindrait les dix millions[280]. Certaines études montrent que de tels jeux ont été utilisés pour commettre des infractions, notamment[281]:

- échanges et affichages de contenus pornogra-phiques mettant en scène des enfants[282];
- fraude[283];
- paris dans des cybercasinos[284];
- diffamation (diffusion de messages calomnieux par exemple).

Certaines estimations prévoient une augmentation des recettes liées aux paris en ligne, qui passeraient de 3,1 milliard USD en 2001 à 24 milliards USD en 2010[285] (A noter cependant qu'en regard des recettes générées par les jeux traditionnels, ces estimations restent relativement faibles[286]).

Les réglementations relatives aux jeux en ligne et hors ligne varient selon les pays[287]. 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,

Figure 10

Cette figure présente l'interface utilisateur d'un cybercasino. Après s'être enregistré et avoir transféré des fonds, l'internaute peut jouer en ligne. À noter que plusieurs cybercasinos autorisent l'utilisation de leurs services sans inscription préalable.

278 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: http://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: http://www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

279 http://www.secondlife.com.

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

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

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

283 *Leapman*, "Second Life world may be haven for terrorists», Sunday Telegraph, 14.05.2007, available at: http://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/.

284 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.

285 Christiansen Capital Advisor.
See http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

286 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: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

287 See, for example, GAO, "Internet Gambling – An Overview of the Issues», available at: http://www.gao.gov/new.items/d0389.pdf; Regarding the WTO Proceedings, "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services», see: http://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.

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)[288]. Ce succès tient au fait que, le jeu étant illégal en Chine[289], 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[290]. Les cybercasinos, sites très répandus (voir Figure 10), 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[291]. Les cybercasinos interviennent également dans les activités de blanchiment de capitaux et de financement du terrorisme[292]. Lorsque les délinquants parient dans des 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[293]. Plusieurs pays ont essayé d'interdire, par la loi, la participation aux jeux en ligne[294]. On peut citer l'*Internet Gambling Prohibition Enforcement Act* (loi d'application de l'interdiction du jeu sur Internet) aux Etats-Unis, qui vise à limiter les jeux illégaux en ligne en poursuivant les prestataires de services financiers qui acceptent d'effectuer des transactions liées à des jeux illégaux[295].

2.5.6 Diffamation et fausses informations

Si Internet permet de diffuser de vraies informations, il permet d'en répandre de fausses tout aussi facilement[296]. 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[297]. Les mineurs utilisent de plus en plus les forums et les sites de réseau social, qui sont aussi des vecteurs de fausses informations[298]. Parmi les actes

---

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

289 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.

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

291 For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

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

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

294 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.

295 See § 5367 Internet Gambling Prohibition Enforcement Act.

296 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: http://www.mttlr.org/voleight/Reder.pdf.

297 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.

298 Regarding the privacy concerns related to those 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: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

répréhensibles[299], on peut citer la diffusion de photographies intimes et la publication de fausses informations concernant des comportements sexuels[300].

La plupart des délinquants profitent du fait que les services de publication en ligne gratuits ou bon marché n'imposent généralement pas aux auteurs de s'identifier ou ne vérifient pas correctement les identités[301]. 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 (Figure 11). 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 Wikipédia[302], 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)[303];
- diffamer (en diffusant des messages calomnieux par exemple)[304];
- révéler des informations confidentielles (en diffusant des secrets d'Etat ou des informations commerciales sensibles par exemple).

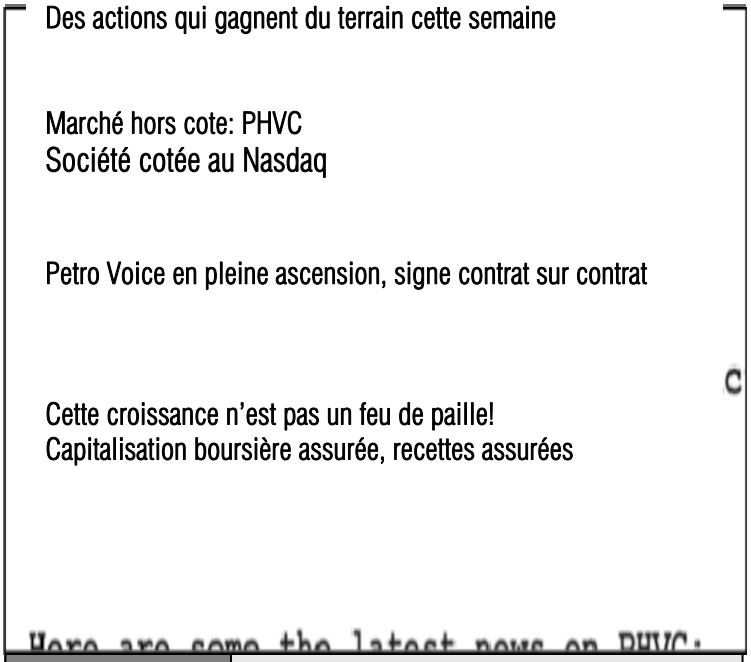


Figure 11

Les courriels de pollupostage, qui couvrent une grande variété de sujets, constituent un problème grave. Outre la promotion de divers produits, on y trouve très fréquemment des informations boursières.

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,

299 Regarding the controversial discussion about the criminalisation 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: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An »Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://www.article19.org/pdfs/standards/definingdefamation.pdf.

300 See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

301 With regard to the challenges of investigating offences linked to anonymous services see below: Chapter 3.2.l2.

302 See: http://www.wikipedia.org

303 See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

304 See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

l'information est toujours disponible en ligne, même si elle a été retirée ou corrigée par son auteur[305]. 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[306] d'une part et protection des victimes d'autre part[307].

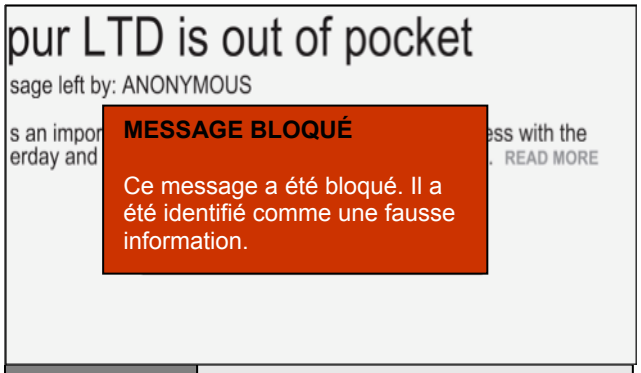


Figure 12

Les forums Internet où quiconque peut déposer un message sans inscription formelle préalable véhiculent fréquemment de fausses informations.

2.5.7 Pollupostage et risques connexes

Le pollupostage (*spam*) désigne l'envoi massif de messages non sollicités (Figure 12)[308]. Parmi les différentes méthodes de pollupostage, 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 pollupostage en 1978[309], le phénomène n'a fait qu'augmenter, pour atteindre aujourd'hui des proportions considérables[310]. Selon les prestataires de messagerie électronique, le pollupostage représenterait jusqu'à 85 à 90% de l'ensemble des courriels[311]. En 2007, les principales sources de pollupostage par courriel étaient les Etats-Unis (19,6% du pollupostage recensé), la République populaire de Chine (8,4%) et la République de Corée (6,5%)[312].

La plupart des fournisseurs de courriel ont réagi à l'augmentation du pollupostage en installant des filtres anti-pollupostage, qui repèrent les courriels incriminés à l'aide de mots-clés ou de listes noires contenant les adresses

---

305 Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as http://www.archive.org

306 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

307 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.

308 For a more 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.

309 *Tempelton*, "Reaction to the DEC Spam of 1978», available at: http://www.templetons.com/brad/spamreact.html.

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

311 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: http://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 http://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; http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html, available April 2007.

312 "2007 Sophos Report on Spam-relaying countries», available at: http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

IP des polluposteurs[313]. Malgré l'évolution des technologies de filtrage, les polluposteurs 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 par pollupostage – sans utiliser le nom de la marque[314].

La capacité à détecter le pollupostage dépend des techniques de diffusion et de leurs évolutions. De nombreux polluposteurs 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[315]), mais en utilisant des botnets[316]. Chaque ordinateur du botnet – qui en contient des milliers[317] – 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 polluposteurs.

Comme il est possible d'envoyer des milliards de courriels pour une somme modique, le pollupostage est une activité très rentable. L'utilisation de botnets permet encore de réduire les coûts[318]. Certains experts avancent ainsi que la seule solution pour lutter contre le pollupostage serait d'augmenter les coûts d'émission des courriels[319]. Selon une analyse des coûts et des profits du pollupostage par courriel publiée en 2007, le coût d'envoi de 20 millions de courriels s'élève à environ 500 USD[320]. Le pollupostage est donc une technique très rentable, notamment pour ceux qui envoient les courriels par milliards, tel ce polluposteur néerlandais, qui déclarait avoir dégagé un bénéfice de 50 000 USD en envoyant au moins 9 milliards de courriels pollués[321].

En 2005, l'OCDE a analysé, dans un rapport, les effets du pollupostage sur les pays en développement[322]. Ces pays déclarent souvent que leurs internautes subissent davantage les effets du pollupostage et des pratiques frauduleuses sur Internet. En effet, la bande passante et l'accès à Internet sont pour eux des ressources

---

313 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: http://www.ciac.org/ciac/bulletins/i-005c.shtml; For an overview on different approaches see: BIAC ICC Discussion Paper on SPAM, 2004, available at: http://www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf

314 Lui/Stamm, "Fighting Unicode-Obfuscated Spam», 2007, page 1, available at: http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

315 Re 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, "Consumer Perspectives On Spam: Challenges And Challenges», available at: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

316 Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf.

317 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.

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

319 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: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

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

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

322 "Spam Issue in Developing Countries», available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

précieuses, plus limitées et plus onéreuses que dans les pays industrialisés[323]. Le pollupostage consommant inutilement des ressources et du temps, les pays en développement sont donc particulièrement touchés.

2.5.8 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[324];
- de vendre illégalement des produits;
- 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[325]. C'est le cas notamment de la vente de médicaments: tel médicament en vente libre dans un pays est seulement prescrit sur ordonnance dans un autre[326]. 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[327]. 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[328], elles sont plus faciles à obtenir, ce qui augmente les risques d'attaque armée.

---

323 See "Spam Issue in Developing Countries», Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

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

325 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: http://www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement.

326 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.

327 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: http://www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, "What's a Legal System to Do? The Problem of Regulating Internet Pharmacies», available at: https://www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

328 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: http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.

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

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[329] peuvent être poursuivies pour violation de droits d'auteur si les produits qu'elles proposent sont téléchargés, copiés et redistribués.

2.6.1 Infractions se rapportant aux atteintes à la propriété intellectuelle

L'industrie du divertissement a profité du passage de l'analogique au numérique[330] pour numériser[331] 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 les DVD sont en outre plus durables que les disques et les vidéocassettes[332].

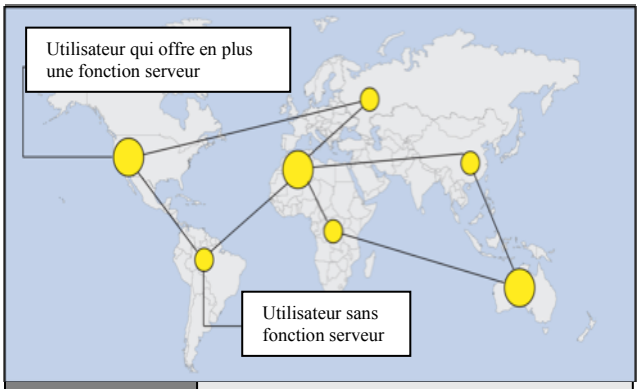


Figure 13

Ce schéma illustre le fonctionnement des systèmes de partage de fichiers de deuxième génération. Alors que les systèmes de première génération reposaient sur des serveurs centraux contenant les listes de documents disponibles, les systèmes de deuxième génération délèguent la fonction serveur aux utilisateurs, ce qui complique le démantèlement des réseaux et la prévention des infractions contre la propriété intellectuelle.

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[333];
- le fait de contourner les systèmes de gestion des droits numériques (DRM)[334].

---

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

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

331 See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.

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

333 *Sieber*, Council of Europe "Organised Crime Report 2004», page 148.

334 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://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: http://www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

Les systèmes de partage de fichiers sont des services en réseau reposant sur le *peer-to-peer*[335], qui permettent aux utilisateurs de partager des fichiers[336], souvent avec des millions d'autres utilisateurs[337]. 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 fichiers 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*[338] 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[339], les autres pays de l'OCDE affichant une tendance analogue[340]. Ces systèmes permettent d'échanger tout type de données informatiques: musiques, films, logiciels, etc.[341] Autrefois principalement utilisé pour échanger de la musique, le partage de fichiers sert aujourd'hui de plus en plus à télécharger des vidéos[342].

Les services de partage de fichiers utilisent une technologie très sophistiquée, qui permet d'échanger de gros fichiers sur de courtes périodes de temps[343]. Ceux de 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. Le célèbre réseau Napster a ainsi fait l'objet de sanctions pour partage illégal de fichiers[344]. Les

---

335 Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking, 2005», available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, "A Survey of Peer-to-Peer Content Distribution Technologies, 2004», available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

336 GAO, File Sharing, "Selected Universities Report Taking Action to Reduce Copyright Infringement», available at: http://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: http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

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

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

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

340 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: http://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.

341 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.

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

343 *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking», 2005, page 11, available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Cope, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: http://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.

344 Regarding Napster and the legal response see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: http://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.

systèmes de deuxième génération ne reposent plus sur un serveur central[345]: ils sont décentralisés (voir Figure 13). 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[346]. 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[347].

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[348]. 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[349].

Cela étant, les systèmes de partage de fichiers posent à l'industrie du divertissement divers problèmes[350]. 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[351], et les fichiers téléchargés par milliards[352]. On trouve même des copies de films avant la sortie officielle en salle[353], 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[354].

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)[355], qui consiste à

---

345 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: http://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: http://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: http://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.

346 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 seqq., available at: http://www.ncjrs.gov/pdffiles1/nij/210798.pdf.

347 *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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing», 2005.

348 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: http://www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

349 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.

350 Regarding the economic impact, see: *Liebowitz*, "File-Sharing: Creative Destruction or Just Plain Destruction», Journal of Law and Economics, 2006, Volume 49, page 1 et seqq.

351 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% of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

352 "The Recording Industry 2006 Privacy Report», page 4, available at: http://www.ifpi.org/content/library/piracy-report2006.pdf.

353 One example is the movie, "Star Wars – Episode 3», that appeared in file-sharing systems hours before the official premiere. See: http://www.heise.de/newsticker/meldung/59762 that is taking regard to a MPAA press release.

354 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.

355 Content Scrambling Systems (CSS) is a Digital Rights Management system that is used is most DVD videos discs. For details about the encryption used, see *Stevenson*, "Cryptanalysis of Contents Scrambling System», available at: http://www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

chiffrer les DVD au niveau de leur contenu pour en empêcher la copie[356]. 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)[357] 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[358]. Les pirates ont en effet développé des outils logiciels permettant aux utilisateurs de diffuser sur Internet des fichiers protégés contre la copie[359], 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[360].

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[361].

2.6.2 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[362]. Les infractions les plus graves comprennent:

- l'utilisation de marques commerciales dans le but de tromper;
- les infractions se rapportant au nom ou au domaine.

---

356 Regarding further responses of the entertainment industry (especially lawsuits against Internet user) 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.

357 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, "Digital Rights Management: The Skeptics' View», available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

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

359 *Sieber*, Council of Europe Organised Crime Report 2004, page 152.

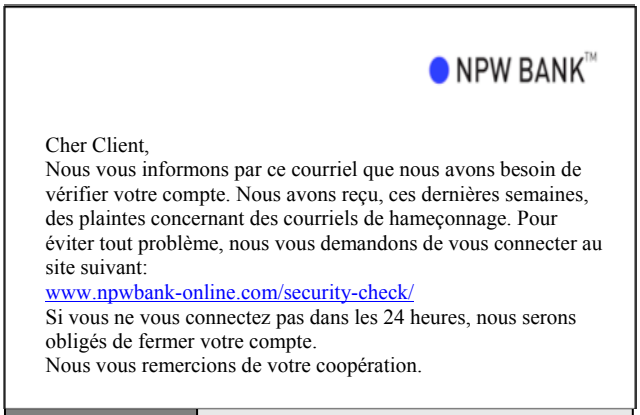
360 See: http://www.golem.de/0112/17243.html.

361 Regarding the similar discussion with regard to tools used to design viruses, see below: Chapter 2.7.4.

362 See Bakken, Unauthorised 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: http://www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf;

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 (voir Figure 14), technique consistant à envoyer des millions de courriels falsifiés (en y insérant des noms de marque par exemple)[363] afin de persuader les destinataires qu'ils proviennent de sociétés reconnues pour légitime[364].

Parmi les infractions se rapportant à des marques commerciales, on compte aussi celles qui visent les domaines Internet[365], tels que le cybersquattage[366], pratique abusive consistant à faire enregistrer le nom de la marque commerciale d'un produit ou d'une société ou un nom approchant[367]. La plupart du temps, les malfaiteurs cherchent à revendre au prix fort le nom de domaine à la société prise pour victime[368] 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[369]. On peut également citer le "détournement de domaine" et l'enregistrement de noms de domaine ayant expiré par mégarde[370].


NPW BANK™

Cher Client,
Nous vous informons par ce courriel que nous avons besoin de vérifier votre compte. Nous avons reçu, ces dernières semaines, des plaintes concernant des courriels de hameçonnage. Pour éviter tout problème, nous vous demandons de vous connecter au site suivant:
www.npwbank-online.com/security-check/
Si vous ne vous connectez pas dans les 24 heures, nous serons obligés de fermer votre compte.
Nous vous remercions de votre coopération.

Figure 14

Cette figure montre un courriel de hameçonnage. Ce type de courriel est rédigé de telle sorte qu'il ressemble à une communication émanant d'une société reconnue pour légitime. Ils contiennent souvent des logos originaux et protégés de la marque commerciale.

2.7 Infractions informatiques

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;
- l'utilisation abusive de dispositifs.

---

363 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 *Gercke*, The criminalisation of Phishing and Identity Theft, Computer und Recht, 2005, 606; *Ollmann*, "The Phishing Guide: Understanding & Preventing Phishing Attacks», available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: Chapter 2.8.d.

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

365 Re the connection with trademark-related offences, see for example: "Explanatory Report to the Convention on Cybercrime», No. 42.

366 Another term used to describe the phenomenon is "domain grabbing». Regarding cyber-squatting see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from Cybersquatters, Virginia Journal of Law and Technology, Vol. 10, Issue 6; *Benoliel*, Cyberspace Technological Standandization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 et seq.; *Struve/Wagner*, Realspace Sovereignty in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 et seq.; *Travis*, The Battle for Mindshare: The Emerging Consesus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003;

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

368 This happens especially with the introduction of new top-level-domains. To avoid cyber-squatting, 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.

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

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

2.7.1 Fraude et fraude informatique

La fraude informatique est l'un des délits les plus courants sur Internet[371], car elle peut être automatisée[372] 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[373]. Une stratégie consiste à veiller à ce que les pertes financières supportées par chaque victime restent en deçA 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[374]. Dans cette catégorie d'escroquerie, on peut citer la fraude aux avances sur commission, notamment la "lettre nigériane" (Figure 15)[375].

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"[376], 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:

Cher ami,

Permettez-moi tout d'abord de me présenter. Je m'appelle Mbuto Butalia. Je suis la femme de l'ex-Président de la République de Thalia. Mon bien-aimé mari est récemment décédé dans un accident d'avion. En rangeant ses papiers, j'ai découvert qu'il possédait un compte secret doté de 10 millions $.
J'aimerais envoyer cet argent à ma famille, qui vit aux États-Unis.
Je ne peux malheureusement pas le faire directement, c'est pourquoi je sollicite votre aide.
Je souhaiterais faire un virement de 10 millions $ sur votre compte. Vous pourriez ensuite envoyer 9 millions $ à ma famille et garder la différence (1 million $). Si vous acceptez, pourriez-vous, dans un premier temps, faire un virement de 10 $ sur mon compte afin que je puisse vérifier vos coordonnées bancaires.

Figure 15

Cette figure présente un courriel typique de fraude aux avances sur commission. Pour recevoir la prétendue commission, le destinataire doit au préalable envoyer une certaine somme d'argent. En l'absence de manipulation d'un ordinateur, cette escroquerie, bien que très populaire, n'est pas considérée comme une fraude informatique.

1. La fraude aux enchères en ligne[377]

Les enchères en ligne sont aujourd'hui l'un des services de commerce électronique les plus populaires. En 2006, des biens pour une valeur totale dépassant 20 milliards USD ont été vendus sur eBay, plus grand site d'enchères au monde[378]. 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.

---

371 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: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

372 Regarding the related challenges see below: Chapter 3.2.8.

373 In 2006, Nearly 50% 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: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

374 Regarding the related automation process: Chapter 3.2.8.

375 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. 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: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response», "Computer Law & Security Report», Volume 21, Issue 3, 237.

376 For more information, see below: Chapter 6.1.13.

377 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: http://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: http://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

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[379]. 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[380]. Les deux escroqueries les plus courantes consistent[381]:

- à proposer à la vente des produits qui n'existent pas et à exiger des acheteurs le paiement avant livraison[382];
- 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 vendeurs et les acheteurs laissent un commentaire[383], qui fournit aux autres utilisateurs une information neutre sur la fiabilité des vendeurs/acheteurs. Selon 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[384]. Dans cette escroquerie appelée "piratage de compte"[385], 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.

2. La fraude aux avances sur commission[386]

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[387]. 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

---

378 See http://www.ebay.com.

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

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

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

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

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

384 Regarding the criminalisation of "account takeovers», see *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

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

386 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. 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: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response», "Computer Law & Security Report», Volume 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: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

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[388]. 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[389].

2.7.2 Falsification informatique

La falsification informatique désigne la manipulation de documents numériques[390], 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);
- 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[391]. L'objectif du hameçonnage est d'amener la victime à révéler des informations personnelles ou confidentielles[392]. 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[393]. Le courriel est rédigé de telle façon qu'il est difficile pour la victime de déceler la supercherie[394]. 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 autres opérations frauduleuses[395].

en espérant que le délai sera
qu'ils transfèrent une somme relativement faible.

NOTE: Ce message est chiffré avec une signature numérique pour éviter toute manipulation.

Figure 16

Contrairement aux documents classiques, les données électroniques peuvent facilement être falsifiées. Il existe des solutions techniques pour prévenir les modifications non autorisées, notamment les signatures numériques.

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

388 For an overview of estimated losses, see *Reich*, "Advance Fee Fraud Scams in-country and across borders», "Cybercrime & Security», IF-1, page 3 et seqq.

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

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

391 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: http://www.usdoj.gov/opa/report_on_phishing.pdf

392 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

393 "Phishing» scams show a number of similarities to spam e-mails. It is likely that those organised crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: Chapter 2.5.g.

394 Regarding related trademark violations, see above: Chapter 2.6.2.

395 For more information about phishing scams see below: Chapter 2.8.4.

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 (Figure 16).

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[396] 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[397].

2.7.3 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[398]. Cet acte peut être effectué sans l'aide de moyens techniques[399], mais aussi en ligne grâce à la technologie Internet[400].

En règle générale, les infractions désignées sous le terme de "vol d'identité" se déroulent en trois phases[401]:

- 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[402]. Dans cette phase, les informations ne sont pas encore directement utilisées mais elles peuvent par exemples être vendues[403]. Des données relatives à des cartes de crédit peuvent par exemple se vendre jusqu'à 60 USD[404].

---

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

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

398 *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: http://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: http://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.

399 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: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

400 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% obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://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: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.

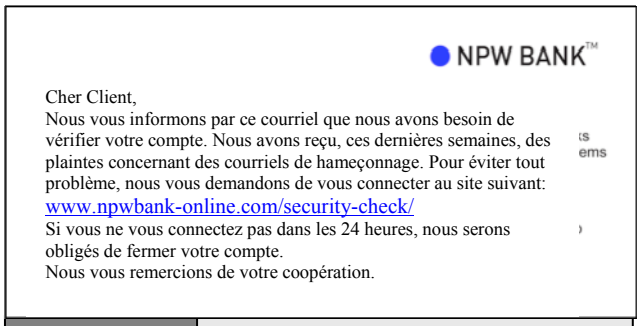
401 *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 et seq., available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

402 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: http://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.

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

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

- 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'identité permet au malfaiteur de commettre de nouvelles infractions[405]. 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[406].


NPW BANK™

Cher Client,
Nous vous informons par ce courriel que nous avons besoin de vérifier votre compte. Nous avons reçu, ces dernières semaines, des plaintes concernant des courriels de hameçonnage. Pour éviter tout problème, nous vous demandons de vous connecter au site suivant:
www.npwbank-online.com/security-check/
Si vous ne vous connectez pas dans les 24 heures, nous serons obligés de fermer votre compte.
Nous vous remercions de votre coopération.

Figure 17

Les courriels de hameçonnage sont utilisés pour inciter les victimes à communiquer des informations confidentielles (coordonnées bancaires, mots de passe, numéros de transaction, etc.), qui sont ensuite utilisées par les malfaiteurs pour commettre des infractions.

Dans la première phase, les méthodes utilisées pour obtenir les 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*[407]), à voler du courrier[408], 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[409]. Des études soulignent d'ailleurs les risques que peut présenter l'utilisation légale de moteurs de recherche à des fins illicites[410]. 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[411]. Outre cette possibilité, les malfaiteurs peuvent aussi recourir à des personnes bien placées ayant accès à des données d'identité. D'après l'étude *Computer Crime and Security Survey 2007*[412], 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 bien placées est supérieur à 20%. Enfin, on a vu apparaître ces dernières années des méthodes d'escroquerie efficaces utilisant

---

405 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf .

406 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 – available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

407 P utting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

408 This method is not considered as an Internet-related approach.

409 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.

410 See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

411 See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.

412 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 U.S corporations, government agencies and financial institutions. The Survey is available at: http://www.gocsi.com/·

des techniques d'ingénierie sociale pour persuader les victimes de divulguer des informations personnelles ou confidentielles (coordonnées bancaires, données de cartes de crédit, etc.)[413]. Voir à ce propos la Figure 17.

Les données recherchées sont de plusieurs types[414]. Parmi les plus courantes:

- **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[415]. 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[416].
- **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)[417]. 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[418] ou saisies sur des sites comme preuve d'identité en vertu d'obligations légales[419].
- **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[420]. 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[421].
- **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[422]. Selon des chiffres récents, au premier semestre 2004, 3% des ménages américains ont été victimes de vol d'identité[423]. Au Royaume-Uni, le coût du

---

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

414 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.

415 *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.

416 See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm.

417 *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: http://www.privacyrights.org/ar/id_theft.htm.

418 Examples is the online community Facebook, available at http://www.facebook.com.

419 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).

420 Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

421 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

422 "Identity Theft, Prevalence and Cost Appear to be Growing», GAO-02-363.

423 United States Bureau of Justice Statistics, 2004, available at http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

vol d'identité pour l'économie britannique a été estimé à 1,3 milliard de livres par an[424]. 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[425]. L'*Identity Fraud Survey 2006* (étude de la fraude à l'identité 2006) estime les pertes en 2005 aux Etats-Unis à 56,6 milliards USD[426]. Outre l'aspect financier, il convient également de mentionner les atteintes à la réputation[427]. 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[428].

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[429].

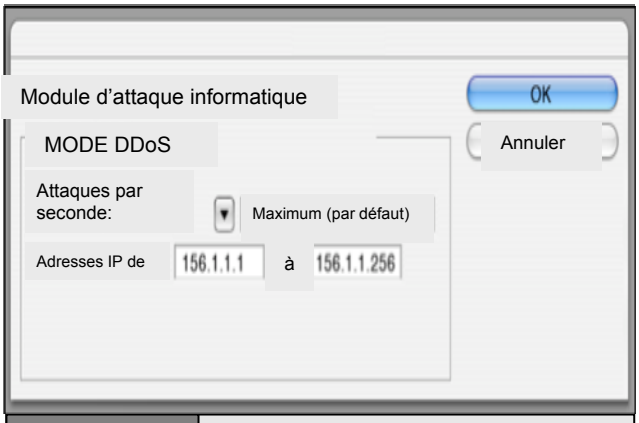


Figure 18

Plusieurs outils permettent aux cyberdélinquants d'automatiser des attaques contre tous les ordinateurs dont l'adresse IP se situe dans une fourchette prédéfinie. Grâce à ces outils, il est possible d'attaquer des centaines d'ordinateurs en quelques heures.

2.7.4 Utilisation abusive de dispositifs

Pour commettre une infraction sur Internet, un équipement relativement élémentaire suffit[430]. 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.

---

424 See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.

425 *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

426 See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.

427 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper», 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

428 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: http://www.heise-security.co.uk/news/80152.

429 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper», 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

430 The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: Chapter 3.2.h.

Il est facile de se procurer sur Internet des outils permettant de commettre des infractions complexes[431]. Si les plus simples sont souvent gratuits, les plus sophistiqués peuvent coûter plusieurs milliers de dollars[432]. Grâce à ces outils, les malfaiteurs peuvent attaquer des systèmes informatiques en un simple clic (Figure 18). 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[433]. On trouve ainsi des outils pour[434]:

- mener des attaques de type DoS[435];
- créer des virus informatiques;
- décrypter une communication chiffrée;
- 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[436] 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[437].

2.8 Infractions combinées

Plusieurs termes servent à décrire des escroqueries complexes relevant de plusieurs types d'infractions. On peut citer:

- le cyberterrorisme;
- le cyberblanchiment;
- le hameçonnage.

---

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

432 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: http://www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (200-500 US Dollar) see: Paget, Identity Theft, White Paper, McAfee, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

433 See above: Chapter 2.4.1.

434 For more examples, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond», page 23 et seq., available at: http://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: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.

435 DoS is an acronym for Denial-of-Service attack. For more information, see above : Chapter 2.4.e.

436 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: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

437 For more details, see below: Chapter 6.1.13.

2.8.1 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[438]. 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[439], mais il est difficile d'évaluer le niveau de la menace[440]. 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[441].

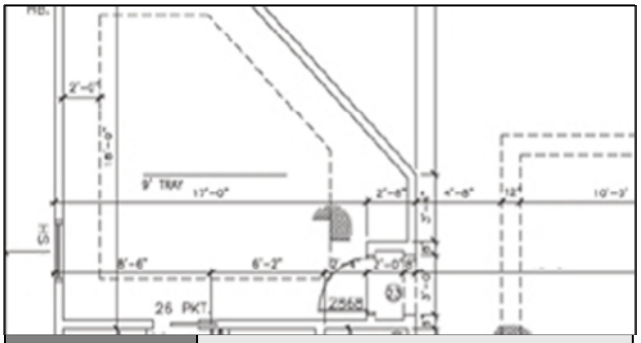


Figure 19

Internet est une source importante d'informations, notamment sur des cibles potentielles : plans de bâtiments publics sur des sites d'architecte, etc.

A la suite des attentats du 11 septembre, la situation a changé. C'est à cette époque qu'ont débuté des discussions intensives sur l'utilisation des TIC par les terroristes[442], sur fond de rapports[443] indiquant qu'Internet avait été utilisé pour préparer les attaques[444]. 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

---

438 *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.

439 *Rollins/ Wilson*, "Terrorist Capabilities for Cyberattack», 2007, page 10, available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf.

440 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: http://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 cyber-terrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, "A Framework for Understanding Terrorist Use of the Internet, 2006», available at: http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp

441 See: Report of the National Security Telecommunications Advisory Committee – Information Assurance Task Force – Electric Power Risk Assessment, available at: http://www.aci.net/kalliste/electric.htm.

442 See: *Lewis*, "The Internet and Terrorism», available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity»; http://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 seqq., available at: http://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 seqq; United States Department of State, "Pattern of Global Terrorism, 2000», in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism», available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities», 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror» in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/ lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

443 See: *Rötzer*, Telepolis News, 4.11.2001, available at: http://www.heise.de/tp/r4/artikel/9/9717/1.html.

444 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: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;

un rôle dans la préparation de l'offensive[445]. Dans ce contexte, les enquêteurs ont mis au jour les différentes façons dont les organisations terroristes utilisent Internet[446]. 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[447] 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[448], 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[449]. 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 des 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[450]. Pire, il n'existe toujours pas de définition admise par tous du terme "terrorisme"[451]. Ainsi, un rapport du *Congressional 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[452]. 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.

---

445 CNN, News, 04.08.2004, available at: http://www.cnn.com/2004/US/08/03/terror.threat/index.html.

446 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.;

447 *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension», in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism», 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

448 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;

449 One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.

450 Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyber Attacks 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 Cyber Terrorism, Cyber War and Other Cyber Threats; *Wilson* in CRS Report, Computer Attack and Cyber Terrorism – Vulnerabilities and Policy Issues for Congress, 2003.

451 See for example *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.

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[453]. 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 Qaida[454]. 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[455]. 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[456]. Ils utilisent les sites Internet et autres médias en ligne à des fins diverses: faire de la propagande[457], publier des messages pour justifier leurs activités[458], contacter et recruter[459] des membres, contacter et trouver des donateurs[460]. A noter que les sites Internet ont récemment été utilisés pour diffuser des vidéos d'exécution[461].

Collecte d'informations

Internet regorge d'informations sur des cibles potentielles[462]. Les architectes qui interviennent dans la construction de bâtiments publics mettent souvent les plans des bâtiments en ligne (Figure 21). 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[463]. 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 des armes[464]. Par ailleurs, certaines informations sensibles ou confidentielles insuffisamment protégées des robots de recherche sont accessibles via des moteurs de recherche[465]. En 2003, le Département de la Défense américain a été informé qu'un manuel de formation lié à Al Qaida indiquait qu'il était possible de

---

452 *Wilson* in CRS Report, Computer Attack and Cyber Terrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

453 ADL, Terrorism Update 1998, available at: http://www.adl.org/terror/focus/16_focus_a.asp.

454 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes see as well: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

455 Regarding the use of YouTube by terrorist organisations, see Heise News, news from 11.10.2006, available at: http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

456 *Zanini/Edwards*, "The Networking of Terror in the Information Age», in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

457 United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

458 Regarding the justification see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

459 *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 et. seqq.

460 See: *Conway*, "Terrorist Use of the Internet and Fighting Back», "Information and Security», 2006, page 16.

461 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.

462 Regarding the related challenges see *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.

463 *Levine*, Global Security, 27.06.2006, available at: http://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, Goolge Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: http://www.derstandard.at/?url/?id=2952935.

464 For further reference see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.

465 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».

trouver des informations sur des cibles potentielles en utilisant des sources publiques[466]. 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[467]. Un incident analogue a été signalé en Australie: des sites Internet du gouvernement contenaient des informations détaillées sur des cibles potentielles d'attaques terroristes[468]. 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[469].

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[470]. D'autres méthodes, plus directes, sont visées ici. Les jeux en ligne, par exemple, seraient utilisés pour préparer des attaques terroristes[471]. 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[472].

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[473]. En 2008, les services secrets occidentaux ont découvert un serveur Internet permettant d'échanger du matériel de formation et de communiquer[474]. On a en outre signalé plusieurs sites mis en place par des organisations terroristes pour coordonner leurs activités[475].

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

---

466 "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.

467 See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.

468 *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18,

469 See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: http://www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

470 See below.

471 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: http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html*; O'Hear*, Second Life a terrorist camp?, ZDNet,

472 Regarding other terrorist related activities in online games see: *Chen/Thoms*, Cyber Extremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 et seqq.

473 *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.

474 *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

475 *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

coordonner leurs attaques[476] et, selon la presse, pour échanger des instructions détaillées concernant les cibles et le nombre d'attaquants[477]. 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[478]. Internet peut être utilisé de diverses façons pour financer le terrorisme. Les organisations terroristes peuvent solliciter des donations en ligne par paiement électronique[479] ou indiquer sur leur 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)[480]. 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[481]. 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[482].

Attaques visant des infrastructures essentielles

Les infrastructures essentielles de l'information, cible de cyberdélits ordinaires tels que la fraude et le vol d'identité, pourraient aussi devenir une cible des organisations terroristes. Du fait de la dépendance grandissante

---

476 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

477 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: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;

478 The Commission analyzing the 9/11 attacks calculated that the costs for the attack could have been between 400.000 and 500.000 USD. 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 have been relatively small. Regarding the related challenges see as well *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

479 See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

480 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.

481 See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4,

482 Regarding virtual currencies see *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

à l'égard des technologies de l'information, les infrastructures essentielles sont plus vulnérables aux attaques[483]. C'est tout particulièrement le cas des systèmes interconnectés par des réseaux informatiques et des réseaux de communication[484]. 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[485]. Les enquêtes sur ces attaques, mais aussi leur prévention, présentent des difficultés bien spécifiques[486]. En effet, contrairement aux attaques physiques, les cyberattaques ne nécessitent pas la présence des attaquants sur les lieux qui sont ciblés[487]. De plus, les attaquants peuvent utiliser des moyens de communication anonymes et des technologies de chiffrement pour cacher leur identité[488]. Comme indiqué précédemment, pour enquêter sur de telles attaques, il faut disposer de moyens spéciaux: instruments de procédure, technologies d'investigation, personnel spécialement formé[489].

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[490]. 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[491]. 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[492].

Les incidents suivants survenus dans le transport aérien attestent de la vulnérabilité des infrastructures essentielles aux attaques par le réseau:

- Les systèmes d'enregistrement de la plupart des aéroports du monde reposent déjà sur des systèmes informatiques interconnectés[493]. En 2004, le ver informatique Sasser[494] a infecté des millions

---

483 *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension», in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism», 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf

484 *Lewis*, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002.

485 *Shimeall/Williams/Dunlevy*,"Countering cyber war», NATO review, Winter 2001/2002, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf

486 *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 et seq.

487 *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.

488 CERT Research 2006 Annual Report, page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf

489 Law Enforcement Tools and Technologies for Investigating Cyber Attacks, DAP Analysis Report 2004, available at: http://www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.

490 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

491 United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17,1996. Vol. 61, No. 138.

492 Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: http://www.gao.gov/new.items/d07706r.pdf.

493 *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: http://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.

494 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.

d'ordinateurs dans le monde, notamment ceux de grandes compagnies aériennes, entraînant l'annulation de plusieurs vols[495].

- Toutes les grandes compagnies aériennes proposent aujourd'hui à leurs clients d'acheter des billets en ligne et s'appuient sur les technologies de l'information pour effectuer diverses opérations. 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[496]. 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[497], rendant certains services indisponibles pendant plusieurs heures, voire plusieurs jours[498]. 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[499].
- 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[500], 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[501].

2.8.2 Guerre numérique ou "cyberguerre"

La guerre numérique ou "cyberguerre" désigne l'utilisation des TIC et d'Internet pour mener une guerre dans le cyberespace. Elle partage certaines caractéristiques avec le cyberterrorisme[502]. Les études se sont dans un premier temps concentrées sur la substitution des conflits armés classiques par des attaques assistées par ordinateur ou visant des ordinateurs[503]. Les attaques par réseau sont généralement moins coûteuses que les opérations militaires traditionnelles[504] et sont à la portée des petits Etats comme des grands.

---

495 *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.

496 *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks», available at: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

497 *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?», available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.

498 *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.

499 *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

500 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.

501 Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: http://www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: http://www.cio.com/article/print/30933.

502 See above: Chapter 2.8.1.

503 Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, "Strategic Information Warfare, 1996», available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

504 *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

Il est difficile de se protéger contre les cyberattaques. Etant donné qu'il existe aujourd'hui peu d'exemples de substitution de conflits armés par des attaques via Internet[505], les études actuelles portent essentiellement sur les attaques visant les infrastructures essentielles et sur le contrôle de l'information dans les conflits (Figure 20).

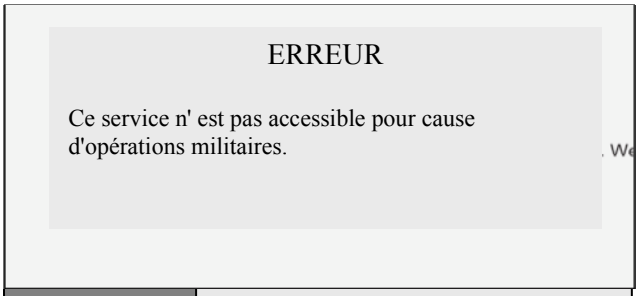


Figure 20

Ces dernières années, Internet est devenu un important médium d'échange d'informations et de propagande pendant les conflits armés. Est-il souhaitable de désactiver progressivement certains services Internet au cours des différentes phases majeures d'un conflit ? Si oui, dans quelle mesure ? Ces questions font souvent l'objet de discussions.

Du fait de l'importance des communications civiles et militaires, les infrastructures de l'information constituent une cible clé pendant les conflits armés. Rien ne prouve cependant que les attaques contre ces infrastructures seront à l'avenir perpétrées via Internet. Certaines personnes ont évoqué à propos d'attaques visant des systèmes informatiques en Estonie[506] et aux Etats-Unis[507] le terme de cyberguerre. Comme on ne peut, en l'occurrence, remonter avec certitude jusqu'à des organisations étatiques officielles, il est cependant difficile de qualifier ainsi ces attaques. Il est également difficile de classer sous le terme de "cyberguerre" des attaques contre des infrastructures menées avec des moyens physiques (armes, explosifs)[508].

Le contrôle de l'information est depuis longtemps une composante importante des conflits armés. L'information est en effet un outil qui permet d'influencer des populations, mais aussi de stigmatiser les forces armées. Dans ce contexte, le contrôle de l'information sur Internet est donc appelé à devenir un moyen d'influence toujours plus important.

2.8.3 Cyberblanchiment

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. On peut affirmer, en première approche, que les virements électroniques par Internet ont permis aux délinquants de s'affranchir des transactions en monnaie physique et du transport d'argent liquide. Cela étant, ceux-ci ont dû mettre au point de nouvelles techniques pour contourner les réglementations plus strictes mises en place afin de détecter les transferts électroniques suspects, réglementations qui reposent sur des obligations imposées aux établissements financiers impliqués dans les transactions[509].

Le blanchiment de capitaux s'effectue généralement en trois phases:

1. Le placement;
2. L'empilage;
3. L'intégration.

---

505 *Shimeall/Williams/Dunlevy*, "Countering cyber war», NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf; *Yurcik/Sharma*, "Internet Hack Back as an Active Defense Strategy», 2005, available at: http://www.projects.ncassr.org/hackback/ccsa05.pdf.

506 *Traynor,* "Russia accused of unleashing cyberwar to disable Estonia», The Guardian, 17.05.2007, available at: http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

507 *Thornburgh*, "Inside the Chinese Hack Attack», Time, 25.08.2005, available at: http://www.time.com/time/nation/printout/0,8816,1098371,00.html.

508 One example is the intentional destruction of communication infrastructure by NATO forces during the war in the former Republic of Yugoslavia. Regarding this issue, see: http://www.nato.int/kosovo/press/p990506c.htm.

509 One of the most important obligations is the requirement to keep records and to report suspicious transactions.

S'agissant du placement d'importantes sommes en liquide, l'utilisation d'Internet ne présente peut-être pas tant d'avantages concrets[510]. En fait, le recours à Internet est surtout intéressant pendant la phase d'empilage (masquage), par le biais notamment de cybercasinos, dont les transactions sont particulièrement difficiles à suivre pour les enquêteurs (Figure 21)[511].

La réglementation des transactions financières est aujourd'hui relativement limitée. De plus, grâce à Internet, les cyberdélinquants peuvent effectuer, pour un coût modique, des virements non imposables entre plusieurs pays. Par ailleurs, l'utilisation de monnaies virtuelles et le recours aux cybercasinos compliquent les enquêtes sur les techniques de blanchiment d'argent en ligne.

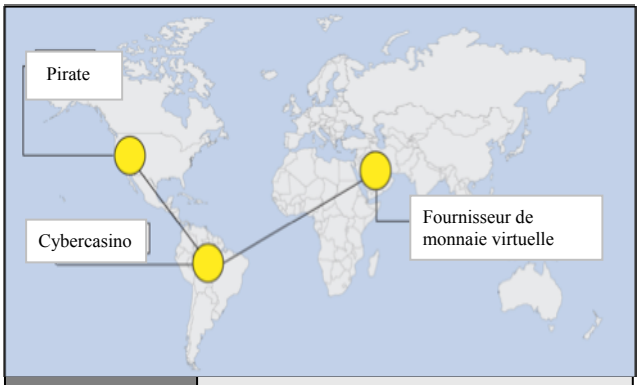


Figure 21

Le schéma ci-dessus illustre les relations qui existent entre les cybercasinos et les monnaies virtuelles dans les escroqueries de blanchiment d'argent reposant sur Internet. En utilisant ce type de service, les cyberdélinquants compliquent le travail des agences de répression qui cherchent à déterminer l'origine des virements et à identifier les auteurs.

1. Utilisation des monnaies virtuelles

La nécessité d'effectuer des 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, a été l'un des principaux moteurs du développement des monnaies virtuelles. Face à la demande, 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 *peer-to-peer* (de personne à personne) et de retrait en liquide[512]. 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[513].

2. 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[514]. De plus, les réglementations relatives aux casinos en ligne et hors ligne diffèrent souvent selon les pays[515]. Pour pouvoir 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, il est indispensable que les casinos consignent leurs transactions et les communiquent aux services de répression.

---

510 Offenders may tend to make use of the existing instruments e.g., the service of financial organisations to transfer cash, without the need to open an account or transfer money to a certain account.

511 For case studies, see: "Financial Action Task Force on Money Laundering», "Report on Money Laundering Typologies 2000 – 2001», 2001, page 8.

512 See: *Woda*, "Money Laundering Techniques With Electronic Payment Systems», Information & Security, Vol. 18, 2006, page 40.

513 Regarding the related challenges see below: Chapter 3.2.l.

514 The costs of setting up an online casino are not significantly larger than other e-commerce businesses.

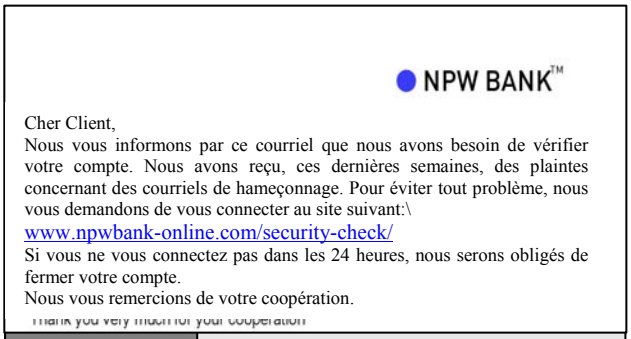
515 Regarding approaches to the criminalisation of illegal gambling, see below: Chapter 6.1.j.

Or les réglementations juridiques 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: si le prestataire de services financiers et le client ne se rencontrent pas, il peut être difficile de contrôler rigoureusement l'identité[516];
- l'absence de contact en face à face: il est difficile d'appliquer les procédures traditionnelles, qui reposent sur la connaissance du client;
- les transactions en ligne, qui mettent souvent en jeu des prestataires situés dans différents pays;
- l'absence de code législatif/pénal pour régir certains mécanismes, d'autant plus problématique lorsque les prestataires autorisent leurs clients à effectuer des transferts de valeurs selon un modèle *peer-to-peer*.

2.8.4 Hameçonnage

Pour obtenir des informations personnelles sur les utilisateurs, les cyberdélinquants ont mis au point différentes techniques, qui vont des logiciels espions[517] aux attaques par "hameçonnage"[518]. L'objectif du hameçonnage est d'amener les victimes à révéler des informations personnelles ou confidentielles[519]. On distingue plusieurs types d'attaques par hameçonnage[520], parmi lesquels le hameçonnage par courriel, qui comprend trois grandes phases. Au cours de la première phase, les cyberdélinquants identifient des sociétés légitimes qui proposent à leurs clients – les cibles potentielles – des services en ligne et communiquent avec eux par voie électronique. Il s'agit par exemple d'établissements financiers. Ils créent ensuite des sites Internet qui ressemblent aux sites de ces sociétés. Ces "sites d'espionnage" 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.).


NPW BANK™

Cher Client,
Nous vous informons par ce courriel que nous avons besoin de vérifier votre compte. Nous avons reçu, ces dernières semaines, des plaintes concernant des courriels de hameçonnage. Pour éviter tout problème, nous vous demandons de vous connecter au site suivant:\
www.npwbank-online.com/security-check/
Si vous ne vous connectez pas dans les 24 heures, nous serons obligés de fermer votre compte.
Nous vous remercions de votre coopération.

Figure 22

Les courriels de hameçonnage sont conçus pour ressembler à des courriels émanant de sociétés légitimes dans le but d'amener la victime à divulguer des informations confidentielles. L'auteur de ce type de courriel cible très souvent les clients d'établissements financiers.

Pour les orienter vers ces sites d'espionnage, les cyberdélinquants envoient aux internautes des courriels qui ressemblent à ceux normalement émis par les sociétfsés dont ces derniers sont clients (Figure 22)[521], commettant souvent par là-même une violation de la marque commerciale[522]. 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, et il lui est précisé que des mesures seront prises s'il refuse de coopérer (fermeture de compte par exemple). Pour

---

516 See: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000 – 2001», 2001, page 2.

517 Regarding the threat of spyware, see *Hackworth*, "Spyware, Cybercrime and Security», IIA-4.

518 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: http://www.usdoj.gov/opa/report_on_phishing.pdf

519 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

520 The following section describes email-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: http://www.techweb.com/wire/security/186701001.

521 "Phishing» shows a number of similarities to spam e-mails. It is thus likely that organised 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: Chapter 2.5.7.

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 est connecté à un site d'espionnage[523].

Dès que les données personnelles sont divulguées, les cyberdélinquants se connectent au compte de la victime et effectuent des opérations: virement, demande de passeport, ouverture de compte, etc. Les attaques réussies sont en augmentation, ce qui montre bien le potentiel de cette technique[524]. Plus de 55 000 sites de hameçonnage ont été signalés à l'APWG[525] en avril 2007[526]. Les techniques de 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 Etats-Unis, qui peuvent servir à commettre des infractions de type "vol d'identité"[527].

2.9 Impact économique de la cybercriminalité

Cela ne fait aucun doute, les pertes financières dues à la criminalité informatique et à la criminalité sur Internet sont importantes. Plusieurs études publiées récemment témoignent ainsi de l'impact économique majeur de la cybercriminalité[528]. L'estimation des pertes financières pose le même problème que la production de statistiques sur la criminalité: il est difficile de savoir dans quelle mesure les chiffres publiés sont exacts, car il est probable que bien des personnes ne signalent pas les infractions dont elles sont victimes[529].

2.9.1 Synthèse des résultats publiés par certaines études

L'étude *Computer Crime and Security Survey 2007*, réalisée par le CSI (Computer Security Institute, institut de sécurité informatique) propose une analyse de l'impact économique de la cybercriminalité[530], fondée 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. Elle concerne surtout les Etats-Unis[531].

---

522 Regarding related trademark violations, see above 2.6.2.

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

524 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).

525 Anti-Phishing Working Group. For more details, see: http://www.antiphishing.org.

526 "Phishing Activity Trends», Report for the Month of April 2007, available at: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

527 See above: Chapter 2.7.3.

528 See, for example: "Deloitte 2007 Global Security Survey» – September 2007; "2005 FBI Computer Crime Survey»; "CSI Computer Crime and Security Survey 2007» is available at: http://www.gocsi.com/; "Symantec Internet Security Threat Report», September 2007, available at: http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport; "Sophos Security Threat Report», July 2007, available at: http://www.sophos.com/pressoffice/news/articles/2007/07/securityrep.html.

529 See for example: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, 2002, page 27, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; See also ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

530 The "CSI Computer Crime and Security Survey 2007», available at: http://www.gocsi.com/

531 See "CSI Computer Crime and Security Survey 2007», page 1, available at: http://www.gocsi.com/.

En tenant compte du cycle économique, l'étude avance que, après une augmentation continue, l'impact financier de la cybercriminalité a diminué à partir de 2002 et les années suivantes. L'étude laisse entendre que ce résultat est discutable; il est d'ailleurs difficile de comprendre pourquoi le nombre d'infractions signalées et la perte moyenne supportée par les victimes ont diminué. En 2006, le montant des pertes a de nouveau augmenté. L'étude n'explique ni la diminution des pertes en 2002 ni son augmentations en 2006. Sur les vingt et une catégories recensées, les pertes les plus importantes (en dollars) concernent les fraudes financières, les virus, les accès non autorisés aux systèmes et les vols de données confidentielles. Les pertes totales supportées en 2006 par l'ensemble des personnes ayant répondu s'élevaient à quelque 66,9 millions USD.

Après plusieurs années de diminution, la perte moyenne par organisation ayant répondu est en augmentation. A noter qu'elle était, en 2006, de 345 000 USD et, en 2001, presque dix fois supérieure (3,1 million USD). Les pertes moyennes dépendent fortement de la nature des organisations qui répondent aux sondages: si, pour une année donnée, des petites et moyennes entreprises (PME) répondent en majorité et que, l'année suivante, elles sont remplacées par de plus grandes entreprises, les statistiques sont fortement impactées.

L'étude *Computer Crime Survey 2005*[532] menée par le FBI adopte une approche analogue à celle de l'étude du CSI, mais avec un panel plus important et plus étendu[533]. Selon cette étude, le coût des incidents de sécurité dus aux infractions informatiques et aux infractions sur Internet s'élevait à 21,7 millions USD[534]. Les infractions les plus fréquentes détectées par les organisations ayant répondu étaient les attaques par virus, les attaques par logiciel espion, la scanne de ports et le sabotage de données ou de réseaux[535]. L'étude *Computer Crime Survey 2005* contient une estimation des pertes totales pour l'économie des Etats-Unis[536], fondée sur les pertes moyennes[537] et sur l'hypothèse selon laquelle 20% des organisations américaines ont été victimes de la cybercriminalité. Cette estimation indique une perte totale de 67 milliards USD[538]. Cela étant, la représentativité des estimations et la cohérence du panel d'année en année demeurent discutables[539].

Le rapport *Computer Economics Malware Report*[540] de 2007 s'attache à déterminer l'impact des logiciels malveillants sur l'économie mondiale en additionnant les coûts totaux estimés[541] qui sont générés par les attaques de ce type de logiciel. L'un des principaux résultats de ce rapport est le changement de cap des concepteurs de logiciels malveillants: autrefois motivée par le vandalisme, leur action vise aujourd'hui principalement à générer des profits. Selon le rapport, les pertes financières dues aux logiciels malveillants ont

---

532 "2005 FBI Computer Crime Survey».

533 The 2005 FBI Computer Crime Survey is based on data of 2066 United States institutions (see 2005 FBI Computer Crime Survey, page 1) while the 2007 CSI Computer Crime and Security Survey is based on 494 respondents (See CSI Computer Crime and Security Survey 2007, page 1, available at: http://www.gocsi.com/).

534 See "2005 FBI Computer Crime Survey», page 10.

535 See "2005 FBI Computer Crime Survey», page 6.

536 See *Evers*, "Computer crimes cost $67 billion, FBI says», ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

537 "2005 FBI Computer Crime Survey», page 10.

538 See "2005 FBI Computer Crime Survey», page 10 As well as *Evers*, "Computer crimes cost $67 billion, FBI says», ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

539 The report makes available useful details of those institutions that responded. See "CSI Computer Crime and Security Survey 2007», page 3, available at: http://www.gocsi.com/

540 "2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code». A summary of the report is available at: http://www.computereconomics.com/article.cfm?id=1225.

541 The costs covered by the report include labour costs to analyze and repair an infected computer system, the loss of user productivity and the loss of revenue due to a loss of performance of infected computer systems. For more information, see the summary of the report available at: http://www.computereconomics.com/article.cfm?id=1225.

atteint un maximum en 2000 (17,1 milliards USD) et en 2004 (17,5 milliards USD), mais ont diminué depuis 2004 pour atteindre, en 2006, 13,3 milliards USD. Cela étant, il demeure des incertitudes quant aux résultats de l'étude, de même qu'il est difficile de savoir si les statistiques sur l'impact des logiciels malveillants sont réalistes. Il y a en effet des différences importantes entre les pertes signalées et les dégâts avérés, comme le montre l'exemple du ver Sasser. Ce ver avait infecté, selon les signalements, des millions de systèmes informatiques[542]. Or, au cours de la procédure civile contre le concepteur du programme, très peu d'entreprises et de particuliers ont répondu à la demande qui leur était faite d'apporter la preuve des pertes subies et de se joindre à la procédure judiciaire. Le concepteur du virus a finalement été condamné à payer des dédommagements inférieurs à 10 000 USD[543].

2.9.2 Difficultés concernant les statistiques sur la cybercriminalité

Il est difficile de savoir si les statistiques sur l'impact économique de la cybercriminalité sont représentatives et si elles fournissent des informations fiables sur l'étendue des pertes[544]. En effet, on ne sait pas avec certitude dans quelle mesure les cyberdélits sont signalés, non seulement dans les sondages, mais aussi aux agences de répression. Les autorités chargées de la lutte contre la cybercriminalité encouragent les victimes à signaler ces délits[545]. Si elles disposaient de données plus précises sur l'incidence réelle de la cybercriminalité, elles pourraient poursuivre les cyberdélinquants plus efficacement, décourager les tentatives d'attaque et adopter une législation mieux adaptée et plus efficace.

Plusieurs organisations publiques et privées ont tenté de mesurer les coûts directs et indirects liés aux logiciels malveillants. S'il est difficile d'estimer les coûts infligés aux entreprises, il est encore plus difficile d'évaluer les pertes financières causées par les logiciels malveillants et autres programmes analogues aux particuliers. Des données éparses montrent cependant que les dommages peuvent être très importants[546]. Les coûts pour les particuliers revêtent diverses formes: dégâts directs causés aux matériels et logiciels, pertes financières et autres dues au vol d'identité ou à d'autres pratiques frauduleuses. Bien que les estimations diffèrent, le tableau d'ensemble est assez cohérent.

Les entreprises, de leur côté, décident parfois de ne pas signaler les cyberdélits dont elles sont victimes, et ce pour plusieurs raisons:

Premièrement, la crainte de subir les effets d'une publicité négative qui entacherait leur réputation[547]. De fait, en annonçant que des pirates sont parvenus à accéder à ses serveurs, une entreprise risquerait de perdre la confiance de ses clients, et les pertes et les conséquences globales pourraient se révéler supérieures aux pertes dues à la seule cyberattaque. Mais, d'un autre côté, en refusant de signaler les cyberdélits et de poursuivre en justice leurs auteurs, on encourage la récidive.

---

542 See: "Sasser Worm rips through the Internet», CNN News, 05.05.2004, available at: http://edition.cnn.com/2004/TECH/internet/05/05/sasser.worm/index.html

543 See Heise News, 06.07.2005, available at: http://www.heise.de/newsticker/meldung/print/61451.

544 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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

545 "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: http://www.heise-security.co.uk/news/80152.

546 ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

547 See *Mitchison/Urry*, "Crime and Abuse in e-Business, IPTS Report», available at: http://www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm

Deuxièmement, les victimes peuvent estimer que les services de répression ne parviendront pas à identifier les malfaiteurs[548]. En effet, étant donné le nombre important de cyberdélits en comparaison des quelques enquêtes qui aboutissent, les victimes peuvent logiquement douter de l'intérêt qu'il y a à signaler les infractions[549].

Enfin, en automatisant leurs attaques, les cyberdélinquants poursuivent l'objectif de réaliser le maximum de profits en lançant un grand nombre d'attaques visant de petits montants (c'est le cas de la fraude aux avances sur commission[550] par exemple). Or les victimes préféreront souvent, pour de petits montants, ne pas enclencher des procédures de signalement qui prennent du temps. De fait, les cas signalés concernent souvent des pertes très importantes[551]. En ne visant que de petits montants, les malfaiteurs conçoivent donc des escroqueries qui, pour la plupart, ne seront pas signalées.

3 Les enjeux de la lutte contre la cybercriminalité

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, alors que, 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

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[552].

Mais l'automatisation des processus d'investigation peut se révéler difficile. 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

Figure 23

Dans cet exemple, les experts informatiques spécialisés en criminalistique sont parvenus à défaire les modifications apportées à l'image et à reconstruire le visage du suspect.

548 See Smith, "Investigating Cybercrime: Barriers and Solutions», 2003, page 2, available at: http://www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf

549 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: http://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: http://www.interpol.int/Public/THB/vico/Default.asp.

550 See SOCA, "International crackdown on mass marketing fraud revealed, 2007», available at: http://www.soca.gov.uk/downloads/massMarketingFraud.pdf.

551 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 5,100 USD each. The number of reported offences is very low, while the average loss of those offences is the high.

552 See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: https://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: https://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.

analyser a préalablement été évaluée, la valeur de hachage stockée dans une base de données et l'image non modifiée[553].

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 (Figure 23). Les experts informatiques spécialisés en criminalistique sont parvenus à défaire les modifications apportées à l'image et à reconstruire le visage du suspect[554]. Si cette enquête réussie met clairement en évidence le potentiel des spécialistes informatiques, 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 tâche blanche, l'identification aurait été impossible.

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[555]. Les bâtiments[556], les voitures et les services aériens reposent également sur les TIC pour effectuer des fonctions de commande et de gestion (Figure 24)[557], de même que 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 quotidienne[558].

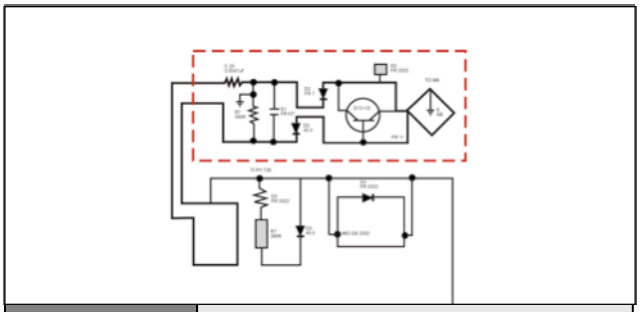


Figure 24

Les techniques informatiques et les dispositifs électroniques remplacent de plus en plus souvent les fonctions manuelles.

Cette dépendance croissante à l'égard des TIC augmente la vulnérabilité des systèmes et des services liés aux infrastructures essentielles[559]. Des interruptions de service, même de courte durée, peuvent entraîner de lourdes

---

553 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.

554 For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: http://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: http://www.interpol.int/Public/THB/vico/Default.asp

555 It was reported that the United States Department of Defence had to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

556 Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

557 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.

558 *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 seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf.

559 Re 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.

pertes financières. Les services civils (entreprises de commerce électronique[560], etc.) ne sont pas les seuls concernés, la dépendance à l'égard des TIC met aussi gravement en danger les communications militaires[561].

Les infrastructures techniques existantes présentent plusieurs faiblesses, parmi lesquelles la monoculture ou homogénéité des systèmes d'exploitation. Bien des particuliers et des PME utilisent en effet le système d'exploitation de Microsoft[562], cible dès lors privilégiée des cyberdélinquants[563].

La dépendance de la société vis-à-vis des TIC n'est pas un phénomène propre aux pays occidentaux[564]: les pays en développement aussi sont confrontés aux problèmes de prévention des attaques visant leurs infrastructures et leurs utilisateurs[565]. Grâce au développement de technologies moins onéreuses en termes d'infrastructures, telles que WiMAX[566], les pays en développement peuvent aujourd'hui proposer des services Internet à un plus grand nombre d'utilisateurs. En théorie, ces pays devraient 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[567] n'ont pu porter leurs fruits qu'en raison de l'insuffisance des mesures de protection[568]. Or 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[569].

---

560 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 computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. 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: http://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.

561 *Shimeall/Williams/Dunlevy*,"Countering cyber war», NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf.

562 One analysis by "Red Sheriff» in 2002 stated that more than 90% of the users worldwide use Microsoft`s operating systems (source: http://www.tecchannel.de – 20.09.2002).

563 Re the discussion about 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 http://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.

564 With regards to the effect of spam on developing countries, see: "Spam issues in developing countries, 2005», available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

565 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: http://www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; "World Information Society Report 2007», page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

566 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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking»; *Nuaymi*, "WiMAX Technology for Broadband Wireless Access».

567 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf

568 See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: http://www.upi.com/Security_Terrorism/Analysis/ 2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

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

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[570].

3.2.2 Nombre d'utilisateurs

La popularité d'Internet et de ses services augmente rapidement et on compte aujourd'hui un milliard d'internautes dans le monde (Figure 25)[571]. Les sociétés informatiques et les FAI s'intéressent tout particulièrement aux pays en développement dont le potentiel de croissance est le plus élevé[572]. En 2005, le nombre d'internautes dans ces pays a dépassé celui des pays industrialisés[573], et il devrait encore augmenter sous l'effet de la baisse du prix du matériel et du développement des accès sans fil[574].

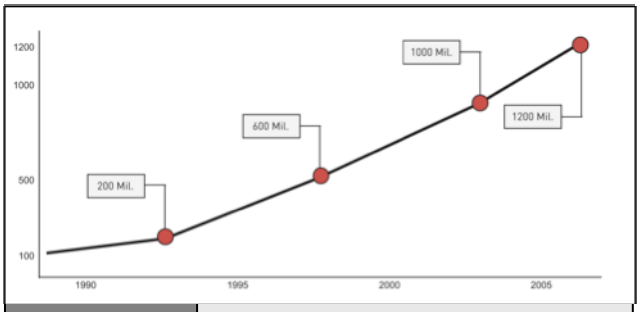


Figure 25

On compte, à l'heure actuelle, plus d'un milliard d'internautes.

Le nombre de cibles potentielles et de cyberdélinquants augmente avec le nombre d'internautes[575]. Il est difficile d'estimer combien de personnes utilisent Internet dans le but de mener des activités illicites, mais, quand bien même ils ne représenteraient que 0,1% des internautes, les cyberdélinquants dépasseraient 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[576].

Etant 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 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[577].

---

570 See below: Chapter 4.

571 According to the ITU, there were 1.14 billion Internet users by the start of 2007, available at: http://www.itu.int/ITU-D/icteye.default.asp.

572 See *Wallsten*, "Regulation and Internet Use in Developing Countries», 2002, page 2.

573 See "Development Gateway's Special Report, Information Society – Next Steps?», 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

574 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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking»; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

575 Regarding the necessary steps to improve cybersecurity, see: "World Information Society Report 2007», page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

576 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: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: Chapter 2.8.d.

577 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.

3.2.3 Disponibilité des équipements et de l'accès

Pour commettre des cyberdélits, il suffit de disposer d'un équipement élémentaire, composé généralement des éléments suivants:

- le matériel;
- le logiciel;
- l'accès à Internet.

S'agissant du matériel, il importe de souligner que la puissance des ordinateurs est en constante augmentation[578]. A noter également plusieurs projets visant à promouvoir l'utilisation des TIC dans les pays en développement[579]. Quoi qu'il en soit, 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.

S'agissant du logiciel, certains outils spécialisés peuvent faciliter la commission de cyberdélits, notamment les programmes[580] conçus pour détecter des ports ouverts ou contourner des protections par mot de passe[581], programmes disponibles en téléchargement. Face aux sites "miroirs" et aux échanges *peer-to-peer*, il est difficile de limiter l'expansion de ces logiciels, qu'on peut se procurer de plus en plus facilement[582].

Dernière condition nécessaire à la commission d'un cyberdélit: disposer d'un accès à Internet. Bien que le coût des accès[583] 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[584]. 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[585]. Les moyens d'accès aux réseaux les plus fréquemment utilisés par les cyberdélinquants sont:

- les terminaux publics d'accès à Internet;
- les réseaux (hertziens) libres (Figure 26)[586];

---

578 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/.

579 Chapter six, "World Information Society Report 2007», ITU, Geneva, available at: http://www.itu.int/wisr/

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

581 *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention», page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf.

582 In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime. See below: Chapter 6.1.13.

583 Regarding the costs, see: The World Information Society Report, 2007, available at: http://www.itu.int/wisr/

584 See "Development Gateway's Special Report, Information Society – Next Steps?», 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

585 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: http://www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

586 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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

- les réseaux piratés;
- 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[587]. L'identification systématique a cependant ses détracteurs[588]. 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[589]. Certains ont également fait valoir qu'une telle limitation pourrait constituer une violation des droits de l'homme[590]. 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 infomation. Dans l'affaire *Autronic c. Suisse*[591], 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.

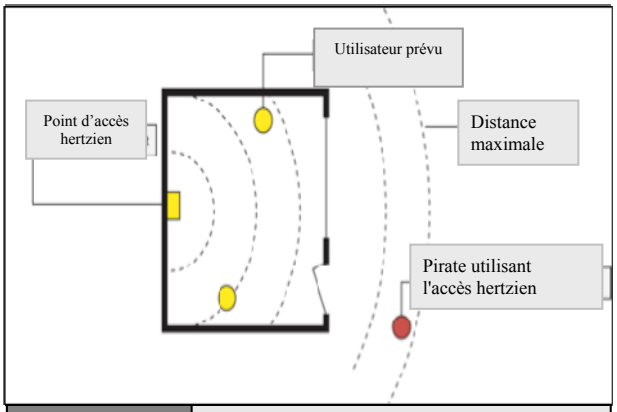


Figure 26

Accéder à Internet sans laisser de traces est une priorité majeure pour de nombreux cyberdélinquants. Ce schéma illustre la façon dont un cyberdélinquant procède pour utiliser le signal émis par un point d'accès hertzien libre afin de se connecter au réseau. Dans une telle configuration, il est quasiment impossible d'identifier le malfaiteur.

3.2.4 Disponibilité de l'information

On trouve sur Internet des millions de pages[592] d'information régulièrement mises à jour. Quiconque souhaite participer peut mettre en ligne et actualiser des informations. Wikipédia[593], encyclopédie en ligne dans laquelle

---

587 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

588 See below: Chapter 6.2.11.

589 Regarding the impact of censorship and control, see: *Burnheim*, "The right to communicate, The Internet in Africa», 1999, available at: http://www.article19.org/pdfs/publications/africa-internet.pdf

590 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: http://www.undp.org/dpa/annualreport2001/arinfocom.pdf; "Background Paper on Freedom of Expression and Internet Regulation», 2001, available at: http://www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

591 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.

592 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: http://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.

593 http://www.wikipedia.org

tout internaute peut publier ses articles, est un exemple du succès des plates-formes de contenu généré par l'utilisateur[594].

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[595]. Certains rapports soulignent d'ailleurs les risques liés à l'utilisation des moteurs de recherche à des fins illicites[596]. 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 (Figure 27)[597]. Avant le développement d'Internet, ces informations étaient certes disponibles, mais d'accès plus difficile; aujourd'hui, tout internaute peut y avoir accès.

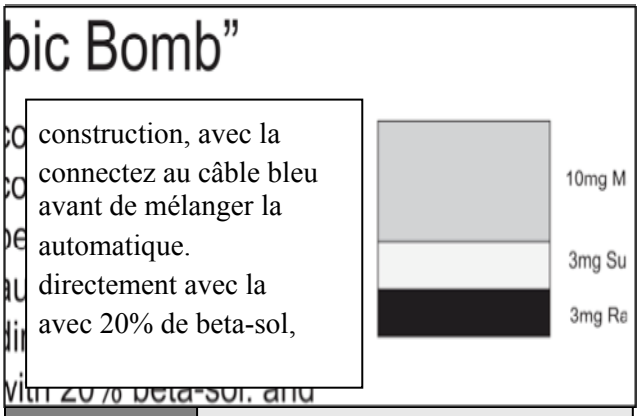


Figure 27

On peut très facilement trouver sur Internet des instructions sur la fabrication d'armes et d'explosifs. On peut voir, sur cette figure, des explications concernant la fabrication d'une bombe à partir différents produits, tous disponibles en pharmacie.

Les cyberdélinquants peuvent également utiliser les moteurs de recherche pour analyser leurs cibles[598]. 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[599]. Les

---

594 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: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

595 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.

596 See Nogguchi, "Search engines lift cover of privacy», The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

597 One example is the "Terrorist Handbook» – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

598 See *Thomas*, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'», Parameters 2003, page 112 et seqq., available at: http://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: http://www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

599 "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy». The reports about the sources of the quotation varies: 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: http://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: http://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.

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[600].

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[601]: 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.

A l'origine, Internet a été conçu comme un réseau militaire[602], reposant sur une architecture décentralisée afin de préserver la fonctionnalité principale intacte et opérationnelle, même en cas d'attaque de certains éléments du réseau. De 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[603].

De ce fait, les internautes peuvent, par exemple, contourner les techniques de filtrage[604] en utilisant des services chiffrés de communication anonyme[605]. Il est norma-lement 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

---

600 See Telegraph.co.uk, news from January the 13th 2007.

601 See for example, *Sadowsky/Zambrano/Dandjinou*, "Internet Governance: A Discussion Document», 2004, available at: http://www.internetpolicy.net/governance/20040315paper.pdf;

602 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: http://www.isoc.org/internet/history/brief.shtml.

603 *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues».

604 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: http://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: http://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: http://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: http://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.

605 For more information regarding anonymous communications, see below: Chapter 3.2.l2.

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 (Figure 28).

3.2.6 Dimensions internationales

De nombreux processus de transfert de données mettent en jeu plusieurs pays[606]. Les protocoles utilisés sur Internet sont conçus pour optimiser le routage en cas d'indisponibilité temporaire des liens de communication directs[607]. 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[608]. Par ailleurs, de nombreux services Internet reposent sur d'autres services situés à l'étranger[609]. 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[610].

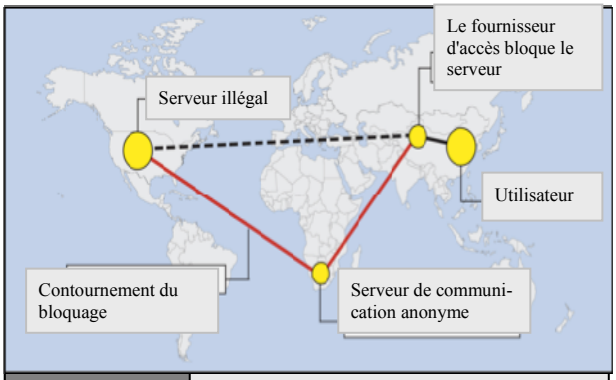


Figure 28

Ce schéma illustre la possibilité de contournement des mécanismes de contrôle central installés par les fournisseurs d'accès. Si un fournisseur d'accès installe une technologie de filtrage, les requêtes de l'utilisateur sont bloquées. Ce mécanisme de contrôle peut être contourné : il suffit pour cela que l'utilisateur passe par un serveur de communication anonyme qui chiffre les requêtes. Dans cet exemple, le fournisseur n'a pas accès aux requêtes envoyées au serveur de communication anonyme et ne peut donc pas bloquer les sites Internet.

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[611]. 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[612]. Il est donc essentiel d'obtenir le soutien et la participation des autorités de tous les pays impliqués.

---

606 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.

607 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».

608 See *Kahn/Lukasik*, "Fighting Cyber Crime and Terrorism: The Role of Technology,» presentation at the Stanford Conference, December 1999, page 6 et seqq.; *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.

609 One example of the international cooperation of companies and the 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 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)*.

610 See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future», No.6, available at: http://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 Simplyfing Data Storage and Management.

611 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 seqq., 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 seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

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

La coopération en matière de cybercriminalité peut difficilement reposer sur les principes de l'entraide judiciaire traditionnelle. En effet, les enquêteurs doivent agir très rapidement[613], alors qu'ils sont souvent freinés par les formalités et le temps nécessaires pour collaborer avec des services de répression étrangers[614]. Il faut souvent du temps pour organiser une opération d'entraide judiciaire traditionnelle, ce qui est problématique, car les données cruciales qui permettent de retrouver l'origine d'une infraction sont souvent effacées après un laps de temps très court[615]. Autre difficulté, le principe de la double incrimination[616], en vertu duquel l'infraction en cause doit être incriminée de manière comparable dans la législation de tous les pays concernés[617]. Ainsi, pour compliquer l'enquête, les cyberdélinquants intègrent parfois délibérément un troisième pays dans leur attaque[618].

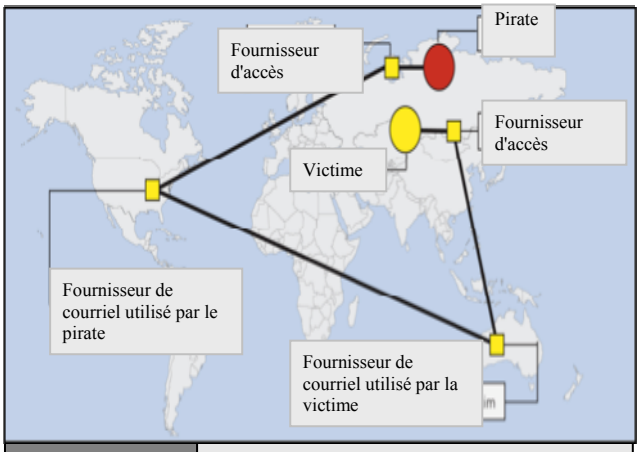


Figure 29

Ce schéma illustre le fait que, même si le pirate et la victime sont situés dans le même pays, un courriel avec un contenu illicite peut transiter par plusieurs pays. Même si ce n'est pas le cas, les processus de transfert de données peuvent être dirigés vers l'extérieur du pays, puis rediriger vers l'intérieur.

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 (Figure 29)[619]. 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[620] du G8 et les dispositions relatives à la coopération internationale énoncées dans la Convention sur la cybercriminalité du Conseil de l'Europe[621].

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

613 See below: Chapter 3.2.10.

614 See *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;

615 See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime», Computer Law Review International 2006, 142.

616 Dual criminality exists if the offence is a crime under both the requestor 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).

617 Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime», 269, available at http://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.

618 See: *Lewis*, "Computer Espionage, Titan Rain and China», page 1, available at: http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

619 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: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

620 See below: Chapter 6.3.8.

621 See below: Chapter 6.3.

demande beaucoup d'efforts et de temps. Les cyberdélinquants cherchent donc à éviter les pays dotés d'une législation forte en matière de cybercriminalité (Figure 30)[622].

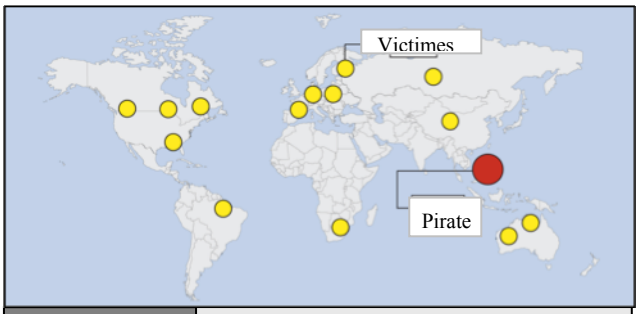


Figure 30

Pour commettre leurs infractions, les pirates peuvent décider de se connecter à Internet de n'importe quel point de la planète, ou presque. Leurs critères de décision incluent notamment : l'état d'avancement de la législation en matière de cybercriminalité, l'efficacité des agences de répression et la possibilité de se connecter à Internet de façon anonyme.

L'un des enjeux majeurs du combat contre la cybercriminalité est de lutter contre les "refuges"[623]. 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[624] et responsable de l'infection de millions d'ordinateurs dans le monde, est tout à fait représentatif de cette problématique[625]: 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[626]. 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;

---

622 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.

623 This issue was addressed by a number of international organisations. The 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: http://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: Chapter 5.2.

624 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: http://www.gao.gov/archive/2000/ai00181t.pdf.

625 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.

626 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», http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

- elle augmente l'ampleur et l'impact des processus;
- 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[627]. Grâce à l'automatisation, les cyberdélinquants peuvent intensifier leurs activités et, par exemple, envoyer automatiquement plusieurs millions de courriels de pollupostage[628] en masse[629] (Figure 31). Les tentatives de piratage aussi sont souvent automatisées[630]: on n'en compte pas moins de 80 millions chaque jour[631], commises à l'aide d'outils logiciels[632] capables d'attaquer des milliers de systèmes informatiques en quelques heures[633]. 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[634]. Or, plus la perte unitaire est faible, moins il y a de risques que la victime signale l'infraction.

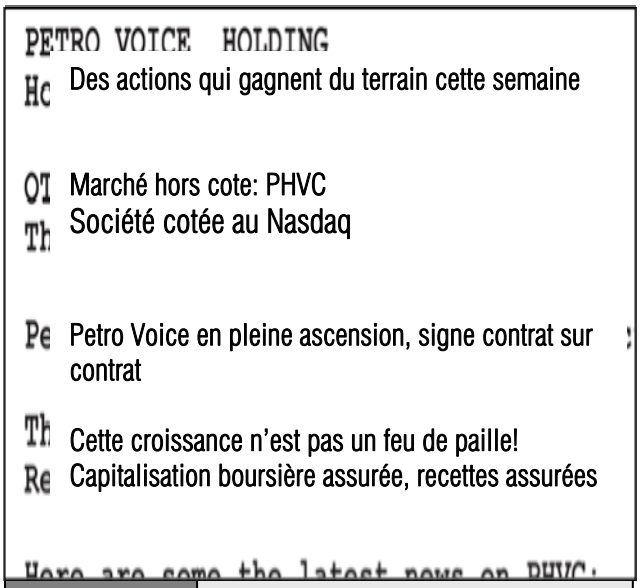


Figure 31

La diffusion des courriels de pollupostage est un exemple de l'utilisation de l'automatisation. Des millions de courriels peuvent être envoyés en très peu de temps.
Légende: identique à la Figure 11

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 pollupostage[635]. 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.

---

627 One example of low- cost services that are automated is e-mail. The automation of registration allows providers offer e-mail addresses free of charge. For more information on the difficulties of prosecuting Cybercrime involving e-mail addresses, see below: Chapter 3.2.l.

628 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: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

629 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: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.

630 *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention», page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf.

631 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: http://www.hackerwatch.org.

632 Regarding the distribution of hacking tools, see: CC Cert, "Overview of Attack Trends», 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.

633 See CC Cert, "Overview of Attack Trends», 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.

634 Nearly 50% of all fraud complains reported to the United States Federal Trade Commission are related to a amount paid between 0 and 25 USD. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission , available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

635 See "Spam Issue in Developing Countries», Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

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[636] des ordinateurs pris isolément qui fait pro importantes, de ces machines.

On peut citer, à ce titre, les attaques récentes essuyées par des sites Internet de l'administration publique en Estonie[637]. Selon certaines analyses, les attaques ont été commises par des milliers d'ordinateurs appartenant à un "botnet"[638], c'est-à-dire un groupe d'ordinateurs infectés sur lesquels s'exécutent des programmes commandés à distance[639]. 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 (Figure 32). Les botnets sont utilisés pour collecter des informations sur les cibles ou pour lancer des attaques massives[640].

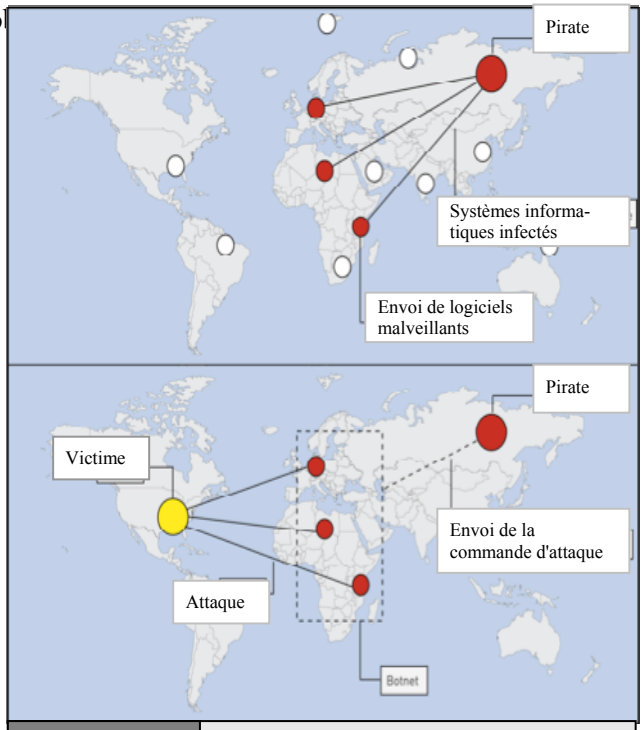


Figure 32

Ces deux schémas montrent la création et l'utilisation d'un botnet.

Ces dernières années, les botnets sont devenus de graves menaces pour la cybersécurité[641]. Leur taille est variable: certains ne compte que quelques ordinateurs, d'autres plus d'un million[642]. Selon certaines analyses en cours, jusqu'à 25% de l'ensemble des ordinateurs connectés à Internet pourraient être infectés par des logiciels dont le but est de les inclure dans un botnet[643]. Les botnets peuvent être utilisés pour commettre divers cyberdélits, notamment:

- attaques par refus de service[644];

---

636 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

637 Regarding the attacks, see: Lewis, "Cyber Attacks Explained», 2007, available at: http://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: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

638 See: *Toth*, "Estonia under cyber attack», http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

639 See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime», 2005, page 3, available at: http://www.cert.org/archive/pdf/Botnets.pdf;

640 See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime», 2005, available at: http://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».

641 See "Emerging Cybersecurity Issues Threaten Federal Information Systems», GAO, 2005, available at: http://www.gao.gov/new.items/d05231.pdf.

642 *Keizer*, Duch "Botnet Suspects Ran 1.5 Million Machines», TechWeb, 21.10.2005, available at http://www.techweb.com/wire/172303160

643 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.

644 E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, "Estonia under cyber attack», http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

- pollupostage[645] ;

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[646]. 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. Etant 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.

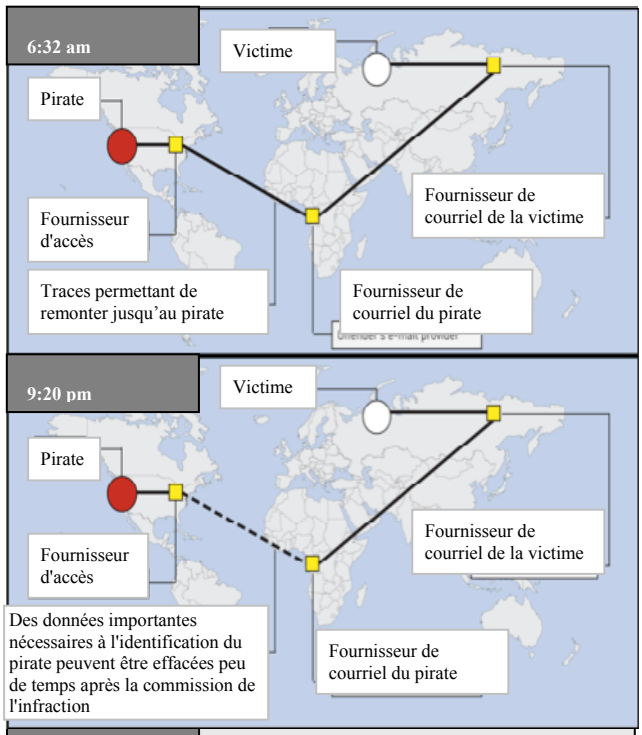


Figure 33

Ces schémas illustrent l'importance d'une réaction immédiate dans les enquêtes de cybercriminalité. Des données essentielles produites pendant le processus d'envoi d'un courriel, qui pourraient permettre d'identifier le pirate, sont souvent effacées peu de temps après l'envoi. Sans ces données, l'identification du pirate est souvent impossible.

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[647].

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 (Figure 33). 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[648]. 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[649].

---

645 "Over one million potential victims of botnet cyber crime», United States Department of Justice, 2007, available at: http://www.ic3.gov/media/initiatives/BotRoast.pdf.

646 *Staniford/Paxson/Weaver*, "How to Own the Internet in Your Space Time», 2002, available at: http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

647 *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime», Computer Law Review International, 2006, page 142.

648 *Gercke*, DUD 2003, 477 et seq.; *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues».

649 Regarding the necessary instruments, see below: Chapter 6.2. One solution that is currently being discussed is data retention. Re 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.

Les "procédures de gel rapide"[650] et les points de contact du réseau 24/7[651] 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[652]), 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[653]. 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:

- les jeux en ligne;
- 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[654].

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[655]. D'où la nécessité de nouvelles techniques d'interception[656].

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

---

650 The term "quick freeze» is used to describe the immediate preservation of data on request of law enforcement agencies. For more information, see below : Chapter 6.2.4.

651 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: Chapter 6.3.8.

652 The graphical user interface called World Wide Web (WWW) was created in 1989.

653 The development of the graphical user interface supported content-related offences in particular. For more information, see above: Chapter 2.5.

654 For more information see above: Chapter 2.5.5.

655 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 http://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.

656 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.

Internet via des réseaux hertziens[657]. 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[658]. 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 personnes qui se sont connectées.

3.2.12 Communications anonymes

Certains services Internet reposent sur des communications anonymes[659]. Qu'il s'agisse d'une offre visant à protéger l'utilisateur ou d'une simple caractéristique du service, l'anonymat est un obstacle à l'identification des cyberdélinquants. Parmi les services concernés, on peut citer – éventuellement en combinaison (Figures 34 et 35):

- les terminaux publics d'accès à Internet (dans les aéroports, les cybercafés, etc.)[660];
- les réseaux hertziens[661];les services mobiles prépayés sans identification;
- les offres de stockage de pages Internet sans identification;
- les serveurs de communication anonyme[662];
- les services de courriel anonyme[663].

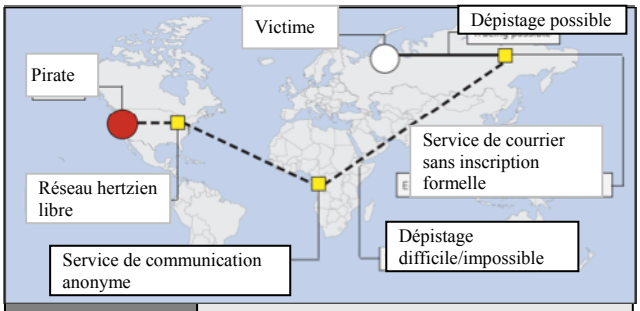


Figure 34

Ce schéma montre comment les pirates peuvent parvenir à rester anonymes en combinant plusieurs approches. L'utilisation de réseaux hertziens libres rend quasiment impossible l'identification des pirates. En utilisant des services de communication et des services de courriel anonymes, qui ne contrôlent pas les renseignements fournis à l'inscription, les pirates peuvent réduire les risques d'identification.

L'utilisation de fausses adresses de courriel est l'une des possibilités qui s'offrent aux cyberdélinquants pour cacher leur identité[664]. De nombreux prestataires proposent l'ouverture gratuite de comptes de courriel. Or les renseignements personnels – lorsqu'ils sont

---

657 Regarding the implication of the use of cell phones as storage media on 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.

658 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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

659 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: http://www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

660 Re 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. andbelow: Chapter 6.2.14

661 Regarding the difficulties that are caused if offenders use open wireless networks, see above: Chapter 3.2.3 .

662 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf;

663 See: *Claessens/Preneel/Vandewalle*, "Solutions for Anonymous Communication on the Internet», 1999.

664 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.

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[665].

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[666]. Plusieurs Etats 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[667]. 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[668]. Cela étant, certains Etats cherchent à résoudre les problèmes que posent les communications anonymes en mettant en place des limitations juridiques[669], notamment l'Italie, qui impose aux fournisseurs d'accès public à Internet d'identifier les utilisateurs dès le début d'une session[670].

Figure 35

Ce schéma montre comment des informations peuvent être cachées dans une image. Le logiciel de chiffrage intègre à l'image des données en modifiant l'information de couleur de certains pixels. Si l'image est suffisamment grande, il est quasiment impossible de déceler les changements, à moins de pouvoir comparer l'image originale et l'image modifiée. Grâce à cette technique, les pirates peuvent dissimuler le fait qu'ils échangent des informations en plus de l'image.

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[671].

---

665 *Donath*, "Sociable Media», 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

666 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.

667 (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).

668 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.

669 See below: Chapter 6.2.11.

670 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: http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

671 Regarding the technical discussion about traceability and anonymity, see: "CERT Research 2006 Annual Report», page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

3.2.13 Technologies de chiffrement

Autre facteur susceptible de compliquer les enquêtes sur les cyberdélits: les technologies de chiffrement[672]. 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[673]. De même que l'anonymat, le chiffrement est un domaine scientifique ancien[674], qui a évolué grâce à la technologie informatique. Le chiffrement des données informatiques, aujourd'hui réalisable en un simple clic, complique le travail des services de répression, qui, pour accéder aux données, doivent d'abord les décrypter[675]. On ne sait pas avec certitude dans quelle mesure les cyberdélinquants utilisent les technologies de chiffrement pour dissimuler leurs activités, mais il a été rapporté que les terroristes y ont recours[676]. 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[677]. Les experts craignent toutefois une augmentation de l'utilisation de ces technologies dans les cyberdélits[678].

Pour protéger leurs fichiers contre les accès non autorisés, les utilisateurs disposent de plusieurs logiciels[679]. Les enquêteurs, de leur côté, utilisent des outils spécialisés, qui les aident à briser les codes de chiffrement[680]. L'opération de décryptage, généralement difficile et lente, peut être facilitée si les enquêteurs ont accès au logiciel qui a servi à chiffrer les fichiers[681]. A défaut, ils peuvent tenter une attaque de type "force brute"[682].

---

672 Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future», No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf.

673 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: http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

674 *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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

675 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

676 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: http://www.terrorismcentral.com/Library/Teasers/Flamm.html.

677 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.

678 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: http://www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

679 Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see http://www.truecrypt.org).

680 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf ;

681 See "Data Encryption, Parliament Office for Science and Technology No. 270», UK, 2006, page 3, available at: http://www.parliament.uk/documents/upload/postpn270.pdf.

682 Brute force attack is one method of defeating a cryptographic scheme by trying a large number of possible codes.

Le temps nécessaire pour briser un code de chiffrement – il faudrait parfois des années – dépend de la technique de chiffrement utilisée et de la longueur de la clé[683]. 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[684]; pour 56 bits, 2 285 années; pour 128 bits, avec un milliard d'ordinateurs dédiés à cette opération, il faudrait des milliers de milliards d'années[685]. 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[686]. Par ailleurs, l'installation d'un logiciel de chiffrement est aisée. Si certains experts informatiques spécialisés en criminalistique ne s'en effraient pas[687], 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[688] sur IP[689]. Les cyberdélinquants y ont recours pour protéger leurs conversations des écoutes[690].

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

---

683 *Schneier*, "Applied Cryptography», Page 185; *Bellare/Rogaway*, "Introduction to Modern Cryptography», 2005, page 36, available at: http://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

684 1099512 seconds.

685 Equivalent to 10790283070806000000 years.

686 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.

687 See *Leyden*, "Vista encryption 'no threat' to computer forensics», The Register, 02.02.2007, available at: http://www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

688 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, "Skype Security Evaluation», 2005, available at: http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

689 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: http://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.

690 *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.

stéganographie[691]. Faire la distinction entre une photo de vacances et une photo dans laquelle des messages chiffrés ont été cachés n'est pas une opération facile[692].

Pour les services de répression, l'accès aux techniques de chiffrement et leur utilisation par des délinquants est problématique. Plusieurs approches juridiques sont actuellement examinées[693]: 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[694], etc. 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. Etant donné le nombre croissant d'attaques informatiques[695], l'autoprotection est un élément essentiel de la cybersécurité.

3.2.14 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 de former les membres des services de répression ainsi que les personnes chargées d'élaborer une législation suffisante et efficace en la matière. Cette partie 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[696]. De même, les premières infractions

---

691 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: http://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

692 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: https://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.

693 See below: Chapter 6.2.9.

694 See below: Chapter 6.2.9.

695 See above: Chapter 3.2.8.

696 See BBC News, "Hacking: A history», 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

(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[697]. 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[698]. Le processus d'ajustement législatif s'effectue en général en trois étapes:

Premièrement, la reconnaissance d'une nouvelle utilisation abusive des technologies de l'information et de la communication. 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)[699], 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

Deuxième étape, 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.

Troisième étape, l'élaboration de nouvelles dispositions législatives. 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[700]. 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

---

697 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.»

698 Within this process the case law based Anglo-American Law System shows advantage with regard to the reaction time.

699 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 percent of internet systems to a halt in November 1988. For more information on the history of the CERT CC see: http://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.

700 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and the UN Resolution 55/63.

conséquent plus essentielles que jamais[701]. 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[702]. 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[703]. 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.)[704]. Or de nouvelles infractions sont découvertes tous les jours, tels le "vol" de monnaies virtuelles dans des jeux en ligne et leur revente sur des plates-formes d'enchères[705]. 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"[706]. 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[707]. Les services de répression doivent donc disposer d'outils appropriés pour enquêter sur les délits en préparation. Or certains mécanismes (conservation des données[708] par exemple) peuvent porter atteinte aux

---

701 See below: Chapter 5.

702 See above: Chapter 2.7.1.

703 Regarding the offences recognised in relation to online games see above: Chapter 2.5.5.

704 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/.

705 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 et seqq;

706 *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/.

707 Re 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.

708 Data retention describes the collection of certain data (such as traffic data) through obliged institutions e.g., Access Providers. For more details, see below: Chapter 6.2.5.

droits des internautes innocents[709]. 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. A 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

Le nombre de documents numériques croît constamment[710], du fait notamment de leur faible coût[711] de stockage en comparaison des documents sur papier. 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[712]. En réponse aux évolutions techniques, les contenus numériques ont été acceptés comme nouvelles sources de preuve[713]. 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[714]. La prise en compte des données numériques en tant qu'éléments de preuve s'accompagne de difficultés bien spécifiques et requiert des procédures spéciales[715]. Très fragiles, elles peuvent être facilement effacées[716] ou modifiées; l'un des problèmes les plus délicats est donc de maintenir leur intégrité[717]. Cela vaut tout particulièrement pour les données stockées en mémoire RAM, automatiquement effacées à l'arrêt des systèmes[718], qui, pour être conservées, nécessitent des techniques spéciales[719]. 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 dans les nuages". Les enquêteurs pouvaient autrefois concentrer leurs recherches sur les données informatiques trouvées sur les lieux. Ils doivent

---

709 Related 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.

710 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

711 *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.

712 *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.

713 *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.

714 *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: http://www.cybex.es/agis2005/elegir_idioma_pdf.htm.

715 Regarding the difficulties of dealing with digital evidence on the basis of the 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.

716 *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.

717 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

718 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

719 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

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[720].

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[721]:

- identification des éléments de preuve pertinents[722];
- collecte et archivage des éléments de preuve[723];
- analyse de la technologie informatique et des éléments de preuve numériques;
- 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[724]. Etant donné que la quantité d'information stockée au format numérique augmente constamment, les enquêteurs sont confrontés à des problèmes de logistique[725]. Outre les recherches manuelles, il est donc important qu'ils appliquent des procédures automatisées[726], notamment des recherches fondées sur les valeurs de hachage pour trouver des images pornographiques connues mettant en scène des enfants[727] ou des recherches par mots-clés[728].

Selon les besoins de chaque enquête, les experts en criminalistique informatique peuvent par exemple:

- analyser les matériels et les logiciels utilisés par le suspect[729];
- aider les enquêteurs à identifier les éléments de preuve pertinents[730];
- récupérer des fichiers effacés[731];

---

720 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

721 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 as well *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 are differentiating between six different phases.

722 This includes the development of investigation strategies

723 The second phase does especially cover 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.

724 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.

725 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol 119, page 532.

726 *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.

727 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

728 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.

729 This does for example include the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

730 tThis does for example include the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

731 *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.

- décrypter des fichiers[732];
- identifier des internautes en analysant des données relatives au trafic[733].

4 Stratégies de lutte contre la cybercriminalité

Du fait du nombre croissant des cyberdélits reconnus et des outils techniques destinés à automatiser les infractions en ligne (systèmes anonymes de partage de fichiers[734], logiciels de création de virus informatiques[735], etc.), la lutte contre la cybercriminalité est devenue une activité essentielle des services de répression dans le monde entier. Dans les pays développés comme dans les pays en développement, cette lutte est un véritable défi à relever. 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, dans le cadre des programmes de cybersécurité nationaux, une stratégie anticybercriminalité efficace.

4.1 Législation relative à la lutte contre la cybercriminalité en tant que partie intégrante d'une stratégie de la cybersécurité

Comme cela a été mentionné précédemment, la cybersécurité[736] joue un rôle essentiel dans le développement des technologies de l'information et des services Internet[737]. Le renforcement de la sécurité d'Internet (et de la protection des internautes) fait aujourd'hui partie intégrante du développement des nouveaux services, mais

---

732 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion 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.

733 Regarding the differnet 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.

734 *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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Design», 2005. See also above: Chapter 3.2.l.

735 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: http://www.212cafe.com/download/e-book/A.pdf. For more information, see above: Chapter 3.2.h.

736 The term "Cybersecurity» is used to summarise various activities such as 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 cyber environment 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 cyber environment. 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. Regarding the definition of cybersecurity, 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 cyber environment 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 cyber environment. 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: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

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

aussi des politiques gouvernementales[738]. 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[739].

Toute stratégie anticybercriminalité doit être intégrée à une stratégie de cybersécurité. Le Programme mondial cybersécurité de l'UIT[740], 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. Inversement, lutter efficacement contre la cybercriminalité suppose de mettre en œuvre des mesures dans chacun des domaines représentés par les cinq grands axes[741].

4.2 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 des problématiques analogues reposent sur la seule différenciation entre pays développés et pays en développement, 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 promouvoir la cybersécurité de multiples façons et avec plus de souplesse, par exemple en concentrant leur action sur des mesures de protection technique 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;

le degré de soutien du secteur privé (via des partenariats public-privé).

4.3 Différences régionales

Etant 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

---

738 See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://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: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

739 For more information see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

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

741 See below: Chapter 4.4.

n'intègrent pas nécessairement diverses caractéristiques importantes des pays en développement[742]. Il faut donc réussir à intégrer les facteurs régionaux et les différentes régionales d'une autre façon.

4.4 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.

4.4.1 Cadre juridique

Des cinq grands axes, le cadre juridique est probablement le plus pertinent en matière de stratégie de lutte contre la cybercriminalité. Il concerne, en premier lieu, la mise en place des dispositions de fond en droit pénal nécessaires à la pénalisation des actes de fraude informatique, d'accès illicite, de brouillage de données, d'atteinte à la propriété intellectuelle, de pornographie mettant en scène des enfants, etc.[743] Il convient de noter que l'existence, dans le code pénal, de dispositions visant des actes analogues commis en dehors d'Internet n'implique pas nécessairement que lesdites dispositions sont applicables à des actes perpétrés sur le réseau[744]. Il est donc essentiel d'analyser en détail les lois nationales en vigueur afin d'identifier les lacunes éventuelles[745]. Outre des dispositions de fond en droit pénal[746], les instances de répression doivent disposer des mécanismes et instruments nécessaires pour instruire les affaires de cybercriminalité[747]. Ce type d'instruction présente plusieurs difficultés[748]. D'une part, les auteurs de ces infractions peuvent agir à partir de n'importe quel endroit sur la planète (ou presque) tout en masquant leur identité[749]. Les mécanismes et les instruments nécessaires pour instruire ce type d'affaire peuvent donc être assez différents de ceux utilisés pour enquêter sur les infractions

---

742 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States of America, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arabic regions.

743 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

744 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 et. Seqq.

745 For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at: http://www.coe.int/cybercrime/. [745] See for example the following surveys on national cybercrime legislation: 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 ;*Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*. , available at: https://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: http://www.mosstingrett.no/info/legal.html.

746 See below: Chapter 6.1.

747 See below: Chapter 6.1.

748 For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.1.

749 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 seqq., available at: http://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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing», 2005.

classiques[750]. D'autre part, du fait de la dimension internationale[751] de la cybercriminalité, le cadre juridique national doit permettre la coopération avec les agences de répression étrangères[752].

4.4.2 Mesures techniques et de procédures

Les enquêtes sur les cyberdélits ont très souvent une forte composante technique[753]. 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[754] à l'iTAN[755] par exemple) 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[756]. 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);
- 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 (services bancaires en ligne par exemple). Cette approche indirecte permet de réduire le nombre de personnes et d'organisations nécessaires à la promotion des mesures de protection technique.

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

---

750 Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.10 and Chapter 6.2.11.

751 See above: Chapter: 3.2.6.

752 See in this context below: Chapter 6.3.

753 *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: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://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;

754 Transaction Authentication Number – for more information, see: "Authentication in an Internet Banking Environment», United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

755 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 relavant 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.

756 Re the various approaches of authentication in Internet banking, see: "Authentication in an Internet Banking Environment», United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

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 un garant des activités de sécurité (diffusion d'outils de protection et d'information concernant les escroqueries les plus récentes, etc.)[757].

4.4.3 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.

4.4.4 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[758].

Il importe également de former les utilisateurs[759]. En effet, certains cyberdélits – notamment ceux qui s'apparentent à la fraude, tels que le 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[760]. On trouve certes sur le marché divers produits logiciels capables d'identifier automatiquement certains sites Internet malveillants[761], mais aucun ne peut les identifier tous. Une stratégie de protection des utilisateurs exclusivement fondée sur les logiciels n'est donc pas totalement fiable[762]. 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.

---

757 Regarding the 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: http://www.coe.int/cybercrime/.

758 Capcity Buidling 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, adding that, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations and water user groups, professional associations, academics and others.

759 At the G8 Conference in Paris in 2000, *Jean-Pieree 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: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks», available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf. Re sceptical views regarding user education, see: *Görling*, "The Myth Of User Education», 2006, available at: http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

760 "Anti-Phishing Best Practices for ISPs and Mailbox Providers», 2006, page 6, available at: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks», available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf.

761 *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: http://www.microsoft.com/presspass/ press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

762 For a different opinion, see: *Görling*, "The Myth Of User Education», 2006, at:http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

Parmi elles, la formation des utilisateurs, qui est l'une des composantes les plus importantes de la prévention de la cybercriminalité[763]. 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:

- campagnes d'information publique;
- cours dans les écoles, les bibliothèques, les centres de formation informatique et les universités;
- partenariats public-privé.

Pour qu'une stratégie de formation et d'information soit efficace, il importe de faire connaître ouvertement les dernières cybermenaces en date. Or certains Etats 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 Etats-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[764]. 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[765].

4.4.5 Coopération internationale

Les processus de transfert de données sur Internet font très souvent intervenir plusieurs pays[766]. 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[767]. De plus, un grand nombre de services Internet (services d'hébergement par exemple) sont proposés par des sociétés situées à l'étranger[768].

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[769]. Or, en vertu du principe de souveraineté

---

763 At the G8 Conference in Paris in 2000, *Jean-Pieree 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.»

764 "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: http://www.heise-security.co.uk/news/80152.

765 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: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

766 Regarding the extend of transnational attacks in the the most damaging cyber attacks 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.

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

768 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: http://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.

769 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 seqq. , 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 seqq. , available at: http://media.hoover.org/documents/0817999825_1.pdf

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[770]. Les enquêteurs doivent donc obtenir le soutien des autorités de tous les pays concernés. Etant 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.

5 Présentation générale des approches législatives internationales

Le présent chapitre se propose de fournir une vue d'ensemble des approches législatives internationales[771] 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 G8[772]

En 1997, le Groupe des huit (G8) a créé un "sous-groupe[773] sur la criminalité liée à la haute technologie" (*Subcommittee on High-tech Crimes*), chargé des questions de lutte contre la cybercriminalité[774]. A leur réunion de Washington D.C., Etats-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[775]. 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 Etats concernés, indépendamment du lieu du préjudice.

---

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

771 This includes regional approaches.

772 The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, Great Britain, United States and the Russian Federation. The Presidency of the group that represents more than 60% of the world economy (Source: http://undp.org) rotates every year.

773 The idea of the creation of five Subgroups – among them, one on High-Tech Crimes – was to improve the implementation of the Forty Recommendations adopted by G8 Heads of State in 1996.

774 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 organised crime, that started with the launch of the Senior Experts Group on Organised Crimes (the "Lyon Group») in 1995. At the Halifax summit in 199, 5 the G8 expressed: "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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

775 Regarding the G8 activities in the fight against Cybercrime see as well: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

- 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[776]. 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[777].

---

776 "Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime», Moscow, 19-20 October, 1999.

777 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.

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[778].

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. A l'époque déjà, dans sa recherche de solutions internationales, le G8 évoquait la Convention du Conseil de l'Europe sur la cybercriminalité[779]. En 2001, lors d'un atelier organisé à Tokyo[780], 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[781].

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[782]. Le G8 prenait encore note de la Convention du Conseil de l'Europe sur la cybercriminalité[783].

A 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[784]. La question du cyberterrorisme[785] a également été abordée au sommet du G8 de Moscou, qui a suivi cette réunion[786].

---

778 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. […]

779 *Jean-Pierre Chevenement*, the French Minister of 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.»

780 G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

781 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.

782 G8 Justice and Home Affairs Communiqué, Washington DC, May 11, 2004.

783 G8 Justice and Home Affairs Communiqué Washington DC, May 11, 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.

784 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

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[787]. Cet accord ne contient pas d'actes précis devant être pénalement sanctionnés.

5.1.2 Nations Unies[788]

Lors du huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants (tenu à La Havane, Cuba, du 27 août au 7 septembre 1990), l'Assemblée générale des Nations Unies a adopté une résolution portant sur la législation en matière de cybercriminalité[789]. En 1994, sur la base de la résolution 45/121 (1990), les Nations Unies ont publié un manuel sur la prévention et le contrôle de la cybercriminalité[790].

En 2000, l'Assemblée générale a adopté une résolution sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles, qui présente certaines similarités avec le plan d'action en dix points adopté par le G8 en 1997[791]. Dans cette résolution, l'Assemblée générale recense plusieurs mesures visant à prévenir l'exploitation 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;*

terrorists and the recruitment of other illegal actors». See: http://www.g7.utoronto.ca/justice/justice2006.htm.

785 Regarding the topic Cyberterrorism see above: Chapter 2.8.1; In addition see See: *Lewis*, "The Internet and Terrorism», available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; Lewis, "Cyber-terrorism and Cybersecurity»; http://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 seqq., available at: http://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 seqq; United States Department of State, "Pattern of Global Terrorism, 2000», in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism», available at: http://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 seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror» in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

786 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.

787 For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

788 The United Nations (UN) is an international organisation founded in 1945 that had 191 Member States in 2007.

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

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

791 A/RES/55/63. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

En 2002, l'Assemblée générale a adopté une autre résolution sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles[792]. Cette résolution rappelle les différentes approches existantes au niveau international pour lutter contre la cybercriminalité et met en avant plusieurs 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.*

En 2004, les Nations Unies ont créé un groupe de travail sur le pollupostage, la cybercriminalité et d'autres questions relatives à Internet, soulignant de ce fait leur volonté de prendre part aux discussions internationales en cours sur les cybermenaces[793].

Lors du 11e Congrès des Nations Unies sur la prévention du crime et la justice pénale, tenue à Bangkok, Thaïlande, en 2005, une déclaration a été adoptée, qui souligne la nécessité d'harmonisation en matière de lutte contre la cybercriminalité[794]. Entre autres éléments de cette déclaration:

> *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*

---

792 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.

793 Regarding the Creation of the Working Group, see the UN press release, 21st of September 2004, available at: http://www.un.org/apps/news/story.asp?NewsID=11991&Cr=internet&Cr1=.

794 "Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice», available at: http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

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.

De plus, plusieurs décisions, résolutions et recommandations du système des Nations Unies traitent de questions se rapportant à la cybercriminalité. Ci-dessous figurent les plus importantes.

- La Commission pour la prévention du crime et la justice pénale de l'Office des Nations Unies contre la drogue et le crime (UNODC)[795] a adopté une résolution sur les mesures efficaces de lutte contre l'exploitation sexuelle des enfants[796].
- En 2004, le Conseil économique et social des Nations Unies[797] a adopté une résolution sur la coopération internationale en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la fraude, l'abus et la falsification d'identité à des fins criminelles et les infractions connexes[798]. En 2007, le Conseil a adopté une résolution sur la coopération internationale en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la fraude économique et la criminalité liée à l'identité[799]. Ces deux résolutions ne traitent pas explicitement des infractions liées à Internet[800], mais elles s'appliquent aussi à ce type d'infraction.

En 2004, le Conseil a adopté une résolution sur la vente via Internet de drogues licites, qui traitait explicitement d'un phénomène lié à la cybercriminalité[801].

5.1.3 Union internationale des télécommunications[802]

L'Union internationale des télécommunications (UIT), en tant d'institution spécialisée des Nations Unies, joue un rôle essentiel dans la normalisation et le développement des télécommunications et dans les questions de cybersécurité. 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*.

---

795 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

796 CCPCJ Resolution 16/2 on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process within the development of the resolution and for an overview about 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:
http://www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative to the resolution see: http://www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

797 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: http://www.un.org/ecosoc/.

798 ECOSOC Resolution 2004/26 International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf

799 ECOSOC Resolution 2007/20 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: http://www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

800 Regarding Internet-related ID-Theft, see above: Chapter 2.7.3 and below: Chapter 6.1.15.

801 ECOSOC Resolution 2004/42 on sale of internationally controlled licit drugs to individuals via the Internet, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

802 The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates. For more information see http://www.itu.int.

Le Plan d'action de Genève souligne l'importance des mesures de lutte contre la cybercriminalité[803]:

> ***C5. Etablir 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, organisée 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[804] 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, aux niveaux 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 Etats 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.*

A l'issue du SMSI, l'UIT a été désignée seul coordonnateur de la grande orientation C5 intitulée "Etablir la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication"[805]. A 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*[806]. Le Programme mondial cybersécurité (GCA) comporte sept buts stratégiques[807] et repose sur cinq grands axes stratégiques[808], portant notamment sur le développement de stratégies pour l'élaboration d'une législation type en matière de cybercriminalité. Les sept buts sont les suivants:

---

803 WSIS Geneva Plan of Action, 2003, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

804 WSIS Tunis Agenda for the Information Society, 2005, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

805 For more information on C5 Action Line 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: http://www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the Meetign Report of the Third Facilitation Meeting for WSIS Action Line C5, 2008, available at: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

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

807 http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

808 The five pillars are: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, International Cooperation. For more information, see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

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.

Un groupe d'experts a été constitué pour définir les stratégies relevant du GCA[809].

5.1.4 Conseil de l'Europe[810]

En 1976, le Conseil de l'Europe soulignait le caractère international des cyberdélits et examinait ce sujet à une conférence portant sur les divers aspects de la criminalité économique. Cette question est depuis une préoccupation majeure de l'organisation[811]. En 1985, le Conseil de l'Europe a désigné un comité d'experts[812] chargé d'examiner les aspects juridiques de la cybercriminalité[813]. En 1989, le Comité européen pour les problèmes criminels a adopté le "rapport sur la criminalité en relation avec l'ordinateur"[814], 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,

809 See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

810 Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

811 Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

812 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.

813 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

814 *Nilsson* in Sieber, "Information Technology Crime», Page 576.

le Comité des Ministres a adopté une recommandation[815], 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 en relation avec l'ordinateur, 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[816]. En annexe à cette recommandation figure un résumé des principes directeurs relatifs à l'élaboration de dispositions législatives adaptées[817].

En 1996, le Comité européen pour les problèmes criminels (CDPC) a décidé de créer un Comité d'experts chargés de la cybercriminalité[818]. A 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[819]. 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[820]. 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. 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 Etats non membres du Conseil de l'Europe, qui prenaient part aux négociations: Canada, Etats-Unis, Japon et Afrique du Sud). En avril 2009, quarante-six Etats[821]

---

815 Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

816 Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

817 The Guidelines deal with investigative instruments (e.g. Search and Seizure) as well as electronic evidence and international cooperation.

818 Decision CDPC/103/211196. The CDPC explained their 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.»

819 Explanatory Report of the Convention on Cybercrime (185), No. 10.

820 The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: http://www.coe.int.

821 Albania, 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, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

avaient signé la convention sur la cybercriminalité et vingt-cinq[822] l'avaient ratifié[823]. Certains pays, notamment l'Argentine[824], le Pakistan[825], les Philippines[826], l'Egypte[827], le Botswana[828] et le Nigéria[829], ont déjà élaboré certaines parties de leur législation en conformité avec la convention. Ainsi, bien que ces pays n'aient pas encore signé la convention, ils soutiennent le processus d'harmonisation et de normalisation voulu par ses rédacteurs. Cette convention est aujourd'hui reconnue comme un instrument international important de la lutte contre la cybercriminalité. Plusieurs organisations internationales la soutiennent[830].

La Convention sur la cybercriminalité a été suivie d'un premier protocole additionnel[831]. Au cours des négociations sur le texte de la convention, il est apparu que la pénalisation du racisme et la diffusion de contenus xénophobes étaient des sujets particulièrement polémiques[832]. Certains Etats, dotés d'une législation

---

822 Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

823 The need for a ratification is laid down in Article 36 of the Convention:
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.

824 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).

825 Draft Electronic Crime Act 2006.

826 Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

827 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

828 Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

829 Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

830 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 Cyber Crime 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: http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda points out: "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: http://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:
http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

831 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

832 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.»

forte en faveur de la protection de la liberté d'expression[833], 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[834]. Ces questions ont donc fait l'objet d'un protocole distinct. En octobre 2008, vingt Etats[835] avaient signé le protocole additionnel et treize[836] l'avaient ratifié.

En 2007, dans le cadre de sa démarche visant à améliorer la protection des mineurs contre l'exploitation sexuelle, le Conseil de l'Europe a introduit une nouvelle convention[837]. Au premier jour de l'ouverture à la signature, vingt-trois Etats ont signé la Convention pour la protection des enfants[838]. L'un des objectifs clés de cette convention est l'harmonisation des dispositions pénales visant à protéger les enfants de l'exploitation sexuelle[839]. A cette fin, la convention intègre un ensemble de dispositions pénales. Outre la pénalisation des abus sexuels sur les enfants (article 18), elle contient une disposition relative à l'échange de contenu pornographique mettant en scène des enfants (article 20) ainsi qu'une disposition relative à la sollicitation d'enfants à des fins sexuelles (article 23).

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 Union européenne[840]

En matière de législation pénale, les compétences de l'Union européenne sont limitées[841]. Elle peut harmoniser les législations nationales en matière pénale seulement dans certains cas précis, notamment la protection des intérêts financiers de l'Union et la cybercriminalité[842].

---

833 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

834 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

835 Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine.

836 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine

837 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

838 Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Irland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Turkey. Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).

839 For more details see *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

840 The European Union is a supranational and intergovernmental union of today 27 member states from the European continent.

841 *Satzger*, International and European Criminal Law, Page 84; *Kapteyn/VerLooren van Themaat*, Introduction to the Law of the European Communities, Page 1395.

842 Regarding the Cybercrime legislation in respect of Computer and Network Misuse in EU Countries see: *Baleri/Somers/Robinson/Graux/Dumontier*, Handbook of Legal Procedures of Computer Network Misuse in EU Countries, 2006.

En 1999, en adoptant la communication de la Commission européenne intitulée "eEurope 2005 – Une société de l'information pour tous", l'Union européenne a lancé l'initiative "eEurope"[843]. En 2000, le Conseil européen a adopté un "plan d'action eEurope" global et s'est exprimé en faveur de sa mise en œuvre avant la fin 2002.

En 2001, la Commission européenne 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 cybercriminalité"[844]. Dans cette communication, la Commission analyse et s'emploie à résoudre le problème de la cybercriminalité, en soulignant notamment la nécessité d'une action efficace pour combattre les menaces qui pèsent sur l'intégrité, la disponibilité et la sécurité de fonctionnement des systèmes d'information et des réseaux.

> *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[845].*
>
> *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[846].*
>
> *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[847];*

---

843 Communication of 8 December 1999 on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000 – *e*Europe – An information society for all – COM 1999, 687.

844 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 Crime26.1.2001, COM(2000) 890.

845 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.

846 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.

847 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.

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[848].

En outre, la Commission a publié en 2001 une communication sur la "Sécurité des réseaux et de l'information"[849], 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[850]. Dans la droite ligne de cette stratégie, la Commission a présenté en 2002[851] une proposition pour une "Décision-cadre relative aux attaques visant les systèmes d'information". La proposition de la Commission a été partiellement modifiée puis adoptée par le Conseil[852].

La décision-cadre, prenant note de la Convention du Conseil de l'Europe sur la cybercriminalité[853], se concentre sur l'harmonisation des dispositions de fond en droit pénal visant à protéger les éléments d'infrastructure.

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.

---

848 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.

849 "Network and Information Security» A European Policy approach – adopted 6 June 2001.

850 For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

851 Proposal of the Commission for a Council Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. 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.

852 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

853 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:

"Legislative action at the level of the European Union also needs to take into account developments in other international fora. In the context of approximation of substantive criminal law on attacks against information systems, the Council of Europe (C.o.E.) is currently the most far-advanced. The Council of Europe started preparing an international Convention on cyber-crime in February 1997, and is expected to complete this task by the end of 2001. The draft Convention seeks to approximate a range of criminal offences including offences against the confidentiality, integrity and availability of computer systems and data. This Framework Decision is intended to be consistent with the approach adopted in the draft Council of Europe Convention for these offences.»

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.

En 2005, la Cour de justice des communautés européennes a déclaré illégale[854] une décision-cadre du Conseil relative à la protection de l'environnement par le droit pénal[855]. Par cet arrêt, la Cour a clarifié la répartition des compétences entre le premier et le troisième pilier pour ce qui concerne les dispositions de droit pénal. Elle a jugé que la décision-cadre sur la protection de l'environnement par le droit pénal, en empiétant sur les compétences que l'article 175 CE attribue à la Communauté, méconnaît dans son ensemble, en raison de son indivisibilité, l'article 47 UE[856]. Dans une communication sur l'arrêt prononcé par la Cour[857], la Commission a déclaré:

"D'un point de vue matériel, au-delà de la matière de la protection de l'environnement, le raisonnement de la Cour s'applique donc à toutes les politiques communautaires et libertés dans lesquelles existent des normes contraignantes auxquelles des sanctions pénales devraient être associées pour garantir leur effectivité."

La Commission a déclaré qu'en vertu de l'arrêt prononcé par la Cour, plusieurs décisions-cadres se rapportant au droit pénal étaient entièrement ou en partie incorrectes, tout ou partie de leurs dispositions ayant été adoptées sur une base juridique erronée. La décision-cadre relative aux attaques visant les systèmes d'information est explicitement mentionnée dans l'annexe de la communication.

Les éléments relatifs au droit de procédure pénale – notamment l'harmonisation des instruments nécessaires pour enquêter sur les cyberdélits et poursuivre en justice leurs auteurs – n'ont pas été intégrés dans la décision-cadre. Cela étant, la Commission a élaboré en 2005 une proposition de directive de l'Union européenne relative à la conservation des données. Trois mois seulement après la présentation de cette directive au Parlement européen, le Conseil a adopté la proposition[858]. 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:

Article 3 – Obligation de conservation de données

1. 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

---

854 Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03.

855 Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

856 "It follows from the foregoing that, on account of both their aim and their content, Articles 1 to 7 of the framework decision have as their main purpose the protection of the environment and they could have been properly adopted on the basis of Article 175 EC. That finding is not called into question by the fact that Articles 135 EC and 280(4) EC reserve to the Member States, in the spheres of customs cooperation and the protection of the Community's financial interests respectively, the application of national criminal law and the administration of justice. It is not possible to infer from those provisions that, for the purposes of the implementation of environmental policy, any harmonisation of criminal law, even as limited as that resulting from the framework decision, must be ruled out even where it is necessary in order to ensure the effectiveness of Community law. In those circumstances, the entire framework decision, being indivisible, infringes Article 47 EU as it encroaches on the powers which Article 175 EC confers on the Community.»

857 Communication From The Commission To The European Parliament And The Council on the implications of the Court's judgment of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

858 2005/0182/COD

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'organisation 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[859].

En 2007, la Commission a publié une communication intitulée "Vers une politique générale en matière de lutte contre la cybercriminalité"[860]. Cette communication fait le point sur la situation et souligne l'importance de la Convention du Conseil de l'Europe sur la cybercriminalité en tant que principal instrument international de la lutte contre la cybercriminalité. En outre, la communication mentionne les questions qui occuperont une place centrale dans les activités futures de la Commission, notamment:

- renforcer la coopération internationale pour lutter contre la cybercriminalité;
- mieux coordonner le soutien financier des activités de formation;
- organiser une réunion d'experts en matière de répression;
- renforcer le dialogue avec l'industrie;
- surveiller l'évolution des cybermenaces afin d'évaluer les besoins en législation complémentaire.

En 2008, l'Union européenne a entamé des discussions sur un projet de modification de la décision-cadre sur la lutte contre le terrorisme[861]. 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[862]. 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.

---

859 *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, 286.

860 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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

861 Draft Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism, COM(2007) 650.

862 "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.»

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 (c)[863] de la décision-cadre, les Etats membres sont tenus 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 (utilisation double), 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).

5.2.2 Organisation de coopération et de développement économiques[864]

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

863 "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.

864 The Organisation for Economic Co-operation and Development was founded 1961. It has 30 member states and is based in Paris. For more information see: http://www.oecd.org.

cybercriminalité[865]. 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[866]. Elle recommandait aux Etats 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[867]. 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[868]. 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.*

---

865 *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.

866 OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

867 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.

868 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: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

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 pollupostage sur les pays en développement[869]. Ce rapport montre que le pollupostage 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[870].

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 Etats[871].

5.2.3 Coopération économique pour l'Asie-Pacifique[872]

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[873]. Ils se sont engagés à:

- faire tout leur possible pour adopter un ensemble complet de lois en matière de cybersécurité et de cybercriminalité, qui soit conforme avec les 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;
- identifier des unités nationales de lutte contre la cybercriminalité et des points de contact internationaux pouvant offrir une assistance dans le domaine la de haute technologie, et mettre en place ces moyens dans la mesure où ils n'existent pas déjà, et ce, d'ici octobre 2003;
- 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.

---

869 Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

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

871 The report is available at: http://www.legislationline.org/upload/ lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

872 The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties that has 21 members.

873 "*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.

Les dirigeants de l'APEC se sont exprimés en faveur d'une coopération plus étroite des agents impliqués dans la lutte contre la cybercriminalité[874]. En 2005, l'APEC a organisé une conférence sur la législation en matière de cybercriminalité[875], dont les objectifs principaux étaient de:

- promouvoir l'élaboration de cadres juridiques complets pour lutter contre la cybercriminalité et promouvoir la cybersécurité;
- aider les services de répression à faire face aux problèmes posés par les technologies de pointe et les progrès technologiques;
- promouvoir la coopération entre les services d'enquête sur les cyberdélits dans l'ensemble de la région.

Le groupe de travail APEC-TEL (APEC Telecommunications and Information Working Group[876]) a pris une part active aux travaux de l'APEC visant à accroître la cybersécurité[877]. Il a adopté en 2002 la stratégie cybersécurité de l'APEC[878] (*APEC Cybersecurity Strategy*). Le groupe de travail a exprimé sa position au regard de la législation en matière de cybercriminalité en se référant aux approches internationales des Nations Unies et du Conseil de l'Europe[879]. La déclaration publiée par les ministres de l'APEC-TEL à la réunion tenue en 2008 à Bangkok, Thaïlande, souligne qu'il est important de poursuivre la collaboration contre la cybercriminalité[880].

5.2.4 Commonwealth

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[881]. Cette volonté d'harmonisation des législations au sein du Commonwealth et de coopération internationale s'explique entre autres par le fait que, sans une telle approche, il aurait fallu pas moins de 1 272 traités bilatéraux pour régir la coopération internationale en la matière[882]. Le groupe d'experts a présenté son rapport et ses recommandations en mars 2002[883]. Le projet de loi type sur la criminalité informatique et en relation avec l'ordinateur (*Draft Model Law on Computer and*

---

874 "*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.

875 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.

876 "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.»

877 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: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

878 For more information see: http://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

879 See: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

880 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: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

881 See "Model Law on Computer and Computer Related Crime», LMM(02)17, Background information.

882 *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.

883 See: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

Computer Related Crime) a été présenté la même année[884]. 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.

5.2.5 Ligue des Etats arabes et Conseil de coopération du Golfe[885]

Plusieurs Etats 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[886]. C'est notamment le cas du Pakistan[887], de l'Egypte[888] et des Emirats Arabes Unis[889]. Lors d'une conférence en 2007, le Conseil de coopération du Golfe[890] a recommandé à ses Etats membres d'adopter une démarche conjointe qui prenne en considération les normes internationales[891].

5.2.6 Organisation des Etats américains[892]

Depuis 1999, l'Organisation des Etats 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)[893].

---

884 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

885 The League of Arab States is a regional organisation with currently 22 members.

886 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

887 Draft Electronic Crime Act 2006

888 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

889 Law No.2 of 2006, enacted in February 2006.

890 Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE

891 Non official transation of the Recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18th of 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.

4) Providing trainings to inspection and law enforcement officials on dealing with such crimes.

5) Providing sufficient number of experts highly qualified in new technologies and Cybercrime particularly in regard to proofs and collecting evidence.

6) 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.

7) 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.

8) Increasing cooperation between Public and Private sectors in the intent of raising awareness and exchange of information in the Cybercrime combating field.

892 The Organisation of American States is an international organisation with 34 active Member States. For more information see: http://www.oas.org/documents/eng/memberstates.asp.

893 For more information see http://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: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

En 1999, le REMJA a recommandé la création d'un groupe d'experts intergouvernemental sur la cybercriminalité. Le groupe d'experts était chargé de:

- faire un état des lieux des activités criminelles qui visent les ordinateurs et les données informatiques ou qui consiste à utiliser des ordinateurs pour commettre une infraction;
- faire un état des lieux des législations, politiques et pratiques nationales concernant ces activités;
- recenser les entités nationales et internationales spécialisées en la matière;
- recenser les mécanismes de coopération du système interaméricain dans la lutte contre la cybercriminalité.

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[894]. Ces recommandations, réitérées à la réunion de 2003[895], recommandent notamment aux Etats membres:

- 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 à soutenir la préparation de cette stratégie;
- dans le cadre du groupe d'experts, 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;
- d'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;
- d'examiner et, le cas échéant, de 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 traditionnelles.

A leur quatrième réunion, les ministres de la Justice ou ministres ou procureurs généraux des Amériques ont recommandé aux Etats, 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[896] 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.

---

894 The full list of recommendations from the 2000 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber; The full list of recommendations from the 2003 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

895 The full list of recommendations is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm

896 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: http://www.oas.org/dil/department_office_legal_cooperation.htm.

A ce jour, les ministres de la Justice ou ministres ou procureurs généraux des Amériques (REMJA) ont tenu sept réunions[897]. Les plus récentes ont eu lieu à Washington D.C., Etats-Unis, en avril 2006 et avril 2008. A noter entre autres recommandations émanant de la réunion de 2006[898]:

- continuer de renforcer la coopération avec le Conseil de l'Europe de sorte que les Etats membres de l'OEA puissent envisager d'appliquer les principes de la Convention du Conseil de l'Europe sur la cybercriminalité[899], d'accéder à cette convention 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 Etats membres de l'OEA puissent bénéficier des avancées accomplies dans ces enceintes;
- 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, au cours de laquelle il a de plus été noté[900]:

- que, compte tenu des recommandations adoptées par le groupe d'experts gouvernementaux et par le REMJA à ses précédentes réunions, les Etats envisagent d'appliquer les principes de la Convention du Conseil de l'Europe sur la cybercriminalité, d'accéder 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.
- 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).

5.3 Démarches scientifiques

Le projet de convention internationale de Stanford (CISAC) est un exemple bien connu de démarche scientifique visant à élaborer un cadre juridique pour lutter contre la cybercriminalité au niveau mondial[901].

---

897 The Conclusions and Recommendation of the Meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas and Cyber Crime are available at: http://www.oas.org/juridico/english/cyber_meet.htm.

898 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 program be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G-8 to help conduct cyber-crime investigations. Pursuant to such recommendation, three OAS Regional Technical Workshops were held during 2006 and 2007, with the first being offered by Brazil and the United States, and the second and third offered by the United States. The List of Technical Workshops is available at: http://www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

899 In the meantime the 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: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp

900 Conclusions and Recommendations of REMJA-VII, 2008, available at: http://www.oas.org/juridico/english/cybVII_CR.pdf

901 *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.

Cette convention a été élaborée pour donner suite à une conférence organisée par l'Université de Stanford, Etats-Unis, en 1999[902]. Elle présente quelques similitudes avec la Convention du Conseil de l'Europe sur la cybercriminalité[903], qui a été rédigée à peu près à la même époque. Les deux conventions couvrent des éléments relatifs au droit pénal matériel, au droit procédural et à la coopération internationale. La différence la plus importante concerne le fait que les infractions et les instruments de procédure mentionnés dans le projet de Convention de Stanford s'appliquent exclusivement aux attaques visant des infrastructures de l'information et aux attaques terroristes, alors que les instruments relatifs au droit procédural et à la coopération internationale mentionnés dans la Convention sur la cybercriminalité s'appliquent également aux infractions traditionnelles[904].

5.4 Relations entre différentes approches législatives internationales

Etant donné la reconnaissance dont jouissent certaines normes concernant des protocoles techniques, la question se pose de savoir comment éviter les incompatibilités entre différentes approches internationales[905]. Si la Convention sur la cybercriminalité est aujourd'hui le principal cadre international en place qui couvre tous les aspects pertinents de la cybercriminalité, d'autres initiatives sont à l'étude. Ainsi une deuxième approche internationale actuellement adoptée par l'Union internationale des télécommunications[906]. A l'issue du Sommet mondial sur la société de l'information, l'UIT a été désignée coordonnateur de ladite grande orientation C5 du SMSI. Ainsi que défini à la phase de Genève du SMSI en 2003, la grande orientation C5 vise à "Etablir la confiance et la sécurité dans l'utilisation des TIC"[907]. A la deuxième réunion de coordination dans le cadre de la grande orientation C5, le Secrétaire général de l'UIT a souligné l'importance de la coopération internationale dans la lutte contre la cybercriminalité. L'élaboration du Programme mondial cybersécurité (GCA) de l'UIT a été annoncée dans la foulée[908]. Le GCA comporte sept buts principaux[909], dont l'un est l'élaboration de

---

902 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: http://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.

903 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: Chapter 6.1.; *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. seqq; *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: http://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*.

904 Regarding the application of Art. 23 et seq. with regard to tradition crimes see: Explanatory Report to the Convention on Cybercrime, No. 243.

905 For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 et seq.

906 The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates.

907 For more information on the C5 Action Line see Meeting Report of 2nd Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: *http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/meetingreport.pdf.*

908 For more information see http://www.itu.int/osg/csd/cybersecurity/gca/.

stratégies pour le développement de législations types de lutte contre la cybercriminalité. Un groupe d'experts a été constitué pour définir les stratégies relevant du GCA[910]. Pour savoir dans quelle mesure une nouvelle législation type interagit avec des normes existantes, il convient de s'intéresser à la démarche adoptée lors de l'élaboration. En règle générale, trois cas sont envisageables:

- Les réglementations sont incompatibles
- Une nouvelle législation type qui définirait des normes incompatibles avec les normes existantes pourrait, au moins dans un premier temps, avoir des effets négatifs sur le nécessaire processus d'harmonisation.
- La nouvelle législation type fait en partie double emploi avec les normes définies par la convention.
- Une nouvelle législation type pourrait s'inspirer de la Convention sur la cybercriminalité en en éliminant les dispositions qui ont pu présenter des difficultés ou dissuader certains pays de la signer. Voir à ce propos la polémique suscitée par une disposition figurant à l'article 32b de la convention, disposition critiquée par la délégation russe à la réunion de 2007 du Comité de la Convention cybercriminalité[911].
- La nouvelle législation type complète les normes de la convention

Une nouvelle législation type peut venir compléter les normes définies par la Convention sur la cybercriminalité et, par exemple, ériger en infraction pénale certains actes relevant de la cybercriminalité et définir des instruments procéduraux qui n'entrent pas encore dans le champ de la convention. La situation a en effet considérablement évolué depuis 2001. Lorsque la convention a été élaborée, le "hameçonnage"[912], le "vol d'identité"[913] et les infractions liées aux jeux en ligne et aux réseaux sociaux n'étaient pas aussi

---

909 1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures. 2. Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime. 3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems. 4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives. 5. Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries. 6. Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas. 7. Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

910 See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

911 Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: *http://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.*

912 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon 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: http://www.usdoj.gov/opa/report_on_phishing.pdf,

913 For an overview about the different legal approaches see: *Gercke*, Internet-related Identity Theft, 2007, available at: http://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; See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://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: http://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.

importants qu'aujourd'hui. Aussi une nouvelle législation type pourrait-elle poursuivre le processus d'harmonisation en intégrant de nouvelles infractions à dimension transnationale[914].

A cet égard, le *Toolkit for Cybercrime Legislation*[915] de l'UIT (boîte à outils pour une législation en matière de cybercriminalité) est un matériel de référence visant à assister les Etats dans la mise en place d'un cadre juridique de dissuasion en matière de cybercriminalité. Il met en avant l'importance d'une harmonisation des cadres juridiques dans le but de combattre plus efficacement les cyberdélits et de faciliter la coopération internationale. Le *Toolkit for Cybercrime Legislation* de l'UIT est élaboré par un groupe d'experts international et pluridisciplinaire. Une première version a été publiée début 2009.

5.5 Relations entre différentes approches législatives nationales et internationales

Comme il a été mentionné précédemment, la cybercriminalité est un fléau véritablement transnational[916]. 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[917], coopération qui est tributaire de l'harmonisation des législations. En raison du principe répandu de double incrimination[918], 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[919]. 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[920]. 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[921]. Les approches nationales tiennent une place importante dans

---

914 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 criminalisation that go beyond the standards of the Convention will proceed with difficulties.

915 Further information on the ITU Cybercrime Legislation Toolkit is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.

916 Regarding the extent of transnational attacks in the most damaging cyber attacks 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.*

917 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.*

918 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties 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 the surrender procedures between Member States (2002/584/JHA).

919 Regarding the dual criminality principle in international investigations see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

920 See Convention on Cybercrime, Art. 23 – Art. 35.

921 See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq.*

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 pollupostage en sont une bonne illustration[922]. Les courriels de pollupostage nuisent en effet tout particulièrement aux pays en développement, question qui a fait l'objet d'un rapport de l'OCDE[923]. Ce rapport montre que le pollupostage 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[924]. Le nombre important des initiatives législatives au niveau national s'explique principalement par le fait que la cybercriminalité a de multiples conséquences selon les pays et chaque Etat 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

A l'heure de la mondialisation technique, où quiconque souhaitant se connecter à Internet doit utiliser les protocoles standard (techniques) en place[925], 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[926]. Or, étant donné la dimension internationale de la cybercriminalité, on peut s'interroger sur la viabilité des approches nationales[927]. 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. Etant 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[928].

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 Etats membres à signer la Convention sur la cybercriminalité; de même ne peut-il pas forcer un Etat signataire à ratifier la convention. Le processus d'harmonisation est donc souvent jugé lent par rapport aux approches législatives nationales et régionales[929]. Contrairement au Conseil de l'Europe, l'Union européenne a les moyens d'obliger ses Etats 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 de l'Union européenne 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

---

922 See above: Chapter 2.6.7.

923 See Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

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

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

926 See for example the following surveys on national Cybercrime legislation: 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; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: https://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: http://www.mosstingrett.no/info/legal.html.

927 Regarding the international dimension see above: Chapter 3.2.6.

928 With regard to the Convention on Cybercrime see: Explanatory Report to the Convention on Cybercrime, No. 33.

929 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.

religieuse[930]. Alors qu'il est peu probable de parvenir à harmoniser au niveau 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[931]. 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[932]. Pour être efficaces, les approches nationales doivent donc en général s'accompagner de mesures additionnelles[933]. Les plus courantes sont:

- 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* (loi d'application relative aux jeux illicites sur Internet), adoptée en 2006 aux Etats-Unis, est un exemple d'une telle approche[934].

---

930 See below: Chapter 6.1.9.

931 See above: Chapter 3.2.6 and Chapter 3.2.7.

932 The issue was addressed by a number of international organisations. The 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: http://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».

933 For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.

934 For an overview about the law see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: *http://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: *http://www.gamblingandthelaw.com/columns/2006_act.htm.* For more information see below: Chapter 6.1.j.

Autre mesure étroitement liée à la précédente, la mise en place d'obligations de filtrage de certains contenus en ligne[935]. Cette approche, qui a fait l'objet de débats à l'occasion de la célèbre affaire Yahoo![936], 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[937] signale qu'une vingtaine de pays environ pratiquent la censure[938].

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.[939] 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 Règles de fond du droit pénal

6.1.1 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.[940] Les motivations des hackers sont très diverses.[941] Il leur est inutile d'être présents sur le lieu

---

935 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: http://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: http://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: http://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: http://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.*

936 See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *http://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.*

937 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: http://www.opennet.net.

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

939. For an overview about legal approaches see also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18 et seq., available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

940 *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/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

941 These range from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimised computer. Even political motivations have been discovered. See: *Anderson*, "Hacktivism and Politically Motivated Computer Crime», 2005, available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf;

du délit;[942] il leur suffit de contourner tous les dispositifs qui protègent les réseaux.[943] 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.[944]

L'accès illégal aux systèmes informatiques empêche les opérateurs de diriger, exploiter et contrôler leurs systèmes en toute tranquillité.[945] L'objectif des dispositifs de protection est de maintenir l'intégrité des systèmes informatiques.[946] Il est essentiel de faire la distinction entre l'accès illégal et les infractions ultérieures, comme l'espionnage de données[947], 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).[948]

La question est de savoir si l'accès illégal doit être criminalisé, en plus des infractions ultérieures ?[949] L'analyse des diverses approches de la criminalisation de l'accès illégal à des systèmes informatiques au niveau national montre que les dispositions en vigueur font 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.[950] 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.[951] D'autres pays, le droit ne criminalise pas l'accès proprement dit mais seulement les infractions ultérieures.[952] 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

---

942 Regarding the independence of place of action and the location of the victim, see above 3.2.7.

943 These can for example be passwords or fingerprint authorisation. 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: http://www.212cafe.com/download/e-book/A.pdf.

944 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 sur la cybercriminalité. See: Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 45.

945 *Gercke*, The Convention sur la cybercriminalité, Multimedia und Recht 2004, Page 729.

946 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 44. "The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

947 With regard to data espionage see above, Chapter 2.4.b and below, Chapter 6.1.2.

948 With regard to data interference see above, Chapter 2.4.d and below, Chapter 6.1.3.

949 *Sieber*, Informationstechnologie und Strafrechtsreform, Page 49 et seq.

950 For an overview of the various legal approaches towards criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003», available at: http://www.mosstingrett.no/info/legal.html.

951 Art. 2 Convention sur la cybercriminalité enables the member states to keep those existing limitations that are mentioned in Art. 2, sentence 2 Convention sur la cybercriminalité. Regarding the possibility to limit the criminalisation see as well: Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 40.

952 An example of this is the German Criminal Code, which criminalised 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.

"hacking" ont conduit à la détection de failles et de points faibles dans la sécurité des systèmes informatiques visés.[953]

Convention sur la cybercriminalité

La Convention sur la cybercriminalité comprend 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 niveau national[954], 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.[955]

La 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 communications mais est indéfini et ouvert à d'autres développements techniques.[956] Il englobe tous les moyens de pénétration dans un autre système informatique, y compris les attaques Internet[957], 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).[958] Cette définition large signifie que l'accès illégal couvre non seulement de futurs développements techniques mais aussi des données secrètes auxquelles ont accès des initiés et des membres du

---

953 This approach is not only found in national legislation, but was also recommended by the Council of Europe Recommendation N° (89) 9.

954 For an overview of the various legal approaches in criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003», available at: http://www.mosstingrett.no/info/legal.html.

955 Regarding the system of reservations and restrictions, see *Gercke*, "The Convention sur la cybercriminalité», Computer Law Review International, 2006, 144.

956 *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

957 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 seqq., available at: http://www.212cafe.com/download/e-book/A.pdf. With regard to Internet related social engineering techniques see the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing , available at: http://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 "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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

958 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 46.

personnel.[959] La deuxième phrase de l'Art. 2 offre la possibilité de limiter la criminalisation de l'accès illégal à l'accès par un réseau.[960]

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.[961]

Elément moral:

Comme toutes les autres infractions définies dans la Convention sur la cybercriminalité, l'Art. 2 repose sur le fait que l'auteur commette les infractions intentionnellement.[962] 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.[963]

Sans droit:

L'accès à un ordinateur ne peut faire l'objet de poursuites, au titre de l'Art. 2 de la Convention, que s'il est commis "sans droit".[964] 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.[965] Outre la question du libre accès, la légitimité des procédures de test de sécurité est également étudiée.[966] 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.[967] 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".[968]

---

959 The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5% of the respondents reported that 80-100% of their losses were caused by insiders. Nearly 40% of all respondents reported that between 1% and 40% 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: http://www.gocsi.com/.

960 Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

961 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 46.

962 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

963 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

964 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

965 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 47.

966 *Jones*, Council of Europe Convention sur la cybercriminalité: Themes and Critiques, Page 7.

967 See for example: World Information Technology And Services Alliance (WITSA), "Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000», available at: http://www.witsa.org/papers/COEstmt.pdf; "Industry group still concerned about draft Cybercrime Convention, 2000», available at: http://www.out-law.com/page-1217.

968 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 47 and Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 62» (Dealing with Article 4).

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"[969], il faut alors vérifier si l'autorisation donnée par la victime couvre l'acte commis par l'auteur.[970] 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.[971] La procédure relative à la façon d'utiliser ces réserves est exposée à l'Art. 42 de la Convention.[972] Ces réserves peuvent concerner des mesures de sécurité[973], l'intention spéciale d'obtenir des données informatiques[974], d'autres intentions malhonnêtes que justifie la culpabilité pénale ou des exigences que l'infraction soit commise contre un système informatique à travers un réseau.[975] On peut trouver une approche similaire dans la Décision-cadre du Conseil de l'UE[976] relative aux attaques visant les systèmes d'information.[977]

---

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

970 This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: http://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 "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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

971 *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

972 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.

973 This limits the criminalisation of illegal access to those cases where the victim used technical protection measures to protect it's computer system. Access an unprotected computer system would therefore not be considered a criminal act.

974 The additional mental element/motivation enables the member states to undertake a more focused approach not implement a criminalisation of the mere hacking. See: Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 47 and Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 62

975 This enables the member states to avoid a criminalisation 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.

976 Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. For more details see above: Chapter 5.1.e.

977 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.

Modèle de loi du Commonwealth "Computer and Computer Related Crimes Act"

On trouve une approche similaire à la section 5 du Modèle de loi du Commonwealth de 2002 sur la criminalité informatique et les délits associés.[978]

> ***Sec. 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 différence principale avec la Convention sur la cybercriminalité est le fait que la Sec. 5 du Modèle de loi du Commonwealth ne contient pas, contrairement à l'Art. 2 de la Convention sur la cybercriminalité, d'options pour faire des réserves.

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999[979], reconnaît que l'accès illégal figure parmi les infractions que les Etats 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'Art. 2 de la Convention 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 reconnu*

---

978 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

979 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 49 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: http://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.

juridiquement") est plus précise que l'expression "sans droit"[980] utilisée dans la Convention sur la cybercriminalité et vise explicitement à intégrer le concept d'autoprotection.[981] La principale différence avec la Convention réside dans le fait que le projet de disposition utilise l'expression "système cybernétique". Le système cybernétique est défini à l'Art. 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'Art. 1 a) de la Convention sur la cybercriminalité.[982] Bien que le projet de Convention se réfère à des actes liés à l'échange de données et met 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.[983]

6.1.2 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.[984] On peut se demander si l'Art. 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,[985] 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.[986] Vu qu'un processus de transfert est nécessaire, il est vraisemblable que l'Art. 3 de la Convention sur la cybercriminalité ne couvre pas des formes d'espionnage de données autres que l'interception de processus de transferts.[987]

A 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 a reçu l'ordre de le réparer) et si à cette occasion (en violation de la légitimation limitée) il

---

980 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

981 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

982 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;

983 Stand alone computer system are covered by Art. 1, paragraph 3 of the Draft Convention because they "control programs». This does not require a network connection.

984 The Explanatory Report points out, that the provision intends to criminalise violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 51.

985 See below: Chapter 6.1.c.

986 See *Gercke*, "The Convention sur la cybercriminalité», Multimedia und Recht 2004, page 730.

987 One key indication of the limitation of the 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 that 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 sur la cybercriminalité, No. 51.

copie des fichiers du système, cet acte n'est en général pas couvert par les dispositions relatives à la criminalisation de l'accès illégal.[988]

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.[989] Aujourd'hui, les utilisateurs d'ordinateurs peuvent avoir recours 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.[990] 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.[991] 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.

Exemples:

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 la loi américaine 18 U.S.C § 1831, 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.

> ***§ 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*

---

988 See in this context especially a recent case from Hong Kong, People's Republic of China. See above: Chapter 2.4.2.

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

990 Regarding the challenges related to the use of encryption technology by offenders see above: Chapter 3.2.m; *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future», No.6, available at: http://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: http://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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

991 One of the consequences related to this aspect is the fact, that the limitation of a criminalisation 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 provision as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

(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.

D'autres pays ont adopté une voie plus large et criminalise l'acte visant à obtenir des données informatiques stockées, même si elles ne contiennent pas de secrets économiques. La précédente version du Code pénal allemand[992] § 202a en est un exemple.

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.[993] En termes d'objets de protection, cette approche est plus large que celle de la loi américaine § 1831 USC, 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.[994] 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.[995]

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 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.[996] 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.

---

992 This provision has recently been modified and now even criminalises illegal access to data. The previous version of the provision was used, because it is suitable to demonstrate the dogmatic structure in a better way.

993 See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

994 A similar approach of limiting criminalisation to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention sur la cybercriminalité: *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: Chapter 6.1.1.

995 This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement self protection measures.

996 See in this context for example a recent cases in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: http://www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Harald, 14.02.2008, available at: http://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: http://www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: http://www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

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[997] sont la preuve évidente du succès des escroqueries basées sur la manipulation des utilisateurs.[998] 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.

6.1.3 Interception illégale

Le recours aux TIC s'accompagne de plusieurs risques liés à la sécurité du transfert de l'information.[999] 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.[1000] Le maillon le plus faible pour l'interception demeure l'utilisateur, en particulier lorsqu'il utilise un ordinateurs 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.[1001] 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

---

997 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*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see above: Chapter 2.8.d.

998 With regard to "phishing» see above: Chapter 2.8.d and below: Chapter 6.1.n and as well: *Jakobsson*, The Human Factor in Phishing, available at: http://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 "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, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

999 Regarding the risks related to the use of wireless networks, see above: Chapter 3.2.c. 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: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

1000 Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1001 Regarding the underlying technology and the security related issues see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: http://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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

ne sont pas protégés contre les interceptions ou accès non autorisés.[1002] Dans la plupart des cas, l'absence de protection est due à une méconnaissance des mesures de protection à mettre en place.[1003]

Dans le passé, les auteurs d'infractions se concentraient principalement sur les réseaux d'entreprises pour pratiquer des interceptions illégales.[1004] 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 cibles.[1005] Ils portent désormais un grand intérêt aux données privées comme les numéros de cartes de crédit, les numéros de sécurité sociale[1006], les mots de passe et les informations sur les comptes bancaires.[1007]

La Convention 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.[1008]

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.*

1002 The computer magazine ct reported in 2004 that field tests proved that more than 50% of 1000 wireless computer networks that were tested in Germany were not protected. See: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182

1003 Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, "Information Technology Security Handbook», page 60, available at: http://www.infodev.org/en/Document.18.aspx.

1004 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1005 Regarding Identity Theft, see above: Chapter: 2.7.3 and below: Chapter 6.1.15 and as well: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://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: http://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: http://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: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1006 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: http://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

1007 See: *Hopkins*, "Cybercrime Convention: A Positive Beginning to a Long Road Ahead», Journal of High Technology Law, 2003, Vol. II, No. 1; Page 112.

1008 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 51.

Les actes couverts:

L'applicabilité de l'Art. 3 est limitée à l'interception de transmissions réalisées par des mesures techniques.[1009] Les interceptions liées aux données électroniques peuvent être définies comme tout acte d'acquisition de données pendant une opération de transfert. [1010]

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.[1011] 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.[1012] 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[1013]; le Rapport explicatif de la Convention contient deux explications quelque peu imprécises concernant l'application de l'Art. 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.[1014] 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 eux-mêmes utilisent l'ordinateur.
- 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".[1015] 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.[1016]

1009 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-criminalisation." Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 53.

1010 Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering».

1011 See *Gercke*, The Convention sur la cybercriminalité, Multimedia und Recht 2004, Page 730.

1012 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1013 See above: Chapter 6.1.2

1014 "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 sur la cybercriminalité No. 55.

1015 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 53.

1016 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 sur la cybercriminalité No. 57.

Le terme "transmission" couvre tous les transferts de données, par téléphone, télécopie, courriel ou transferts de fichiers.[1017] L'infraction établie au titre de l'Art. 3 ne s'applique qu'aux transmissions non publiques.[1018] Une transmission est dite "non publique" si le processus utilisé est confidentiel.[1019] 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".

Elément moral:

Comme toutes les autres infractions définies par la Convention sur la cybercriminalité, l'Art. 3 impose que l'auteur commette les infractions intentionnellement.[1020] 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.[1021]

Sans droit:

L'interception de communications ne peut faire l'objet de poursuites au titre de l'Art. 3 de la Convention que si elle est effectuée "sans droit".[1022] Les rédacteurs de la Convention ont donné une série d'exemples d'interceptions qui ne sont pas effectuées sans droit:

- acte sur ordre ou avec l'autorisation des participants à la transmission;[1023]
- activités autorisées de contrôle ou de protection approuvées par les participants;[1024]
- interception légitime sur la base de dispositions du droit criminel ou dans l'intérêt de la sécurité nationale.[1025]

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'Art. 3.[1026] Les rédacteurs ont souligné que

---

1017 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 51.

1018 *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1019 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 54.

1020 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1021 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1022 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

1023 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 58.

1024 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 58.

1025 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 58.

1026 Cookies are data sent by a server to a browser and the send 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 seqq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

les pratiques commerciales courantes (comme les cookies) n'étaient pas considérées comme des interceptions sans droit.[1027]

Restrictions et réserves:

L'Art. 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.

Modèle de loi du Commonwealth "Computer and Computer Related Crimes"

On trouve une approche similaire à la section 8 du Modèle de loi du Commonwealth de 2002 sur la criminalité informatique et les délits associés.[1028]

Sec. 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.

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999[1029] ne criminalise pas de manière explicite l'interception de données informatiques.

6.1.4 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.[1030] Les attaques ou la tentative d'obtention de ces

---

1027 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 58.

1028 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1029 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: http://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.

1030 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 sur la cybercriminalité, 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 sur la cybercriminalité No. 60.

informations peut entraîner des pertes financières.[1031] Outre la suppression, l'altération de telles informations peut également avoir des conséquences majeures.[1032] Dans certains cas, les législations précédentes ont complètement aligné la protection des données sur la protection des objets tangibles. Cela permet aux auteurs d'infractions de concevoir des escroqueries qui ne conduisent pas à des sanctions criminelles.[1033]

Convention sur la cybercriminalité

A l'Art. 4, la Convention sur la cybercriminalité inclut une disposition qui protège l'intégrité des données contre les brouillages non autorisés.[1034] L'objectif de cette provision 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.[1035]

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:

- Les termes "endommagement" et "détérioration" désignent tout acte lié à l'altération négative de l'intégrité du contenu informatif de données et de programmes[1036];
- 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.[1037] Jeter un fichier dans la poubelle virtuelle n'efface pas ce fichier du disque dur.[1038] Même

---

1031 The 2007 Computer Economics Malware Report focuses on single of 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: http://www.computereconomics.com/article.cfm?id=1225.

1032 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: Chapter 2.7.1 and below: Chapter: 6.1.16.

1033 Regarding the problems related to those gaps see for example the LOVEBUG case where a designer of a computer worm could not be prosecuted due to missing criminal law provisions related to data interference. See above: Chapter 2.4.d 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», http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1034 A similar approach to Art. 4 Convention sur la cybercriminalité 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».

1035 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 60.

1036 As pointed out in the Explanatory Report the two terms are overlapping. See: Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 61.

1037 Regarding the more conventional ways to delete files by Using Windows XP see the Information provided by Microsoft, available at: http://www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

1038 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

lorsque l'on "vide" la poubelle, on n'efface pas nécessairement le fichier.[1039] Il n'est donc pas certain que la possibilité de récupérer un fichier effacé empêche l'application de cette disposition.[1040]

- Le terme "suppression" de données informatiques désigne une action qui touche à la disponibilité des données pour la personne ayant accès au support où l'information est stockée de manière négative.[1041] L'application de ces dispositions fait particulièrement débat en ce qui concerne les attaques par déni de service.[1042] [1043] Pendant les attaques, les données fournies sur le système informatique visé ne sont plus disponibles pour l'utilisateur potentiel ni pour le propriétaire du système informatique.[1044]
- Le terme "altération" désigne la modification de données existantes, sans nécessairement diminuer leur disponibilité.[1045] Cet acte couvre notamment l'introduction de logiciels malveillants comme les logiciels espions, les virus ou les publiciels sur l'ordinateur de la victime.[1046]

Elément moral:

Comme toutes les autres infractions définies par la Convention sur la cybercriminalité, l'Art. 4 impose que l'auteur commette les infractions intentionnellement.[1047] 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.[1048]

1039 See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: http://www.cert.org/archive/pdf/05hb003.pdf.

1040 The fact, that the Explanatory Report mentions that the files are unrecognisable 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 sur la cybercriminalité No. 61.

1041 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 61.

1042 A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications 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: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.In 2000 a number of well known US 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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1043 With regard to the criminalisation of "Denial-of-Service» attacks see as well below: Chapter 6.1.5.

1044 In addition criminalisation of "Denial of Service» attacks is provided by Art. 5 Convention sur la cybercriminalité. See below: Chapter 6.1.5.

1045 Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is likely that the provision could cover unauthorised corrections of faulty information as well.

1046 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://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 recognised functions of malicious software see above: Chapter 2.4.d. Regarding the economic impact of malicious software attacks see above: Chapter 2.9.1.

1047 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1048 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

Sans droit:

De même que pour les dispositions examinées ci-dessus, les actes doivent être commis "sans droit".[1049] Le droit d'altérer des données a été examiné, en particulier dans le contexte du "remailer".[1050] Les remailers sont utilisés pour modifier certaines données afin de faciliter l'anonymat des communications.[1051] Le Rapport explicatif mentionne qu'en principe ces actes sont considérés comme une protection légitime de la vie privée et donc comme étant effectués avec autorisation.[1052]

Restrictions et réserves:

L'Art. 4 donne la possibilité de limiter la criminalisation aux cas où un danger grave survient; c'est une approche similaire à la Décision-cadre de l'UE sur les attaques contre des systèmes d'information[1053] qui permet aux Élément membres de limiter l'application de la disposition de fond de la législation pénale aux "cas qui ne sont pas mineurs".[1054]

Modèle de loi du Commonwealth "Computer and Computer Related Crimes Act"

On peut trouver une approche en accord avec l'Art. 4 de la Convention sur la cybercriminalité à la section 8 du modèle de loi du Commonwealth 2002.[1055]

> ***Sec. 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*

1049 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

1050 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité, 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.

1051 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.

1052 With regard to the possible difficulties to identify offenders that made use of anonymous or encrypted information, the Convention leaves the criminalisation of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 62.

1053 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1054 For further information, see: *Gercke*, "The EU Framework Decision on Attacks against Information Systems», Computer und Recht 2005, page 468 et seq.

1055 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(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.

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999[1056] 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, le Modèle de loi du Commonwealth et l'approche du projet de Convention de Stanford 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 (Art. 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 (Art. 3, paragraphe 1b). Aussi, le projet de loi 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 le Modèle de loi du Commonwealth suivent tous deux une voie plus large en protégeant l'intégrité des données informatiques sans qu'il y ait obligatoirement d'autres effets.

6.1.5 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.[1057] Le manque de disponibilité de pages Internet qui sont victimes d'attaques par

---

1056 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: http://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.

déni de service (DOS)[1058] démontre combien est sérieuse la menace de ces attaques.[1059] Des attaques de ce type peuvent entraîner de graves pertes financières et toucher les systèmes les plus puissants.[1060] Les entreprises ne sont pas les seules cibles. Dans le monde entier des experts discutent actuellement des scénarios possibles de cyber terrorisme qui prennent en compte des attaques contre des infrastructures critiques comme l'alimentation en énergie et les télécommunications.[1061]

Convention sur la cybercriminalité

Pour protéger l'accès des opérateurs et des utilisateurs aux TIC, la Convention sur la cybercriminalité inclut une disposition dans son Art. 5 qui criminalise l'entrave intentionnelle à l'utilisation légitime d'un système informatique.[1062]

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.*

1057 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1058 A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see above: Chapter 2.4.e and 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: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

1059 For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, "Inferring Internet Denial-of-Service Activities», page 1, available at: http://www.caida.org/publications/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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1060 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, page 431-448.

1061 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.; Related to Cyberterrorism see above Chapter 2.8.a and *Lewis*, "The Internet and Terrorism», available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity»; http://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 seqq., available at: http://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 seqq; United States Department of State, "Pattern of Global Terrorism, 2000», in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism», available at: http://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 seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror» in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf. *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

1062 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 sur la cybercriminalité, No. 65.

Les actes couverts:

L'application de cette disposition implique que le fonctionnement d'un système informatique a été entravé.[1063]

- Le terme "entrave" se rapporte à des actions qui portent atteinte au bon fonctionnement du système informatique.[1064] L'application de cette disposition est limitée au cas où l'entrave est le résultat de l'une des actions mentionnées.

La liste des actions par lesquelles le fonctionnement du système informatique a été influencé de manière négative est péremptoire.[1065]

- Le terme "introduction" n'est ni défini 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'Art. 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.[1066]
- Les termes "endommagement" et "détérioration" se recoupent et sont définis par les rédacteurs de la Convention, dans le Rapport explicatif concernant l'Art. 4, comme une altération négative de l'intégrité du contenu informatif de données et de programmes.[1067]
- Le terme "effacement" a également été défini par les rédacteurs de la Convention et du Rapport explicatif concernant l'Art. 4 comme une action où l'information est retirée du support de stockage.[1068]
- Le terme "altération" désigne la modification de données existantes, sans nécessairement diminuer la disponibilité des données.[1069]
- 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.[1070]

De plus, cette disposition est limitée lorsqu'elle s'applique à des cas où l'entrave est "grave". Il est de la responsabilité des Parties de déterminer les critères à remplir pour que l'entrave soit jugée grave.[1071] De

---

1063 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1064 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 66.

1065 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 66.

1066 Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection..

1067 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 61. Regarding the fact, that the definition does not distinguish between the different ways how information can be deleted see above: Chapter 6.1.d. Regarding the impact of the different ways to delete 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1068 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 61.

1069 Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is therefore likely that the provision could cover unauthorised corrections of faulty information as well.

1070 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 61.

1071 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 sur la cybercriminalité, No. 67.

possibles restrictions au titre des législations nationales pourraient inclure un montant minimal de dommages ainsi qu'une limitation de la criminalisation des attaques contre des systèmes informatiques importants.[1072]

Application de la Disposition en ce qui concerne les spams:

On s'est posé la question de savoir si le problème des spams[1073] pouvait être traité au titre de l'Art. 5, sachant que les spams peuvent surcharger les systèmes informatiques.[1074] 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".[1075] Les rédacteurs ont également noté que les Parties peuvent avoir une conception différente de l'entrave dans leur droit interne[1076] par exemple, en faisant de certains actes d'ingérence, des infractions administratives ou en les rendant passibles d'une sanction.[1077]

Elément moral:

Comme toutes les autres infractions définies par le Convention sur la cybercriminalité, l'Art. 5 exige que l'auteur commette une infraction de façon intentionnelle.[1078] 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.[1079]

Sans droit:

L'action doit être exécutée "sans droit".[1080] 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

---

1072 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://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 of operations resulting from attacks against a computer system can be covered by the provision.

1073 "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: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: Chapter 2.5.g.

1074 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1075 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 69.

1076 Regarding legal approaches in the fight against spam see below: Chapter 6.1.l.

1077 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 69.

1078 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1079 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1080 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

inquiétés de la criminalisation possible de leurs travaux.[1081] 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.[1082]

Restrictions et réserves:

Contrairement aux Art. 2 – 4, l'Art. 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[1083] de l'Union Européenne sur les attaques contre les systèmes d'information.[1084]

Modèle de loi du Commonwealth "Computer and Computer Related Crimes Act"

On peut trouver une approche en accord avec l'Art. 5 de la Convention sur la cybercriminalité à la section 7 du modèle de loi du Commonwealth 2002.[1085]

> ***Sec 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;*

1081 See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

1082 Explanatory Report to the Council of Europe Convention sur la cybercriminalité 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, authorised 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 criminalised by this article, even if it causes serious hindering.»

1083 Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

1084 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».

1085 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

La principale différence avec la Convention réside dans le fait que, sur la base de la Sec. 7 du Modèle de loi du Commonwealth, même les actions exécutées avec témérité sont criminalisées. En suivant cette voie, le Modèle de loi 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 Sec. 7 du Modèle de loi du Commonwealth recouvre davantage d'actions par rapport à l'Art. 5 de la Convention sur la cybercriminalité.

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999[1086] 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, le Modèle de loi du Commonwealth et la voie du projet de Convention réside dans le fait que ce dernier couvre toutes les manipulations de systèmes informatiques alors que la Convention sur la cybercriminalité et le Modèle de loi du Commonwealth limitent la criminalisation à l'entrave au bon fonctionnement d'un système informatique.

6.1.6 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. [1087] 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.[1088]

1086 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: http://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.

1087 For an overview on hate speech legislation, see for example: For an overview on hate speech legislation see the data base provided at: http://www.legislationline.org. For an overview on other Cybercrime related legislation see the database provided at: http://www.cybercrimelaw.net.

1088 Regarding the challenges of international investigation see above: Chapter 3.2.f 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;

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.[1089] Sur cette base, la législation vise à protéger le développement harmonieux des mineurs.[1090] L'impact négatif éventuel de l'accès à la pornographie sur le développement des mineurs fait l'objet d'une controverse.[1091] 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.[1092] De même, l'expression "les rendre accessibles" s'applique non seulement à

1089 For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

1090 *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 5.

1091 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, Marco 2003, page 330 et seq., available at: http://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.

1092 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».

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.[1093]

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.[1094]

> ***Sec. 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[1095] les enquêtes internationales concernant de telles approches sont difficiles.[1096]

6.1.7 Pédopornographie

L'Internet devient le principal instrument de commerce et d'échange de matériel contenant de la pédopornographie.[1097] 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.[1098] , Dans le monde entier, des millions d'utilisateurs ont accès et peuvent télécharger les images postées sur une page Internet.[1099] 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.[1100] Dans la plupart des cas, ils

---

1093 *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 28.

1094 The draft law was not in power by the time this publication was finalised.

1095 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime», 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1096 Regarding the challenges of international investigation see above: Chapter 3.2.f and See *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.

1097 *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.

1098 Regarding the methods of distribution, see: *Wortley/Smallbone*, "Child Pornography on the Internet», page 10 et seq., available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication see above: Chapter 3.2.m.

1099 It was reported that some websites containing child pornography experienced 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: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1100 Regarding the challenges related to investigations involving anonymous communication technology see above: Chapter 3.2.l.

ne sont tout simplement pas conscients du sillage électronique qu'ils laissent derrière eux alors qu'ils naviguent sur l'Internet.[1101]

Convention sur la cybercriminalité du Conseil de l'Europe

Afin d'améliorer et d'harmoniser la protection des enfants contre l'exploitation sexuelle,[1102] 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.

1101 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues».

1102 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 91.

La plupart des pays criminalisent déjà les abus envers les enfants ainsi que les méthodes classiques de distribution de matériels pédopornographiques.[1103] La Convention ne se limite donc pas à combler les lacunes des législations pénales nationales[1104], elle cherche également à harmoniser les diverses règlementations.[1105] L'Art. 9 couvre trois éléments controversés:

- l'âge de la personne en cause;
- la criminalisation de la possession de matériels pédopornographiques; et
- la création ou l'intégration d'images fictives.[1106]

Age limite pour les mineurs:

L'une des différences les plus importantes entre les législations nationales est l'âge de la personne en cause. En matière de pédopornographie, certains pays définissent le terme "mineur" dans leur législation nationale comme toute personne âgée de moins de 18 ans et se conforment ainsi à la définition de l'"enfant" donnée à l'Art. 1 de la Convention internationale des droits de l'enfant de l'ONU[1107]. D'autres pays le mineur est un être humain âgé de moins de 14 ans.[1108] On trouve une approche similaire dans la Décision-cadre du Conseil de l'Europe relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie de 2003[1109] et dans la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels de 2007.[1110] Insistant sur l'importance d'une norme internationale uniforme concernant l'âge, la Convention définit ce terme conformément à la Convention de l'ONU.[1111] Toutefois, reconnaissant les différences immenses qui existent dans les législations nationales, la Convention permet aux Parties d'exiger une limite d'âge différente, laquelle ne doit pas être inférieure à 16 ans.

Criminalisation de la possession de matériels pédopornographiques:

La criminalisation de la possession de matériels pédopornographiques diffère également d'un système juridique national à un autre.[1112] La demande pour de tels matériels pourrait encourager leur production sur une base

---

1103 *Akdeniz* in *Edwards / Waelde*, "Law and the Internet: Regulating Cyberspace»; *Williams* in *Miller*, "Encyclopaedia of Criminology», Page 7. Regarding the extend of criminalisation, see: "Child Pornography: Model Legislation & Global Review», 2006, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalisation 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: http://www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf. *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.

1104 Regarding differences in legislation, see: *Wortley/Smallbone*, "Child Pornography on the Internet», page 26, available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1105 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 91.

1106 For an overview of the discussion, see: *Gercke*, "The Cybercrime Convention», Multimedia und Recht 2004, page 733.

1107 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.

1108 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) ...".

1109 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.

1110 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http:// http://conventions.coe.int.

1111 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 104.

1112 Regarding the criminalisation 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 criminalisation of child pornography.

permanente.[1113] Le fait de posséder des matériels pédopornographiques pourrait encourager les abus sexuels sur enfants; les rédacteurs estiment donc qu'une solution efficace pour mettre un frein à la production de matériels pédopornographiques serait de rendre passible de sanctions pénales la possession de tels matériels.[1114] Toutefois, la Convention permet aux Parties, au paragraphe 4, d'exclure la criminalisation de la simple possession en limitant uniquement la responsabilité pénale à la production, à l'offre et à la distribution de matériels pédopornographiques.[1115]

La création ou l'intégration d'images fictives:

Bien que les rédacteurs aient cherché à améliorer la protection de l'enfant contre l'exploitation sexuelle, les intérêts juridiques couverts par le Paragraphe 2 sont plus larges. Le Paragraphe 2(a) s'intéresse directement à la protection contre l'abus sexuel sur mineur. Les Paragraphes 2(b) et 2(c) couvrent des images qui ont été produites sans violation des droits de l'enfant – par exemple, images qui ont été crées par l'utilisation de logiciels de modélisation 3D.[1116] La raison de la criminalisation de la pédopornographie fictive réside dans le fait que ces images peuvent, sans nécessairement créer de danger pour un véritable "enfant", être utilisées pour convaincre des enfants à participer à de telles actions.[1117]

Elément moral:

Comme toutes les autres infractions définies par la Convention sur la cybercriminalité, l'Art. 9 exige que l'auteur commette les infractions de façon intentionnelle.[1118] Dans le Rapport explicatif, les rédacteurs ont souligné de manière explicite que les interactions avec la pédopornographie, sans intention, ne sont pas couvertes par la Convention. Un manque d'intention peut être pertinent, en particulier, si l'auteur ouvre accidentellement une page de l'Internet contenant des images pornographiques enfantines et en dépit du fait qu'il a immédiatement refermé ladite page, certaines images ont été stockées dans des répertoires temporaires ou des fichiers cachés.

Sans droit:

Les actions liées à la pédopornographie ne peuvent faire l'objet de poursuites au titre de l'Art. 9 de la Convention que s'ils se déroulent "sans droit".[1119] Les rédacteurs de la Convention n'ont pas précisé davantage dans quels cas l'utilisateur agit avec autorisation. En général, l'action n'est pas exécutée "sans droit" que si des membres d'organismes d'application de la loi agissent dans le cadre d'une enquête.

1113 See: "Child Pornography: Model Legislation & Global Review», 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

1114 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 98.

1115 *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1116 Based on the National Juvenile Online Victimisation Study, only 3% of the 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

1117 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 102.

1118 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1119 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

Convention du Conseil de l'Europe sur la protection des enfants:

On trouve une autre approche de la criminalisation des actes en matière de pédopornographie à l'Art. 20 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.[1120]

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).*

Les actes couverts:

Cette Disposition est basée sur l'Art. 9 de la Convention sur la cybercriminalité et est donc comparable, dans une large mesure, à cette dernière.[1121] La différence principale réside dans le fait que la Convention sur la cybercriminalité est axée sur la criminalisation d'actes liés à des services d'information et de communication ("production de pédopornographie en vue de sa distribution par un système informatique") alors que la Convention sur la protection de l'enfant adopte principalement une approche élargie ("production de pédopornographie") et couvre même des actions qui ne sont pas liées aux réseaux informatiques.

En dépit des similitudes en ce qui concerne les actes couverts, l'Art. 20 de la Convention sur la protection des enfants ne contient qu'un seul acte qui n'est pas couvert par la Convention. Basé sur l'Art. 20, paragraphe 1f de la Convention sur la protection des enfants, l'acte qui consiste à obtenir l'accès à de la pédopornographie par l'intermédiaire d'un ordinateur est pénalisé. Cela permet aux autorités de police de poursuivre des auteurs lorsqu'elles ont pu prouver que l'auteur avait ouvert des sites Internet contenant de la pédopornographie mais qu'elles n'ont pas pu prouver que l'auteur téléchargeait des matériels. De telles difficultés à recueillir des preuves

---

1120 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1121 *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

se rencontrent, par exemple, lorsque l'auteur fait appel à une technologie de chiffrage pour protéger des fichiers téléchargés sur son support de stockage.[1122] Le Rapport explicatif de la Convention sur la protection des enfants signale que cette disposition devrait également être applicable aux cas où l'auteur ne fait que regarder des images de pédopornographie en ligne sans les télécharger.[1123] De manière générale, l'ouverture d'un site Internet déclenche automatiquement un processus de téléchargement, souvent sans que l'utilisateur le sache.[1124] Le cas évoqué dans le Rapport explicatif n'est donc pertinent que lorsqu'il n'y a pas de téléchargement en tâche de fond.

Modèle de loi du Commonwealth

On peut trouver une approche en accord avec l'Art. 9 de la Convention sur la cybercriminalité à la section 10 du modèle de loi du Commonwealth 2002.[1125]

> ***Sec. 10***
>
> *(1) Toute personne qui, intentionnellement, commet l'une des actions suivantes:*
>
> *(a) publie de la pédopornographie par le biais d'un système informatique; ou*
>
> *(b) produit de la pédopornographie en vue de sa publication par le biais d'un système informatique; ou*
>
> *(c) possède de la pédopornographie dans un système informatique ou sur un support de stockage de données informatiques; commet une infraction passible, après déclaration de culpabilité, d'une peine de prison d'une durée maximale de [durée de la période], ou d'une amende maximale de [montant de l'amende], ou des deux.*[1126]
>
> *(2) C'est une défense contre l'inculpation au titre du paragraphe (1) (a) ou (1) (c) si la personne prouve que la pédopornographie avait un objectif scientifique, de recherche, médical ou d'application de la loi, de bonne foi.*[1127]

1122 Regarding the challenges related to the use of encryption technology see above: Chapter 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.

1123 See Explantory Report to the Convention on the Protection of Children, No. 140.

1124 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 are 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: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

1125 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1126 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].

1127 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.

(3) Dans cette section:

l'expression "pédopornographie" inclut les matériels qui décrivent visuellement:

(a) un mineur ayant une conduite explicite sur le plan sexuel; ou

(b) une personne qui apparaît comme mineure et qui a une conduite explicite sur le plan sexuel; ou

(c) des images réalistes représentant un mineur ayant une conduite explicite sur le plan sexuel.

"mineur" désigne toute personne de moins de [x] ans.

"publie" comprend:

(a) distribuer, transmettre, disséminer, faire circuler, livrer, montrer, prêter en vue d'un gain, échanger, troquer, vendre ou offrir à la vente, louer ou offrir à la location, offrir d'une autre façon ou mettre à disposition de toute autre façon;

(b) avoir en possession ou en garde, ou sous contrôle, dans le but d'effectuer une action mentionnée au paragraphe (a); ou

(c) imprimer, photographier, copier ou faire de toute autre manière (de même nature ou de nature différente) dans le but de commettre un acte mentionné au paragraphe (a).

Les différences principales avec la Convention sur la cybercriminalité reposent dans le fait que le Modèle de loi du Commonwealth ne prévoit pas de définition fixe du terme "mineur" et laisse à ses Etats membres le soin de définir l'âge limite.

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999 [1128] ne contient pas de disposition criminalisant l'échange de pédopornographie par le biais de systèmes informatiques. Les rédacteurs de la Convention ont souligné qu'en général aucun type de discours ou publication n'est nécessaire pour être traité comme une infraction au titre de Projet de Convention de Stanford.[1129] Reconnaissant les différentes approches nationales, les rédacteurs de la Convention ont laissé aux Etats le soin de prendre une décision concernant cet aspect de la criminalisation.[1130]

6.1.8 Incitation à la haine et racisme

Tous les pays ne criminalisent pas l'incitation à la haine.[1131]

Convention sur la cybercriminalité

Vu que les Parties négociant la Convention sur la cybercriminalité n'ont pu se mettre d'accord[1132] sur une position commune concernant la criminalisation de ce type de matériel, des dispositions relatives à ce sujet ont été intégrées dans un Premier protocole séparé à la Convention sur la cybercriminalité.[1133]

1128 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: http://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.

1129 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1130 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1131 For an overview of hate speech legislation, see the database provided at: http://www.legislationline.org.

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.

1132 Explanatory Report to the First Additional Protocol to the Council of Europe Convention sur la cybercriminalité 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.»

1133 Additional Protocol to the Convention sur la cybercriminalité, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

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.

L'une des difficultés principales liée aux dispositions criminalisant les matériels xénophobes est de conserver un équilibre entre la liberté de parole[1134] d'une part et, d'autre part, empêcher la violation des droits des personnes ou des groupes. Sans aller dans le détail, les difficultés qui sont survenues pendant la négociation de la Convention sur la cybercriminalité[1135] et l'état des signatures/ratifications du Protocole additionnel[1136] montre que les différentes mesures de protection de la liberté de parole sont une entrave au bon déroulement d'un processus d'harmonisation.[1137] En ce qui concerne, en particulier, le principe commun de la double incrimination[1138], le manque d'harmonisation conduit à des difficultés dans l'application de la loi en cas de dimension internationale.[1139]

1134 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

1135 Explanatory Report to the First Additional Protocol to the Council of Europe Convention sur la cybercriminalité, No. 4.

1136 Regarding the list of states that signed the Additional Protocol see above: Chapter 5.1.4.

1137 Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/Computer Law Review International(2000)27.pdf.

1138 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime», 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1139 Regarding the challenges of international investigation see above: Chapter 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;

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999 [1140] ne comprend pas de disposition criminalisant le discours de haine. Les rédacteurs de la Convention ont fait remarquer qu'en général, aucun type de discours de haine ou de publication n'est nécessaire pour être traité comme infraction au titre du Projet de Convention de Stanford.[1141] Reconnaissant différentes approches nationales, les rédacteurs de la Convention ont laissé aux états de prendre une décision concernant cet aspect de la criminalisation.[1142]

6.1.9 Infractions d'ordre religieux

L'intensité de la protection des religions et de leurs symboles diffère d'un pays à l'autre.[1143]

Convention sur la cybercriminalité

Les négociations relatives à ce sujet entre les Parties à la Convention sur la cybercriminalité ont connu les mêmes difficultés que celles découvertes à propos de matériels xénophobes.[1144] Les pays qui ont négocié les dispositions du Premier protocole additionnel à la Convention sur la cybercriminalité ont cependant convenu d'ajouter la religion comme objet de 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.*

1140 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: http://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.

1141 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1142 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1143 Regarding the 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: http://www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf;

1144 See above: Chapter 6.1.h as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention sur la cybercriminalité, No. 4.

Bien que ces deux dispositions considèrent la religion comme une caractéristique, elles ne protègent ni la religion ni les symboles religieux par la criminalisation. Ces dispositions criminalisent les menaces et les insultes faites à des personnes au motif qu'elles appartiennent à un groupe.

Exemples de législations nationales

Quelques pays vont au-delà de cette approche et criminalisent davantage les actes liés à des questions religieuses. La Sec. 295B – Sec. 295C du Code pénal du Pakistan en est un exemple:

> ***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.*

En ce qui concerne les incertitudes relatives à l'application de cette disposition, le Projet de loi sur la criminalité électronique de 2006 du Pakistan contient deux dispositions axées sur les infractions liées à l'Internet[1145]:

> ***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.*

De même qu'en ce qui concerne les dispositions criminalisant la distribution de matériel xénophobe lié à l'Internet, l'une des principales difficultés des approches internationales de la criminalisation des infractions religieuses est celle qui est liée au principe de liberté de parole.[1146] Comme cela a déjà été souligné auparavant,[1147] les différentes mesures de protection de la liberté de parole sont une entrave au processus d'harmonisation. En particulier, en ce qui concerne le principe commun de la double incrimination[1148], le manque

---

1145 The draft law was not in power, at the time this publication was finalised.

1146 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

1147 Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ Computer Law Review International(2000)27.pdf.

1148 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime», 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

d'harmonisation conduit à des difficultés dans l'application de la loi dans le cas d'une dimension internationale.[1149]

6.1.10 Jeux illégaux

Le nombre croissant de sites Internet proposant des jeux illégaux est préoccupant,[1150] car ils peuvent être utilisés pour contourner l'interdiction sur les jeux en vigueur dans certains pays.[1151] Si des services sont opérés à partir de lieux qui n'interdisent pas les jeux en ligne, il est difficile pour les pays qui criminalisent le jeu sur Internet d'empêcher leurs citoyens d'utiliser ces services.[1152]

Exemple de législation nationale

La Convention sur la cybercriminalité n'interdit pas les jeux en ligne. On trouvera un exemple de législation nationale à cet égard dans le Code pénal allemand, Sec. 284:

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 a pour objectif de limiter les risques d'addiction[1153] aux jeux en définissant des procédures pour l'organisation de tels jeux.[1154] Elle ne se concentre pas de manière explicite sur les jeux de hasard liés à

1149 Regarding the challenges of international investigation see above: Chapter 3.2.f 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;

1150 The 2005 eGaming data report estimates the total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: http://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: http://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

1151 For an overview of different national Internet gambling legislation, see: "Internet Gambling – An overview of the Issue», GAO-03-89, page 45 et seqq., available at: http://www.gao.gov/new.items/d0389.pdf.

1152 Regarding the situation in the People's Republic of China, see for example: "Online Gambling challenges China's gambling ban», available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

1153 Regarding the addiction see: *Shaffer*, Internet Gambling & Addiction, 2004 , available at: http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: https://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: http://www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

1154 See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

l'Internet mais les inclut également.[1155] A cet égard, elle criminalise les jeux illégaux qui se déroulent sans l'autorisation d'une autorité publique compétente. De plus, elle criminalise quiconque qui (intentionnellement) met les équipements nécessaires à disposition qui sont ensuite utilisés pour des jeux illégaux.[1156] Cette criminalisation va au-delà des conséquences de l'assistance et de la provocation car les auteurs d'infractions peuvent être passibles de condamnations plus sévères.[1157]

Pour éviter des enquêtes criminelles, les opérateurs de sites Internet de jeux illégaux peuvent déplacer, physiquement, leurs activités[1158] vers des pays qui ne criminalisent pas les jeux illégaux.[1159] De tels déplacements constituent un défi pour les autorités de police car le fait qu'un serveur se trouve à l'extérieur du territoire national[1160] n'affecte pas, en général, les possibilités pour un utilisateur à l'intérieur d'un pays d'y accéder.[1161] Afin d'améliorer les possibilités pour les autorités de police de lutter contre les jeux illégaux, le gouvernement allemand a élargi la criminalisation aux utilisateurs.[1162] S'appuyant sur la Sec. 285, les autorités de police peuvent poursuivre les utilisateurs qui participent à des jeux illégaux et peuvent lancer des enquêtes, même lorsque les opérateurs de ces jeux de hasard ne peuvent être poursuivis s'ils se trouvent hors des frontières allemandes:

> ***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.*

Il est souvent difficile d'identifier les délinquants qui utilisent des sites de jeu pour des activités de blanchiment d'argent.[1163] La loi américaine sur les jeux illégaux sur Internet de 2005[1164] est un exemple d'approche[1165] visant à empêcher les jeux illégaux et le blanchiment d'argent.

1155 See *Thumm*, Strafbarkeit des Anbietens von Internetgluecksspielen gemaess § 284 StGB, 2004.

1156 Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which did not know that their services were abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

1157 For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously the criminalisation is limited to those cases where the offender is intentionally making the equipment available.

1158 This is especially relevant with regard to the location of the server.

1159 Avoiding the creation of those safe havens is a major intention of harmonisation processes. The issue of safe havens was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out 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: http://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*».

1160 With regard to the principle of sovereignty changing the location of a server can have a great impact on the ability of the 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: http://www.law.uga.edu/intl/roth.pdf.

1161 Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene see above: Chapter 3.2.6 and Chapter 3.2.7.

1162 For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

1163 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: http://www.gao.gov/new.items/d0389.pdf.

1164 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: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm. Shaker, Americas'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.

1165 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 Approache sin the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: http://www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

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

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.

L'intention de cette loi est de répondre aux difficultés et menaces que font peser les jeux sur l'Internet (transfrontières).[1166] Elle contient deux réglementations importantes: en premier lieu, l'interdiction relative à l'acceptation de tout instrument financier en vue de se livrer à des jeux illégaux sur Internet par toute personne engagée dans l'activité de paris et de spéculations. Cette disposition ne règlemente pas l'acte exécuté par l'utilisateur de sites de jeu sur Internet ou d'institutions financières.[1167] Toute violation de cette interdiction peut conduire à des sanctions pénales.[1168] De plus, cette loi exige du Secrétaire du Trésor et du Conseil des gouverneurs de la réserve fédérale de prescrire des règlementations qui exigent que les fournisseurs de transactions financières soient identifiés et de bloquer les transactions restreintes en relation avec des jeux illégaux sur Internet au moyen de politiques et de procédures raisonnables. Cette seconde réglementation affecte non seulement les personnes engagées dans des activités de paris ou de spéculation mais, en général, toutes les institutions financières. Contrairement à l'acceptation d'instruments financiers pour des jeux illégaux sur l'Internet par des personnes engagées dans des activités de paris ou de spéculations, les institutions financières, d'une manière générale, n'assument pas de responsabilité pénale. En ce qui concerne l'impact international de

1166 *Landes*, "Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation», available at: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm.

1167 *Rose*, "Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed», 2006, available at: http://www.gamblingandthelaw.com/columns/2006_act.htm.

1168 Based on Sec. 5366 the criminalisation is limited to the acceptance of financial instruments for unlawful Internet gambling

ces règlementations, les conflits potentiels avec l'Accord général sur le commerce et les services (GATS)[1169] font actuellement l'objet d'investigations.[1170]

6.1.11 Libelle et Diffamation

Le libellé et la publication de fausses informations ne sont pas des actes qui sont exclusivement commis sur les réseaux. Mais comme cela a déjà été signalé, l'anonymat possible des communications[1171] et les difficultés logistiques liées au très grand nombre d'informations disponibles sur Internet[1172] sont des paramètres abstraits qui facilitent la commission de ces actes.

La question de savoir si cela exige la criminalisation de la diffamation fait l'objet de controverses.[1173] Les préoccupations concernant la criminalisation de la diffamation sont liées, en particulier, au conflit potentiel avec le principe de la "liberté de parole". Un grand nombre d'organisations ont donc demandé le remplacement des lois sur la diffamation pénale.[1174] Le Rapporteur spécial des Nations unies sur la liberté d'opinion et d'expression et le Représentant de l'OSCE pour la liberté des médias se sont exprimés:

> *"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".*[1175]

1169 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.

1170 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: http://www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

1171 See above: Chapter 3.2.l.

1172 See above: Chapter 3.2.2.

1173 See for example: Freedom of Expression, Free Media and Information, Statement of Mr. *McNamara*, United States 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: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://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.

1174 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: http://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 at the 25th of February 2005:

1175 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: http://www.osce.org/documents/rfm/2004/10/14893_en.pdf.

European Convention of Human Rights and the constitutional principle of freedom of expression — the cornerstone of all modern democracies — the European Court of Human Rights, the United States Supreme Court, the UN Rapporteur on Freedom of Opinion and Expression, the OAS Special Rapporteur on Freedom of Expression, the OSCE Representative on Freedom of the Media, constitutional and supreme courts of many countries, and respected international media NGOs have repeatedly stated that criminal defamation laws are not acceptable in modern democracies. These laws threaten free speech and inhibit discussion of important public issues by practically penalising political discourse. The solution that all of them prefer and propose is to transfer the handling of libel and defamation from the criminal domain to the civil law domain»

Malgré ces préoccupations, quelques pays[1176] ont mis en œuvre des dispositions législatives pénales qui criminalisent le libelle ainsi que la publication de fausses informations. Il est important de souligner le fait que même dans les pays qui criminalisent la diffamation, le nombre de cas varie énormément. Ainsi, au Royaume-Uni, en 2004, aucun suspect n'a été condamné pour libelle et on ne dénote qu'un seul cas en 2005.[1177] En Allemagne, les statistiques pénales indiquent qu'il y a eu en 2006 187 527 cas de diffamation.[1178] La Convention sur la cybercriminalité, le Modèle de loi du Commonwealth et le Projet de Convention de Stanford ne contiennent aucune disposition se rapportant directement à ces actes.

Exemple de législation nationale

La Sec. 365 du Code pénal du Qeensland (Australie) est un exemple de disposition législative pénale traitant du libelle. Le Queensland a réintroduit la responsabilité pénale pour la diffamation en 2002 par un Projet de loi modifiant la diffamation pénale.[1179]

Disposition:

365 Diffamation pénale[1180]

(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. […]

La Sec. 185 du Code pénal allemand est un autre exemple de la criminalisation du libelle:

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.

Ces deux dispositions n'ont pas été prises pour couvrir uniquement les actes liés à l'Internet. L'application n'est pas limitée à certains moyens de communications et elle peut donc couvrir les actes commis au sein d'un réseau ainsi que ceux commis à l'extérieur du réseau.

1176 Regarding various regional approaches regarding the criminalisation of defamation see Greene (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: http://www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf.

1177 For more details see the British Crime Survey 2006/2007 published in 2007, available at: http://www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

1178 See Polizeiliche Kriminalstatistik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

1179 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: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf

1180 The full text of the Criminal Code of Queensland, Australia is available at: http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

6.1.12 Spam

Vu que jusqu'à 75 pour cent[1181] de tous les courriels sont déclarés comme spam[1182], la nécessité de sanctions pénales pour les spams a fait l'objet de débats approfondis.[1183] Les solutions législatives nationales concernant les spams diffèrent d'un pays à un autre.[1184] L'une des raisons principales qui font que les spam restent un problème est que la technologie de filtrage ne parvient pas encore à tous les identifier et bloquer.[1185] Les mesures de protection contre les courriels non sollicités n'offrent que des solutions limitées.

En 2005, l'OCDE a publié un rapport qui analysait l'impact des spams dans les pays en développement.[1186] Ce rapport insiste notamment sur le fait que des représentants de pays en développement déclarent souvent que les utilisateurs d'Internet dans leurs pays souffraient beaucoup plus de l'impact des spams et de harcèlements avec menaces sur réseau. L'analyse des résultats de ce rapport prouve que cette impression est correcte. Du fait de ressources plus limitées et plus onéreuses, les spams posent un problème beaucoup plus grave dans les pays en développement que dans les pays occidentaux.[1187]

Cependant, ce n'est pas uniquement l'identification des spams qui pose problème. Il est, en effet, difficile de faire la distinction entre les courriels non désirés par les destinataires, mais qui sont envoyés légalement, et ceux qui sont envoyés de manière illicite. La tendance actuelle en ce qui concerne les transmissions par ordinateurs (y compris les courriels et la VoIP) met en lumière l'importance de la protection des communications contre ces attaques. Lorsque les spams dépassent un certain niveau, ils peuvent gêner gravement l'utilisation des TIC et réduire la productivité des utilisateurs.

Convention sur la cybercriminalité

La Convention sur la cybercriminalité ne criminalise pas les spams de manière explicite.[1188] Les rédacteurs ont suggéré que la criminalisation de ces actes soit limitée à l'entrave grave et intentionnelle aux communications.[1189] Cette approche ne se focalise pas sur les courriels non sollicités mais sur les effets sur un système informatique ou un réseau. S'appuyant sur l'approche juridique de la Convention sur la

---

1181 The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see http://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

1182 For a more information on the phenomenon see above: Chapter 2.5.g. 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.

1183 Regarding the development of spam e-mails, see: *Sunner*, "Security Landscape Update 2007», page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1184 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.

1185 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: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

1186 "Spam Issues in Developing Countries», a. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

1187 See "Spam Issues in Developing Countries», Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

1188 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1189 Explanatory Report to the Council of Europe Convention sur la cybercriminalité 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."

cybercriminalité, la lutte contre les spams pourrait se baser uniquement sur les interférences illégales avec les réseaux et les 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 de Stanford

Le projet informel de Convention de Stanford de 1999[1190] ne contient pas de disposition criminalisant les spams. Tout comme la Convention sur la cybercriminalité, le Projet de Convention de Stanford ne criminalise les spams que si des courriels non sollicités aboutissent à un brouillage intentionnel du système.

Exemple de législation nationale

Cela limite la criminalisation des spams aux cas où le volume de spams a une influence sérieuse sur la puissance de traitement des systèmes informatiques. Les spams qui ont une incidence sur l'efficacité du commerce, mais pas nécessairement sur les systèmes informatiques, ne peuvent faire l'objet de poursuites. Un certain nombre de pays adoptent donc une approche différente. On trouve un exemple dans la loi américaine 18 U.S.C § 1037.[1191]

> ***§ 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).*

1190 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: http://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.

1191 Regarding the United States 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 U.S. conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 et. seq. , available at: http://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.

(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 antispam de 2003.[1192] L'intention de cette Loi était de créer une norme nationale unique élaborée pour contrôler le courrier électronique commercial.[1193] Elle s'applique aux messages électroniques commerciaux mais non aux messages se rapportant à des transactions et à des relations commerciales existantes. L'approche règlementaire exige que les messages électroniques commerciaux incluent une indication de sollicitation, y compris des instructions relatives au droit d'opposition a postériori (opt-out) et l'adresse physique de l'expéditeur.[1194] La loi américaine 18 U.S.C. § 1037 criminalise les expéditeurs de spams notamment si ils falsifient les informations contenues dans les entêtes des courriels afin de détourner la technologie de filtrage.[1195] En outre, cette disposition criminalisait l'accès non autorisé à un ordinateur protégé et le déclenchement de la transmission de messages électroniques commerciaux multiples.

6.1.13 Abus de dispositifs

La disponibilité d'outils logiciels et matériels conçus pour commettre des infractions est une autre question grave.[1196] Outre la prolifération de "dispositifs de piratage", l'échange de mots de passe qui permet à des utilisateurs non autorisés d'accéder à des systèmes informatiques est une difficulté sérieuse.[1197] Vu la disponibilité et la menace potentielle de ces dispositifs, il est difficile de focaliser la criminalisation sur la seule utilisation de ces outils pour commettre des délits. La plupart des législations pénales nationales contiennent des dispositions qui criminalisent la préparation et la production de ces outils en plus de la "tentative d'infraction". La criminalisation de la production de ces outils est une façon de lutter contre la distribution de tels dispositifs. D'une manière générale, cette criminalisation qui, en général accompagne un déplacement vers l'avant important de la responsabilité pénale, est limitée aux délits les plus graves. Dans la législation de l'UE, en particulier, on note des tendances à élargir la criminalisation aux actes préparatoires à des infractions moins graves. [1198]

Convention sur la cybercriminalité

Prenant en compte certaines autres initiatives du Conseil de l'Europe, les rédacteurs de la Convention ont défini une infraction pénale indépendante en ce qui concerne des actes illégaux spécifiques à propos de certains

---

1192 For more details about the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003» – short: CAN-SPAM act 2003 see: http://www.spamlaws.com/f/pdf/pl108-187.pdf.

1193 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)).

1194 For more details see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1195 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.

1196 "Websense Security Trends Report 2004», page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; "Information Security – Computer Controls over Key Treasury Internet Payment System», GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

1197 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.

1198 One example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

dispositifs ou à l'accès à des données à utiliser à des fins abusives dans le but de commettre des infractions contre la confidentialité, l'intégrité et la disponibilité de systèmes ou de données informatiques:[1199]

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.

Les objets couverts:

Le paragraphe 1(a) désigne à la fois les dispositifs[1200] conçus pour commettre et encourager la cybercriminalité et les mots de passe permettant d'accéder à un système informatique.

- Le terme "dispositifs" couvre le matériel ainsi que des solutions basées sur des logiciels pour commettre l'une des infractions mentionnées. Le Rapport explicatif mentionne, par exemple, des logiciels tels que des programmes-virus ou des programmes conçus ou adaptés pour accéder à des systèmes informatiques.[1201]
- Les expressions "mot de passe d'ordinateur, code d'accès ou données similaires", contrairement aux dispositifs n'effectuant pas des opérations, sont des codes d'accès. A cet égard, l'une des questions examinées est de savoir si la publication des vulnérabilités d'un système est couverte par cette

---

1199 Explanatory Report to the Council of Europe Convention sur la cybercriminalité 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".

1200 With its 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.

1201 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 72.

disposition.[1202] Contrairement aux systèmes de code d'accès classique, les vulnérabilités ne permettent pas nécessairement un accès immédiat à un système informatique mais permettent à l'auteur d'utiliser ces points faibles pour réussir à attaquer un système informatique.

Les actes couverts:

La Convention criminalise une large palette d'actions. 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 conçus pour contourner des mesures techniques) figure dans la législation de l'UE concernant l'harmonisation des droits d'auteur[1203] et un certain nombre de pays ont mis en œuvre des dispositions similaires dans leur législation pénale.[1204]

- Le terme "distribution" couvre des actions actives de transmission de dispositifs ou de mots de passe à d'autres.[1205]

1202 See in this context *Biancuzzi*, The Law of Full Disclosure, 2008, available at: http://www.securityfocus.com/print/columnists/466.

1203 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation 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.

1204 See for example one approach in the United States legislation:

18 U.S.C. § 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)v of this section, or both. […]

1205 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 72.

- Le terme "vente" désigne les activités exécutées pour la vente de dispositifs et de mots de passe en contrepartie d'argent ou d'autres compensations.
- L'expression "obtention pour utilisation" couvre des actes liés à l'obtention active de mots de passe et de dispositifs.[1206] Le fait que l'acte d'approvisionnement est lié à l'utilisation de tels outils requiert, en général, une intention de l'auteur d'approvisionner les outils à utiliser qui va au-delà de l'intention "régulière" qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées aux Art. 2 à 5.

L'importation couvre des activités d'obtention de dispositifs et de codes d'accès à partir de pays étrangers.[1207] Il en résulte que des auteurs qui importent de tels outils pour les vendre peuvent être poursuivis même s'ils offrent ces outils. En ce qui concerne le fait que l'obtention de tels outils n'est criminalisée que si elle peut être liée à l'utilisation est sujet à caution si la seule importation sans l'intention de vendre ou utiliser les outils est couverte par l'Art. 6 de la Convention sur la cybercriminalité.

L'expression "mise à disposition" désigne l'action consistant à mettre des dispositifs en ligne pour qu'ils soient utilisés par autrui.[1208] Le Rapport explicatif suggère que l'expression "mise à disposition" couvre également la création ou la compilation d'hyperliens visant à faciliter l'accès à ces dispositifs.[1209]

Outils à double usage:

Contrairement à l'approche de l'Union européenne relative à l'harmonisation des droits d'auteur[1210], cette Disposition de la Convention s'applique non seulement aux dispositifs qui sont conçus exclusivement pour faciliter la commission d'infraction, mais couvre également les dispositifs qui sont généralement utilisés à des fins légitimes et pour lesquels l'intention spécifique des auteurs est de commettre des infractions. Dans le Rapport explicatif, les rédacteurs ont suggéré que cette approche était trop restrictive concernant des dispositifs conçus uniquement pour commettre des infractions et pourrait conduire à des difficultés insurmontables en ce qui concerne l'établissement de la preuve dans les procédures pénales rendant cette disposition pratiquement inapplicable ou applicable uniquement dans de rares cas.[1211]

Pour assurer la bonne protection des systèmes informatiques, les spécialistes utilisent et possèdent divers outils logiciels qui pourraient leur permettre de se concentrer sur l'application de la loi. La Convention examine ces questions sous trois angles différents[1212]:

1206 This approach could lead to a broad criminalization. Therefore Art. 6, Subparagraph 3 Convention sur la cybercriminalité enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.

1207 Art. 6, Subparagraph 3 Convention sur la cybercriminalité enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.

1208 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 72.

1209 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 72: "This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices".

1210 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

1211 Explanatory Report to the Council of Europe Convention sur la cybercriminalité 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.

1212 Regarding the United States approach to address the issue see for example 18 U.S.C. § 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

- Elle permet aux Parties à l'Art. 6, paragraphe 1(b) de faire des réserves concernant la possession d'un nombre minimal de tels articles, avant que soit attribuée la responsabilité pénale.
- a cette exception près, la criminalisation de la possession de ces dispositifs est limitée par l'exigence de l'intention d'utiliser ces dispositifs pour commettre un crime comme exposé aux Art. 2 à 5 de cette Convention.[1213] Le Rapport explicatif signale que cette intention spéciale a été incluse "pour éviter le danger de surcriminalisation lorsque des dispositifs sont produits et placés sur le marché à des fins légitimes, par exemple pour lancer des contre-attaques sur des systèmes informatiques".[1214]
- Enfin, les rédacteurs de la Convention énoncent clairement au paragraphe 2 que les outils créés pour les essais autorisés ou la protection d'un système informatique ne sont pas couverts par cette disposition qui ne couvre que les actes non autorisés.

Criminalisation de la possession:

Le paragraphe 1(b) va au-delà de la réglementation du paragraphe 1(a) en érigeant en infraction pénale la possession de dispositifs ou de mots de passe si elle est liée à l'intention de commettre des infractions. La criminalisation de la possession d'outils fait l'objet de controverses.[1215] L'Art. 6 n'est pas limité aux outils qui sont conçus exclusivement pour commettre des infractions et les opposants à la criminalisation de la possession de ces dispositifs craignent la création de risques inacceptables pour les administrateurs de systèmes et les spécialistes de la sécurité des réseaux.[1216] La Convention autorise les Parties à exiger qu'un certain nombre de ces éléments soient détenus avant que la responsabilité pénale soit retenue.

Elément moral:

Comme toutes les autres infractions définies par la Convention sur la cybercriminalité, l'Art. 6 exige que l'auteur commette les infractions intentionnellement.[1217] En sus de l'exigence générale de l'intention en ce qui concerne les actes couverts, l'Art. 6 de la Convention sur la cybercriminalité exige qu'il y ait intention spécifique d'utiliser le dispositif pour commettre l'une ou l'autre des infractions établies aux Art. 2 à 5 de la Convention sur la cybercriminalité.[1218]

(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.

1213 Gercke, Cybercrime Training for Judges, 2009, page 39, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1214 Explanatory Report to the Council of Europe Convention sur la cybercriminalité 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'."

1215 See *Gercke*, The Convention sur la cybercriminalité, Multimedia und Recht 2004, Page 731.

1216 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: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

1217 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1218 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 76.

Sans droit:

Pareillement aux dispositions examinées ci-dessus, les actions doivent être commises "sans droit".[1219] En ce qui concerne les craintes que la Disposition puisse être utilisée pour criminaliser l'exploitation légitime d'outils logiciels dans des mesures d'autoprotection, les rédacteurs de la Convention ont souligné que de tels actes n'étaient pas considérés comme étant exécutés "sans droit".[1220]

Restrictions et réserves:

Du fait du débat sur la nécessité de criminaliser la possession des dispositifs, la Convention offre le choix d'une réserve complexe à l'Art. 6, paragraphe 3 (en plus du paragraphe 1(b), deuxième phrase). Si une Partie utilise cette réserve, elle peut exclure la criminalisation de la possession d'outils et un certain nombre d'actions illégales au titre du paragraphe 1(a) – par exemple, la production de tels dispositifs.[1221]

Modèle de loi du Commonwealth

On trouve dans la Sec. 9 du Modèle de loi du Commonwealth de 2002 une approche conforme à l'Art. 6 de la Convention sur la cybercriminalité.[1222]

> ***Sec. 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.*

1219 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

1220 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 77.

1221 For more information see: Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 78.

1222 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(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.

La différence principale avec la Convention sur la cybercriminalité repose dans le fait que le Modèle de loi du Commonwealth criminalise les actes commis avec témérité. Durant les négociations concernant le Modèle de loi du Commonwealth, d'autres amendements à la Disposition qui criminalise la possession de tels dispositifs ont été discutés. Le groupe d'experts a suggéré la criminalisation dans le cas d'auteurs possédant plus d'un dispositif.[1223] Le Canada a proposé une approche similaire sans définir par avance le nombre de dispositifs aboutissant à la criminalisation.[1224]

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999[1225] inclut une disposition criminalisant les actes liés 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;

Les rédacteurs de la Convention ont souligné qu'en général aucun type de discours ou publication ne doit être qualifié de criminel au titre du Projet de Convention de Stanford.[1226] La seule exception faite est liée aux dispositifs illégaux.[1227] Dans ce contexte, les rédacteurs ont mis en lumière le fait que la criminalisation devait

---

1223 Expert Groups suggest 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.*

1224 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.*

1225 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: http://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.

1226 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1227 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

être limitée aux actes mentionnés et ne pas couvrir, par exemple, la discussion sur la vulnérabilité des systèmes.[1228]

6.1.14 Falsification informatique

Les poursuites pénales visant des actes de falsification informatique ont tendance à se raréfier du fait que la plupart des textes juridiques sont des documents tangibles. Avec la numérisation, cette situation évolue.[1229] La généralisation de l'utilisation de documents numériques s'accompagne de la création d'un arrière plan juridique concernant leur utilisation, par exemple, par la reconnaissance juridique des signatures numériques. En outre, les dispositions contre la falsification informatique jouent un rôle important dans le combat contre le "hameçonnage".[1230]

Convention sur la cybercriminalité

La plupart des législations pénales criminalisent la falsification de documents matériels.[1231] Les rédacteurs de la Convention ont signalé que la structure dogmatique de l'approche juridique nationale variait d'un pays à l'autre.[1232] Alors qu'un concept est basé sur l'authenticité de l'auteur du document, un autre repose sur l'authenticité de la Déclaration. Les rédacteurs ont décidé de mettre en œuvre des normes minimales et de protéger la sécurité et la fiabilité des données électroniques en créant une infraction parallèle à la falsification

---

1228 "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: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1229 See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

1230 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.

1231 See for example 18 U.S.C. § 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.

1232 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 82.

classique de documents matériels pour combler les lacunes du droit pénal qui pourrait ne pas s'appliquer aux données stockées électroniquement.[1233]

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.*

L'objet couvert:

Les données, qu'elles soient ou non directement lisibles et intelligibles, constituent la cible de la falsification informatique. Les données informatiques sont définies par la Convention[1234] comme "toute représentation de fait, 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". Cette disposition ne se réfère pas seulement aux données informatiques comme l'objet d'un des actes mentionnés. En outre, il faut que ces actes se traduisent par des données non authentiques.

L'Art. 7 exige, au moins en ce qui concerne l'élément moral, que les données soient l'équivalent d'un document public ou privé. Cela signifie que les données doivent être pertinentes sur le plan légal[1235]; la falsification de données qui ne peuvent être utilisées à des fins juridiques n'est pas couverte par cette disposition.

1) Les actes couverts:
   - L'entrée de données[1236] doit correspondre à la production d'un faux document matériel.[1237]
   - Le terme "altération" se réfère à la modification de données existantes.[1238] Le Rapport explicatif insiste en particulier sur les variations et les modifications partielles.[1239]
   - Le terme "suppression" de données informatiques désigne tout acte qui affecte la disponibilité des données.[1240] Dans le Rapport explicatif, les rédacteurs se réfèrent en particulier au fait de retenir ou de cacher des données.[1241] Cet acte peut être commis, par exemple en bloquant certaines informations d'une base de données pendant la création automatique d'un document électronique.

1233 Explanatory Report to the Council of Europe Convention sur la cybercriminalité 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.»

1234 See Art. 1 (b) Convention sur la cybercriminalité.

1235 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 84.

1236 For example by filling in a form or adding data to an existing document.

1237 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 84.

1238 With regard the definition of "alteration» in Art. 4 see Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 61.

1239 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 83.

1240 With regard the definition of "suppression» in Art. 4 see Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 61.

1241 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 83.

- Le terme "effacement" est défini à l'Art. 4 qui couvre les actes par lesquels des informations sont retirées.[1242] Le Rapport explicatif ne se réfère qu'au fait de retirer des données figurant sur un support.[1243] Mais la portée de cette disposition milite fortement en faveur d'une définition plus large du terme "effacement". Sur la base d'une telle définition élargie, cet acte peut être soit commis en retirant un fichier complet soit en effaçant une partie des informations d'un fichier.[1244]

Elément moral:

Comme toutes les autres infractions définies dans la Convention sur la cybercriminalité, l'Art. 3 repose sur le fait que l'auteur commet les infractions intentionnellement.[1245] 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.[1246]

Sans droit:

Les actes de falsification ne peuvent être poursuivis au titre de l'Art. 7 de la Convention que s'ils sont commis "sans droit".[1247]

Restrictions et réserves:

L'Art. 7 offre également la possibilité de faire une réserve afin de limiter la criminalisation, en exigeant des éléments additionnels comme l'intention de frauder, avant que la responsabilité pénale soit engagée.[1248]

Modèle de loi du Commonwealth

Le Modèle de loi du Commonwealth de 2002 ne contient pas de disposition criminalisant la falsification informatique.[1249]

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999[1250], contient une disposition qui criminalise les actes liés aux données informatiques falsifiées.

1242 With regard the definition of "deletion» see Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 61.

1243 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 83.

1244 If only part of a document is deleted the act might also be covered by the term "alteration».

1245 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1246 Explanatory Report to the Council of Europe Convention sur la cybercriminalité, No. 39.

1247 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

1248 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 85.

1249 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

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 différence principale avec l'Art. 7 de la Convention sur la cybercriminalité repose dans le fait que l'Art. 3 1b) ne se focalise pas sur la simple manipulation de données mais exige une interférence avec un système informatique. L'Art. 7 de la Convention sur la cybercriminalité n'exige pas un tel acte. Il suffit que l'auteur ait agi dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.

6.1.15 Vol d'identité

Compte tenu de la couverture médiatique de ce sujet[1251], des résultats d'enquêtes récentes[1252] ainsi que de nombreuses publications juridiques et techniques[1253] parues dans ce domaine, on peut dire que le vol d'identité est un phénomène de masse.[1254] Malgré les aspects mondiaux de ce phénomène, tous les pays n'ont pas encore inclus dans leurs législations pénales nationales des dispositions qui criminalisent tous les actes liés au vol d'identité. La Commission de l'Union européenne a récemment déclaré que le vol d'identité n'avait pas encore été criminalisé dans tous les Etats membres de l'UE[1255] et que la coopération européenne en matière de répression serait mieux servie si l'usurpation d'identité était érigée en infraction pénale dans tous les Etats membres. Elle a annoncé qu'elle engagerait sous peu des consultations afin de savoir s'il était judicieux de légiférer.[1256]

1250 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: http://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.

1251 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*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

1252 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.

1253 See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://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: http://www.privacyrights.org/ar/id_theft.htm.

1254 Regarding the phenomenon of identity theft see above: Chapter 2.7.3.

1255 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.

1256 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.

L'un des problèmes liés à la comparaison des instruments juridiques existant dans la lutte contre le vol d'identité est le fait qu'ils sont extrêmement différents les uns des autres.[1257] Le seul élément cohérent des approches existantes réside dans le fait que le comportement condamné est lié à une ou plusieurs des phases suivantes:[1258]

- Phase 1: Acte d'obtenir des données d'identification personnelle;
- Phase 2: Acte de posséder ou de transférer des données d'identification personnelle;
- Phase 3: Acte d'utiliser des données d'identification personnelle à des fins criminelles.

Sur la base de ces observations, on trouve en général deux approches systématiques pour criminaliser le vol d'identité:

- L'élaboration d'une disposition qui criminalise l'acte d'obtenir, posséder et utiliser des données d'identification personnelle (à des fins criminelles).
- La criminalisation individuelle d'actions typiques liée à l'obtention de données d'identification personnelle (comme l'accès illégal, la production et la diffusion de logiciels malveillants, de falsifications informatiques, d'espionnage de données et d'ingérence avec les données) et aussi d'actes liés à la possession et à l'utilisation de telles informations (comme la fraude informatique).

Exemple d'une approche par une disposition unique

Les exemples les plus connus d'approches par disposition unique sont les lois américaines 18 U.S.C. § 1028(a)(7) et 18 U.S.C. 1028A(a)(1). Ces dispositions couvrent une grande série d'infractions liées au vol d'identité. Dans cette approche, la criminalisation n'est pas limitée à une certaine phase mais couvre les trois phases mentionnées ci-dessus. Il faut néanmoins insister sur le fait que cette disposition ne couvre pas toutes les activités liées au vol d'identité, notamment celles où la victime agit et non l'auteur de l'infraction.

> ***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 Eats-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;*

1257 *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.

1258 *Gercke*, Internet-related Identity Theft, 2007, available at: http://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.

(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

Pour commettre des délits liés au vol d'identité, l'auteur doit entrer en possession de données liées à l'identité.[1259] En criminalisant le "transfert" de moyens d'identification avec l'intention de commettre une infraction, ces dispositions criminalisent les actes liés à la Phase 1 d'une manière très large.[1260] Du fait que ces dispositions se concentrent sur l'acte de transfert, elles ne couvrent pas les actes effectués par l'auteur avant le début du processus de transfert.[1261] Des actes comme l'envoi de courriels d'hameçonnage et la conception de logiciels malveillants qui peuvent être utilisés pour obtenir des données liées à une identité d'ordinateur des victimes ne sont pas couverts par les lois américaines 18 U.S.C. § 1028(a)(7) et 18 U.S.C. 1028A(a)(1).

Phase 2

En criminalisant la possession, avec l'intention de commettre une infraction, ces dispositions adoptent de nouveau une large approche en ce qui concerne la criminalisation d'actes liés à la seconde phase. Cela inclut notamment la possession de données d'identification personnelle avec l'intention de les utiliser ultérieurement dans le cadre de l'une des infractions classiques liées au vol d'identité.[1262] La possession de données d'identification personnelle sans l'intention de les utiliser n'est pas couverte.[1263]

1259 This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data see above *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.

1260 The reason for the success is the fact that the provisions are focussing on the most relevant aspect of phase 1: the transfer of the information from the victim to the offender.

1261 Examples for acts that are not covered is the illegal access to a computer system in order to obtain identity related information.

1262 One of the most common ways the obtained information are used are linked to fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1263 Further more it is uncertain if the provisions criminalise the possession if the offender does not intent to use them but sell them. The prosecution could in this case in general be based on fact that 18 U.S.C. § 1028 does not only criminalise the possession with the intent to use it to commit a crime but also to aid or abet any unlawful activity.

Phase 3

En criminalisant l'"utilisation" avec l'intention de commettre une infraction, ces dispositions couvrent les actes liés à la phase 3. La loi américaine 18 U.S.C. § 1028(a)(7) ne concerne pas, comme il est indiqué auparavant, une infraction spécifique (comme la fraude).

Exemple d'une approche de disposition multiple

La différence principale entre la Convention sur la cybercriminalité et les approches par disposition unique (comme, par exemple, l'approche des Etats-Unis) réside dans le fait que la Convention ne définit pas une offense cybernétique séparée de l'utilisation illicite de données d'identification personnelle.[1264] Pareillement à la situation concernant la criminalisation de l'obtention de données d'identification personnelle, la Convention ne couvre pas tous les actes possibles liés à l'utilisation illicite d'informations personnelles.

Phase 1

La Convention sur la cybercriminalité[1265] contient un certain nombre de dispositions qui criminalisent les actes de vol d'identité liés à l'Internet en Phase 1. Il s'agit, notamment:

- de l'accès illégal (Art. 2)[1266];
- de l'interception illégale (Art. 3)[1267];
- de l'atteinte à l'intégrité des données (Art. 4) [1268].

Compte tenu des diverses possibilités pour un auteur d'accéder aux données, il faut signaler que tous les actes possibles de la Phase 1 ne sont pas couverts. Ainsi, l'espionnage de données est un exemple d'infraction qui est souvent lié à la Phase 1 du vol d'identité mais qui n'est pas couvert par la Convention sur la cybercriminalité.

Phase 2

Les actes qui sont exécutés entre l'obtention de l'information et son utilisation à des fins criminelles ne peuvent pas vraiment être couverts par la Convention sur la cybercriminalité. Il est impossible, en particulier, d'empêcher le développement d'un marché noir des données d'informations personnelles en criminalisant la vente de telles informations en se basant sur les dispositions contenues dans la Convention.

Phase 3

La Convention sur la cybercriminalité du Conseil de l'Europe définit un certain nombre d'infractions liées à la cybercriminalité. Certaines peuvent être commises par l'auteur en utilisant des données d'informations personnelles. A titre d'exemple, on citera la fraude informatique qui est souvent évoquée dans le contexte du vol

---

1264 See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf .

1265 Similar provisions are included in the Modèle de loi du Commonwealth and the Draft Stanford Convention. For more information about the Modèle de loi du Commonwealth see: "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Draft Stanford 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: http://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.

1266 See above: Chapter 6.1.1.

1267 See above: Chapter 6.1.3.

1268 See above: Chapter 6.1.4.

d'identité.[1269] Les enquêtes sur les vols d'identité soulignent que la plupart des données obtenues ont été utilisées pour la fraude à la carte de crédit.[1270] Si la fraude à la carte de crédit est commise en ligne, il est vraisemblable que son auteur sera poursuivi au titre de l'Art. 8 de la Convention sur la cybercriminalité. D'autres infractions qui peuvent être exécutées en utilisant des données d'informations personnelles qui ont été obtenues précédemment mais qui ne sont pas mentionnées dans la Convention ne sont pas couvertes par ce cadre juridique. Il est notamment impossible d'entamer des poursuites en cas d'utilisation de données d'informations personnelles avec l'intention de cacher l'identité.

6.1.16 Fraude informatique

La fraude est une activité courante dans le cyberespace.[1271] C'est également un problème courant au-delà de l'Internet et c'est pour cette raison que la plupart des législations nationales contiennent des dispositions qui criminalisent de telles infractions.[1272] Or, l'application de dispositions existantes à des cas liés à l'Internet peut s'avérer difficile lorsque les dispositions législatives criminelles nationales classiques sont basées sur la fausseté de la personne.[1273] Dans la plupart des cas de fraude commis sur l'Internet, c'est en fait un système informatique qui répond à un acte de l'auteur. Si les dispositions criminelles classiques traitant de la fraude ne couvrent pas les systèmes informatiques, une mise à jour de la législation nationale est nécessaire.[1274]

1269 *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1270 See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 – available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf .

1271 See above: Chapter 2.7.1.

1272 Regarding the criminlisation of computer-related fraud in the UK see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 et seq.

1273 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.

1274 A national approach that is explicitly address computer-related fraud is 18 U.S.C. § 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 U.S.C. 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;

Convention sur la cybercriminalité

La Convention sur la cybercriminalité cherche à criminaliser toute manipulation exagérée dans le cadre du traitement de données avec l'intention d'affecter un transfert illégal de propriété en fournissant un article qui concerne la fraude informatique:[1275]

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.*

Les actes couverts:

L'Art. 8a) contient une liste des actes les plus pertinents de la fraude informatique.[1276]

- L'"introduction" de données informatiques couvre tous les types de manipulations d'introductions comme l'introduction de données incorrectes dans l'ordinateur ainsi que les manipulations de logiciels et autres interférences avec le traitement de données.[1277]
- Le terme "altération" désigne la modification de données existantes.[1278]
- Le terme "suppression" de données informatiques désigne tout acte qui affecte la disponibilité des données.[1279]
- Le terme "effacement" correspond à la définition de ce terme à l'Art. 4 qui couvre les actes au cours desquels des informations sont retirées.[1280]

Outre la liste des actes, l'Art. 8 b) contient la clause générale qui criminalise "l'atteinte au fonctionnement d'un système informatique" liée à la fraude. Cette clause générale a été ajoutée à la liste des actes couverts afin de laisser ouverte cette disposition dans la perspective de développements ultérieurs.[1281]

Le Rapport explicatif signale que l'atteinte au fonctionnement d'un système informatique couvre des actes tels que les manipulations de matériels, 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.[1282]

1275 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 86.

1276 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 sur la cybercriminalité No 86.

1277 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 86.

1278 With regard the definition of "alteration» in Art. 4 see Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 61.

1279 With regard the definition of "suppression» in Art. 4 see Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 61.

1280 With regard the definition of "deletion» see Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 61.

1281 As a result, not only data- related offences, but also hardware manipulations, are covered by the provision.

1282 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 87.

Perte économique:

Selon la plupart des législations criminelles nationales, l'infraction doit entraîner une perte économique. La Convention suit un concept similaire et limite la criminalisation aux actes par lesquels les manipulations occasionnent directement à autrui un préjudice économique ou matériel qui englobe l'argent et les immobilisations corporelles ou incorporelles ayant une valeur économique.[1283]

Elément moral:

Comme pour les autres infractions énumérées, la Convention sur la cybercriminalité exige à son Art. 8 que l'auteur ait agi dans une intention frauduleuse ou malhonnête en vue d'obtenir un avantage économique ou autre pour lui-même ou autrui.[1284] Le Rapport explicatif donne comme exemples d'actes exclus de la responsabilité criminelle par suite d'un manque d'intention particulière les pratiques 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.[1285]

Sans droit:

La fraude informatique ne peut faire l'objet de poursuites au titre de l'Art. 8 de la Convention que si elle est commise "sans droit".[1286] Cela inclut l'exigence que les avantages économiques doivent être obtenus sans droit. Les rédacteurs de la Convention ont signalé que les actes commis conformément à un contrat valable entre les personnes affectées ne sont pas considérés comme étant sans droit[1287].

Modèle de loi du Commonwealth

Le Modèle de loi du Commonwealth de 2002 ne contient pas de disposition criminalisant la fraude informatique.[1288]

Projet de Convention de Stanford

Le projet informel de Convention de Stanford de 1999[1289], ne contient pas de disposition criminalisant la fraude informatique.

1283 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 88.

1284 "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."

1285 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 sur la cybercriminalité No 90.

1286 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

1287 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No 90.

1288 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

6.1.17 Infractions liées aux atteintes 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.[1290] La reproduction d'œuvres musicales, artistiques 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 cohérente.[1291]

L'industrie des loisirs a réagi en mettant en œuvre des mesures techniques (gestion des droits numériques ou DRM) pour empêcher la reproduction[1292], mais, jusqu'à présent, ces mesures ont généralement été contournées peu après leur introduction.[1293] Il existe divers outils logiciels sur l'Internet qui permettent aux utilisateurs de copier des CD de musique et des DVD de films qui sont 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 l'Internet.[1294]

Convention sur la cybercriminalité

La Convention comporte donc une disposition couvrant ces infractions liées aux atteintes à la propriété intellectuelle qui s'efforce d'harmoniser les diverses réglementations que l'on trouve dans la législation nationale:

> ***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,*

1289 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: http://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.

1290 Regarding the ongoing transition process, see: "OECD Information Technology Outlook 2006», Highlights, page 10, available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.

1291 For more information on the effects of the digitalisation for the entertainment industry see above: Chapter 2.6.a.

1292 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 the copy protection that 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

1293 Regarding the technical approach of copyright protection see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: http://www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

1294 For details see above: Chapter 2.6.1.

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.

Les infractions aux droits d'auteur sont déjà criminalisées dans la plupart des pays[1295] et sont visées dans un certain nombre de traités internationaux.[1296] La Convention a pour objectif de fournir des principes

---

1295 Examples are 17 U.S.C. § 506 and 18 U.S.C. § 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) oftitle 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: http://www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

1296 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: http://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: http://www.unctad.org/en/docs/iteipc200610_en.pdf; Regarding international approaches of anti-circumvention laws see: Brown, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: http://www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

fondamentaux concernant la criminalisation des violations des droits d'auteur afin d'harmoniser les législations nationales existantes. Les violations concernant les brevets ou les marques déposées ne sont pas couvertes par cette disposition.[1297]

Références à des accords internationaux:

Contrairement aux autres cadres juridiques, la Convention ne désigne pas de façon explicite les actes à criminaliser mais se réfère à un certain nombre d'accords internationaux.[1298] C'est l'un des aspects critiqués en ce qui concerne l'Art. 10. Outre le fait que cela rend plus difficile de découvrir l'ampleur de la criminalisation et que ces accords risquent d'être modifiés ultérieurement, soulever la question de savoir si la Convention oblige les états signataires à signer les accords internationaux mentionnés à l'Art. 10. Les rédacteurs de la Convention ont souligné qu'aucune obligation de ce type ne sera introduite par la Convention sur la cybercriminalité.[1299] Les états qui n'ont pas signé les accords internationaux mentionnés ne sont donc ni obligés de signer les accords ni de criminaliser les actes liés à des accords qu'ils n'ont pas signé. L'Art. 10 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 limite la criminalisation aux actes qui ont été commis au moyen d'un système informatique.[1300] 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 et tient compte de la terminologie utilisée à l'Art. 61 de l'Accord sur les ADPIC[1301] qui régit l'obligation de criminaliser les violations de droits d'auteurs.[1302]

Echelle commerciale:

La limitation à des actes qui sont commis sur une échelle commerciale tient compte également de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) qui exige des sanctions pénales uniquement pour "piratage sur une échelle commerciale". La plupart des violations de droits d'auteurs dans des systèmes à partage de fichiers ne sont pas commises sur une échelle commerciale et ne sont donc pas couverts par l'Art. 10. La Convention s'efforce de fixer des normes minimales pour les infractions liées à

1297 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 109.

1298 Explanatory Report to the Council of Europe Convention sur la cybercriminalité 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."

1299 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité, 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."

1300 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 16 and 108.

1301 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.

1302 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 113.

l'Internet. Aussi, les Parties peuvent aller au-delà du seuil de "l'échelle commerciale" dans la criminalisation des violations de droits d'auteurs.[1303]

Sans droit:

D'une manière générale, les dispositions de la loi pénale substantielle définies par la Convention sur la cybercriminalité exigent que l'acte soit commis "sans droit".[1304] Les rédacteurs de la Convention ont souligné que le terme "violation" impliquait déjà que l'acte était commis sans autorisation.[1305]

Restrictions et réserves:

Le paragraphe 3 permet aux signataires de faire 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 de Stanford

Le projet informel de Convention de Stanford de 1999[1306], n'inclut pas de disposition criminalisant les violations de droits d'auteurs. Les rédacteurs de la Convention ont fait remarquer que les infractions en matière de droits d'auteurs n'étaient pas incluses du fait des difficultés associées.[1307] Au lieu de cela, ils se sont référés directement aux accords internationaux existants.[1308]

6.2 Droit de procédure

6.2.1 Introduction

Comme il est expliqué dans les sections précédentes, la lutte contre la cybercriminalité exige des dispositions adéquates en matière de droit pénal substantiel.[1309] ans les pays soumis au droit civil, au moins, les autorités de police ne pourront pas enquêter sur des délits tant ces législations ne seront pas en place. Mais les exigences de ces autorités dans la lutte contre la cybercriminalité ne sont pas limitées aux dispositions du droit pénal

---

1303 Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 114.

1304 The element "without right» is a common component in the substantive criminal law provisions of the Convention sur la cybercriminalité. 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 sur la cybercriminalité, No. 38.

1305 See Explanatory Report to the Council of Europe Convention sur la cybercriminalité, 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.

1306 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: http://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.

1307 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1308 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1309 See above: Chapter 4.4.1 and Chapter 6.1.

substantiel.[1310] Afin de mener à bien leurs enquêtes, elles doivent disposer, en plus de la formation et du matériel, de moyens de procédure qui leur permettent de prendre les mesures nécessaires pour identifier les auteurs et recueillir les preuves requises pour les poursuites judiciaires.[1311] Ces mesures peuvent être les mêmes que celles qui sont prises pour d'autres enquêtes qui n'ont pas de rapport avec la cybercriminalité; mais en ce qui concerne le fait que l'auteur ne doit pas nécessairement être présent ou même proche de la scène du délit, il est très vraisemblable que les enquêtes en matière de cybercriminalité devront être effectuées de manière différente des enquêtes classiques.[1312]

La raison pour laquelle différentes techniques d'enquête sont nécessaires n'est pas due seulement à l'indépendance du lieu et de la scène du délit. Dans la plupart des cas, il s'agit d'une combinaison d'un certain nombre des difficultés mentionnées auparavant pour les autorités de police qui font que les enquêtes en matière de cybercriminalité sont uniques.[1313] Si l'auteur se trouve dans un autre pays[1314], qu'il a utilisé des services qui permettent des communications anonymes et que de plus il commet des délits en utilisant différents terminaux Internet publics, il devient très difficile de mener une enquête sur ce délit en se basant seulement sur les instruments classiques comme la recherche et la saisie. Pour éviter toute incompréhension, il est important de souligner que les enquêtes de cybercriminalité doivent s'appuyer sur un travail de détective classique et avoir recours aux moyens d'enquête classiques – mais les enquêtes de cybercriminalité vont de pair avec les difficultés qui ne peuvent être résolues qu'au moyen d'instruments d'enquête classiques.[1315]

Quelques pays ont déjà mis au point de nouveaux instruments pour permettre aux autorités de police d'enquêter en matière de cybercriminalité et de délits classiques en procédant à des analyses de données informatiques.[1316] Comme c'est le cas en ce qui concerne le droit pénal substantiel, la Convention sur la cybercriminalité du Conseil de l'Europe contient un ensemble de dispositions qui reflètent des normes minimales largement acceptées en ce qui concerne les instruments de procédure requis pour mener des enquêtes de cybercriminalité.[1317] La vue générale qui suit se réfèrera donc aux instruments proposés par cette convention internationale et, de plus, mettra en lumière des approches nationales qui vont au-delà des règlementations de la Convention.

1310 This was as well highlighted by the drafters of the Council of Europe Convention sur la cybercriminalité that 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 sur la cybercriminalité No. 132. Regarding the substantive criminal law provisions related to Cybercrime see above: Chapter 6.1.

1311 Regarding the elements of a Anti-Cybercrime strategy see above: xxx. Regarding user-based approaches in the fight against Cybercrime see: *Görling*, The Myth Of User Education, 2006 at http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See as well the comment made by *Jean-Pieree 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.»

1312 Due to the protocols used in Internet communication and the 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: Chapter 3.2.7.

1313 Regarding the challenges of fighting Cybercrime see above: Chapter 3.2.

1314 The pure fact that the offender is acting from a different country can go along with additional challenges for the law enforcement agencies as the investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases the investigation never the less requires an international cooperation of the authorities in both countries that in general is more time consuming compared to investigations concentrating on a single country.

1315 See in this context as well: Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 134.

1316 For an overview about the current status of the implementation of the Convention sur la cybercriminalité and its procedural law provisions in selected countries see the country profiles made available on the Council of Europe website: http://www.coe.int/cybercrime/.

1317 See Art. 15 – 21 Council of Europe Convention sur la cybercriminalité.

6.2.2 Enquêtes sur ordinateurs et sur l'Internet (expertise légale en informatique)

Il existe plusieurs définitions de "l'expertise légale en informatique".[1318] On peut la définir comme étant "l'examen d'équipements et de systèmes de TI en vue d'obtenir des informations dans le cadre d'enquêtes pénales ou civiles".[1319] Lorsqu'ils commettent des infractions, les auteurs laissent des traces.[1320] Cela est valable autant pour les enquêtes classiques que pour les enquêtes informatiques. La différence principale entre une enquête classique et une enquête de cybercriminalité repose dans le fait que cette dernière exige en général des techniques d'enquête spécifiques liées aux données et qu'elle peut être facilitée par le recours à des outils informatiques spécialisés.[1321] En plus d'instruments de procédures adéquats, il faut pour exécuter ces analyses que les autorités soient capables de gérer et d'analyser des données pertinentes. En fonction des infractions et de la technologie informatique nécessaires, les exigences en ce qui concerne l'instrument d'enquête de procédure et la technique analytique d'expertise légale en informatique diffèrent[1322] et s'accompagnent de difficultés uniques.[1323]

Généralement, ces deux aspects des enquêtes de cybercriminalité sont étroitement liés et on les désigne souvent par l'expression terme générique d' "expertise légale en informatique", qui recouvre la collecte et l'analyse de preuves.[1324] Comme cela a été décrit auparavant, l'expression "expertise légale en informatique" recouvre l'application de techniques d'enquêtes et d'analyses informatiques à la recherche de preuves potentielles. Ces activités englobent de nombreuses analyses allant de l'analyse générale comme la recherche de

---

1318 *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: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://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;

1319 *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

1320 For an overview on different kind 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: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

1321 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

1322 For an overview about 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: https://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: http://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: https://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf;

1323 *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

1324 See in this context ABA International Guide to Combating Cybercrime, 128 et seq.

pédopornographie sur les disques durs d'ordinateurs[1325], à des enquêtes spécifiques d'expertise légale sur les iPod[1326] et l'accès à des fichiers chiffrés.[1327] Les spécialistes de l'expertise légale en informatique apportent leur soutien aux enquêtes effectuées par les services spécialisés de la police et par les procureurs. En ce qui concerne les enquêtes sur Internet, ces spécialistes sont capables, par exemple, d'apporter leur concours aux activités suivantes[1328]:

- identifier de possibles traces numériques, (en particulier l'emplacement possible de données de trafic)[1329];
- apporter leur aide aux prestataires de services sur Internet en identifiant les informations qu'ils peuvent fournir en soutien des enquêtes;
- protéger les données pertinentes recueillies et vérifier la continuité de la possession.[1330]

Dès qu'une preuve potentielle est identifiée, les experts peuvent aussi, par exemple, fournir une assistance dans les cas suivants:

- protection du système informatique faisant l'objet de l'enquête pendant l'analyse, à partir d'une modification possible ou de l'endommagement de données;[1331]
- découverte de tous les fichiers pertinents concernant le système informatique en question et les supports de stockage;[1332]
- décrypter les fichiers cryptés;[1333]
- récupérer des fichiers supprimés;
- identifier l'usage du système informatique dans le cas où plus d'une personne y aurait accès;[1334]
- révéler le contenu de fichiers temporaires utilisés par des applications et par le système d'exploitation;
- analyser les preuves recueillies;[1335]
- fournir une documentation relative à l'analyse;[1336]

1325 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.

1326 *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2

1327 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf;

1328 Regarding the models of Forensic Investigations see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.

1329 *Gercke*, Cybercrime Training for Judges, 2009, page 56, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1330 This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.

1331 This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.

1332 This includes stored files as well as deleted files that have not yet been completely removed from the hard disk. In addition experts might be able to identify temporary, hidden or encrypted files. *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.

1333 Regarding legal approaches related to the use of encryption technology see below: Chapter 6.2.9.

1334 *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1.

1335 *Gercke*, Cybercrime Training for Judges, 2009, page 55, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

- apporter la preuve pour d'autres enquêtes;
- fournir des services de consultance spécialisés et des témoignages.

Le rôle des spécialistes en expertise légale en informatique dans la protection de l'intégrité des preuves met en lumière le fait que le travail de ces spécialistes associe des aspects techniques et juridiques. L'une des principales difficultés dans ce contexte est la chaîne de possession qui exige que l'audit précis des données d'origine se fasse en parallèle avec les exigences très strictes liées aux travaux pratiques des spécialistes en expertise légale en informatique[1337]

La mesure de la participation de ces spécialistes démontre leur importance dans le cadre du processus d'enquête. De plus, le lien entre le succès des enquêtes relatives à Internet et la disponibilité de ressources en expertise légale en informatique signifie qu'il faut mettre en place des formations dans ce domaine. Ce n'est que si les enquêteurs sont soit formés en expertise légale en informatique soit ont accès à des spécialistes dans ce domaine que l'on pourra conduire avec efficacité enquêtes et poursuites dans le monde de la cybercriminalité.

6.2.3 Sauvegardes

Au cours de ces dernières années, les autorités de police dans le monde ont mis en lumière le besoin urgent d'instruments d'enquête adéquats.[1338] Dans ces conditions, il est peut-être surprenant que la Convention sur la cybercriminalité ait été critiquée en ce qui concerne les instruments de procédure.[1339] Ces critiques se focalisent principalement sur le fait que la Convention contient un certain nombre de dispositions qui prévoient des instruments d'enquête (Art. 16 – Art. 21) mais une seule une disposition (Art. 15) qui traite des sauvegardes.[1340] En outre, on peut noter que contrairement aux dispositions du droit pénal substantiel contenu dans la Convention, on ne compte que très peu de possibilités d'ajustements nationaux dans le cadre de la mise en œuvre de la Convention.[1341] La critique en tant que telle se concentre pour l'essentiel sur les aspects quantitatifs. Il est vrai que la Convention suit le concept de réglementation centralisée des sauvegardes au lieu de les associer individuellement à chaque instrument. Mais cela ne signifie pas nécessairement un affaiblissement de la protection des droits des suspects.

La Convention sur la cybercriminalité a été élaborée, dès le début, comme un cadre international et un instrument pour lutter contre la cybercriminalité qui n'est pas limité aux Etats membres du Conseil de l'Europe.[1342] Pendant les négociations sur les instruments de procédure nécessaires, les rédacteurs de la Convention, qui comprenaient des représentants de pays non européens comme les Etats-Unis et le Japon, ont compris que les approches nationales existantes en matière de sauvegarde et notamment de protection des

---

1336 Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at: http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

1337 Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at: http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

1338 See *Gercke*, Convention sur la cybercriminalité, Multimedia und Recht. 2004, page 801 for further reference.

1339 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 Finacial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at http://www.ccc.de.

1340 See *Breyer,* Council of Europe Convention sur la cybercriminalité, DUD, 2001, 595 et seqq.

1341 Regarding the possibilities of making reservations see Article 42 of the Convention sur la cybercriminalité:

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.

1342 See above: Chapter 5.1.4.

suspects dans le cadre des divers systèmes de droit pénal étaient si différentes les unes des autres qu'il serait impossible de fournir une solution détaillée unique pour tous les Etats membres.[1343] Les rédacteurs de la Convention ont donc décidé de ne pas inclure de réglementation spécifique dans le texte de la Convention mais au contraire de demander aux Etats membres de veiller à ce que soient appliquées les normes fondamentales de sauvegarde nationales et internationales.[1344]

> ***Article 15 – Conditions et sauvegardes***
>
> *1. Chaque Partie veille à ce que l'instauration, la mise en oeuvre 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'Art. 15 repose sur le principe que les Etats signataires appliqueront les conditions et sauvegardes qui existent déjà dans leur droit interne. Si les législations contiennent des normes centrales applicables à tous les instruments d'enquête, ces principes s'appliqueront également aux instruments liés à l'Internet.[1345] Lorsque le droit interne ne repose pas sur une réglementation centralisée des sauvegardes et des conditions, il faut analyser les sauvegardes et conditions mises en œuvre eu égard aux instruments classiques qui sont comparables aux instruments liés à l'Internet.

Mais la Convention ne se réfère pas uniquement aux sauvegardes existant dans les législations nationales. Cela aurait l'inconvénient que les exigences d'application diffèrent d'une façon telle que les aspects positifs de l'harmonisation ne s'appliqueraient plus. Pour garantir que les Etats signataires qui pourraient avoir des sauvegardes et des traditions juridiques différentes mettent en œuvre certaines normes[1346], la Convention sur la cybercriminalité définit les normes minimales en se référant aux cadres fondamentaux comme les suivants:

- Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales adoptée par le Conseil de l'Europe en 1950;

1343 "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 sur la cybercriminalité No. 145.

1344 "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 sur la cybercriminalité No. 145.

1345 For the transformation of safeguards to 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.

1346 This is especially relevant with regard to the protection of the suspect of an investigation.

- Pacte international relatif aux droits civils et politiques des Nations-Unies, de 1966;
- Autres instruments internationaux applicables concernant les droits de l'homme.

La Convention pouvant être signée et ratifiée également par des pays qui ne sont pas membres du Conseil de l'Europe[1347], il est important de souligner que non seulement le Pacte international relatif aux droits civils et politiques des Nations-Unies mais aussi la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe seront pris en considération lorsque l'on évaluera les systèmes de sauvegarde d'Etats signataires qui ne sont pas membres de la Convention sur la cybercriminalité.

En ce qui concerne les enquêtes de cybercriminalité, l'une des dispositions les plus pertinentes de l'Art. 15 de la Convention sur la cybercriminalité est la référence à l'Art. 8, paragraphe 2, de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe.

> ***Art. 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 sécurité 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'est efforcée de définir de façon plus précise les normes qui régissent les enquêtes électroniques et notamment la surveillance. Aujourd'hui, la jurisprudence est devenue l'une des sources les plus importantes en ce qui concerne les normes internationales liées aux enquêtes relatives à la communication.[1348] Cette jurisprudence prend particulièrement en considération la gravité de l'ingérence des enquêtes[1349], ses objectifs[1350] et sa proportionnalité.[1351] Les principes fondamentaux qui peuvent être extraits de la jurisprudence sont les suivants:

- une base juridique suffisante pour les instruments d'enquête est nécessaire;[1352]
- la base juridique légale doit être précise en ce qui concerne le sujet;[1353]
- les compétences des autorités de police doivent être prévisibles;[1354]

1347 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.

1348 ABA International Guide to Combating Cybercrime, page 139.

1349 "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.

1350 "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

1351 "Powers of secret surveillance of citizens, characterising 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.

1352 "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.

1353 "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.

- la surveillance des communications ne peut être justifiée que dans le contexte d'infractions graves.[1355]

De plus, l'Art. 15 de la Convention sur la cybercriminalité tient compte du principe de proportionnalité.[1356] Cette disposition est particulièrement pertinente pour les Etats signataires qui ne sont pas membres du Conseil de l'Europe. Lorsque le système national de sauvegardes existant ne protège pas de manière adéquate les suspects, il est obligatoire que les Etats membres élaborent les sauvegardes nécessaires dans le cadre du processus de ratification et de mise en œuvre.

Enfin, l'Art. 15, sous-paragraphe 2 de la Convention sur la cybercriminalité se réfère explicitement à quelques unes des sauvegardes les plus importantes[1357], y compris:

- la supervision;
- les motifs justifiant l'application;
- la limitation du champ d'application et de la durée.

Contrairement aux principes fondamentaux décrits ci-dessus, les sauvegardes qui sont mentionnées ici ne doivent pas nécessairement être mises en œuvre en ce qui concerne un instrument quelconque mais seulement si cela est approprié vu la nature ou la procédure concernées. C'est aux organes législatifs nationaux de prendre la décision à cet égard.[1358]

Un aspect important lié au système de sauvegardes prévu par la Convention sur la cybercriminalité réside dans le fait que la capacité des autorités de police à utiliser ces instruments de manière souple d'une part et, d'autre part, à garantir les sauvegardes effectives dépend de la mise en œuvre d'un système progressif de sauvegardes. La Convention n'empêche pas de manière explicite les Parties de mettre en œuvre les mêmes sauvegardes (par exemple les exigences de l'ordonnance d'un tribunal) pour tous les instruments mais une telle approche aurait une influence sur la souplesse des autorités de police. La capacité à assurer une protection adéquate des droits des suspects dans un système progressif de sauvegardes dépend, en grande partie, de l'équilibre entre l'impact potentiel d'un instrument d'enquête et les sauvegardes associées. Pour parvenir à cet équilibre, il faut faire la différence entre des instruments plus ou moins exigeants. La Convention sur la cybercriminalité contient un certain nombre d'exemples de ce type de différenciation qui permettent aux Parties de mieux développer un système de sauvegardes progressives:

- différenciation entre l'interception de données relatives au contenu (Art. 21)[1359] et la collecte de données relatives au trafic (Art. 20).[1360] Contrairement à la collecte de données relatives au trafic, l'interception de données relatives au contenu est limitée à des infractions graves.[1361]

1354 "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

1355 "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, characterising 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.

1356 "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 sur la cybercriminalité No. 146.

1357 The list is not concluding. See: Explanatory Report to the Council of Europe Convention sur la cybercriminalité No. 146.

1358 "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 sur la cybercriminalité No. 147.

1359 See below 6.2.9

- différenciation entre l'ordre de conservation rapide de données informatiques stockées (Art. 16)[1362] et la soumission des données informatiques conservées, basée sur l'injonction de produire (Art. 18).[1363] L'Art. 16 n'autorise les autorités de police qu'à donner l'ordre de préserver les données mais pas de les divulguer.[1364]
- différenciation entre l'obligation de soumettre les "données relatives aux abonnés"[1365] et les "données informatiques"[1366] à l'Art. 18.[1367]

Si l'intensité d'un instrument d'enquête et l'impact potentiel sur un suspect sont correctement évalués et si les sauvegardes sont conçues en accord avec les résultats d'analyse, le système de sauvegardes progressives ne conduit pas à un système déséquilibré d'instruments de procédure.

6.2.4 Conservation et divulgation rapides de données stockées dans un système informatique (Procédure de "gel rapide")

L'identification d'un auteur qui a commis un acte de cybercriminalité nécessite souvent l'analyse de données relatives au trafic.[1368] C'est le cas, en particulier, lorsque l'adresse IP utilisée par l'auteur peut aider les autorités de police à retrouver sa trace. Tant que les autorités de police ont accès aux données pertinentes relatives au trafic, il est même possible, dans certains cas, d'identifier un auteur qui utilise des terminaux Internet publics qui ne demandent pas d'identification.[1369]

L'une des difficultés principales auxquelles sont confrontés les enquêteurs est le fait que les données de trafic très pertinentes pour les informations en question sont souvent supprimées automatiquement après une courte période. La raison de cette suppression automatique est le fait qu'au terme d'un processus (par exemple, l'envoi d'un courriel, l'accès à l'Internet ou le téléchargement d'un film), les données de trafic générées pendant le processus et qui garantissent que le processus a pu se dérouler ne sont plus nécessaires. En ce qui concerne les aspects économiques de cette activité, la plupart des fournisseurs d'accès à Internet cherchent à supprimer les informations le plus rapidement possible car le stockage de données pour des périodes plus longues nécessiterait des capacités de stockage encore plus grandes (onéreuses). [1370]

1360 See below 6.2.10.

1361 "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 sur la cybercriminalité 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 sur la cybercriminalité No. 230.

1362 See below 6.2.4.

1363 See below 6.2.7.

1364 As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorise the law enforcement agencies to prevent the deletion of the relevant data. The advantage of a 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.

1365 A definition of the term "subscriber information» is provided in Art. 18 Subparagraph 3 Convention sur la cybercriminalité.

1366 A definition of the term "computer data» is provided in Art. 1 Convention sur la cybercriminalité.

1367 As described more in detail below the differentiation between "computer data» and "subscriber information» the Art. 18 Convention sur la cybercriminalité enables the signatory states to develop graded safeguards with regard to the production order.

1368 "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 sur la cybercriminalité No. 155.; Regarding the identification of suspects by IP-based investigations see: Gercke, Preservation of User Data, DUD 2002, 577 et seq.

1369 *Gercke*, Preservation of User Data, DUD 2002, 578.

1370 The cost issue was especially raised within the discussion about 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: http://www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

Toutefois, les aspects économiques ne sont pas les seuls pour lesquels les autorités de police doivent effectuer leurs enquêtes rapidement. Certains pays ont un arsenal législatif qui empêche le stockage de certaines données de trafic au terme d'un processus. On citera à titre d'exemple de telles restrictions l'Art. 6 de la Directive 2002/58/E6 du Parlement européen et du Conseil concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.[1371]

> ***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'Art. 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 un aspect critique des enquêtes relatives à Internet. D'une manière générale, comme il est vraisemblable qu'un certain temps s'écoulera entre la commission, la découverte de l'infraction et la notification des autorités de police, il est important de mettre en œuvre des mécanismes qui empêchent que les données pertinentes soient effacées pendant l'enquête qui peut parfois être longue. A cet égard, deux approches différentes sont actuellement examinées[1372]:

- Conservation des données; et
- Protection des données (procédure de "gel rapide").

Une obligation de conservation des données oblige le prestataire de services Internet de conserver les données relatives au trafic pendant une certaine période.[1373] Selon les approches législatives les plus récentes, les données doivent être conservées pendant des périodes allant de 6 à 24 mois.[1374] Cela permettrait aux autorités de police d'accéder aux données lorsque cela est nécessaire pour identifier un auteur d'infraction même plusieurs

---

1371 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.

1372 The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantaged 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. A similar discussion took place during the negotiation of the Convention sur la cybercriminalité. The drafters explicitly pointed out, that the Convention does not establish a data retention obligation. See Explanatory Report to the Convention sur la cybercriminalité, No. 151., available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

1373 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.

1374 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.

mois après la commission d'infraction.[1375] L'obligation de conservation des données a été récemment adoptée par le Parlement de l'Union européenne[1376] et est actuellement à l'étude aux Etats-Unis[1377] En ce qui concerne les principes de conservation des données, on trouvera d'autres informations ci-dessous.

Convention sur la cybercriminalité

La protection des données est une approche différente dont l'objectif est de veiller à ce qu'une enquête de cybercriminalité n'échoue pas tout simplement parce que les données relatives au trafic ont été effacées pendant l'enquête.[1378] S'appuyant sur la législation relative à la protection des données, les autorités de police peuvent ordonner à un prestataire de services d'empêcher l'effacement de certaines données. La protection rapide des données informatiques est un instrument qui devrait permettre aux autorités de police de réagir immédiatement et d'éviter le risque d'effacement résultant de la longueur des procédures d'enquête.[1379] Les rédacteurs de la Convention sur la cybercriminalité ont décidé de se focaliser sur la "protection des données" au lieu de la "conservation des données.[1380] L'Art. 16 de la Convention sur la cybercriminalité contient une réglementation:

> ***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 oeuvre 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.*

1375 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.»

1376 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.

1377 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 StoppingAdults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: http://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.

1378 See *Gercke*, The Convention sur la cybercriminalité, Multimedia und Recht 2004, page 802.

1379 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 sur la cybercriminalité, No. 160.

1380 *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

Du point de vue des fournisseurs d'accès à Internet (FAI) la conservation des données est un moyen moins exigeant que leur conservation.[1381] Les FAI n'ont pas à stocker toutes les données de tous les utilisateurs; en revanche ils doivent veiller à ce que des données spécifiques ne soient pas effacées dès qu'ils reçoivent un ordre venant d'une autorité compétente. La conservation des données offre des avantages car elle couvre la conservation proprement dite, non seulement du point de vue des FAI, mais aussi dans la perspective de la protection de ces données. Il n'est pas nécessaire de conserver les données de millions d'utilisateurs d'Internet mais seulement les données qui sont liées à d'éventuels suspects dans le cadre d'enquêtes criminelles. Il faut, néanmoins, souligner que la conservation des données offre des avantages lorsque lesdites données sont supprimées immédiatement après la commission d'une infraction. Dans ces cas, l'ordre de conservation des données, contrairement à une obligation de conservation des données ne permet pas d'empêcher l'effacement des données concernées.

L'injonction, au sens de l'Art. 16, oblige uniquement le FAI à sauvegarder les données qu'il a traitées et qui n'étaient pas effacées au moment où il a reçu l'injonction.[1382] L'ordre n'est pas limité aux données de trafic car ces dernières ne sont citées qu'à titre d'exemple. L'Art. 16 n'oblige pas l'auteur à commencer à collecter des informations qu'en principe il ne stockerait pas.[1383] De plus, l'Art. 16 n'oblige pas le fournisseur à transférer les données pertinentes aux autorités. Cette disposition autorise uniquement les autorités de police à empêcher la suppression des données pertinentes mais n'engage pas les fournisseurs à transférer les données. L'obligation de transfert est règlementée aux Art. 17 et 18 de la Convention sur la cybercriminalité. L'avantage d'une séparation de l'obligation de conserver les données et l'obligation de les divulguer tient au fait qu'il est possible de requérir différentes conditions pour leur application.[1384] En ce qui concerne l'importance de la réaction immédiate, il serait judicieux, par exemple, de suspendre l'exigence d'une injonction émanant d'un juge et de permettre à la justice ou à la police d'ordonner la conservation.[1385] Cela permettrait aux autorités compétentes de réagir plus rapidement. Les droits du suspect peuvent être protégés en demandant une injonction de divulgation des données.[1386]

La divulgation des données conservées figure parmi d'autres aspects réglementés à l'Art. 18 de la Convention sur la cybercriminalité:

1381 See *Gercke*, The Convention sur la cybercriminalité, Multimedia und Recht 2004, page 803.

1382 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 sur la cybercriminalité, No. 159.

1383 Explanatory Report No 152.

1384 Regarding the advantages of a system of graded safeguards see above: Chapter 6.2.3.

1385 "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 sur la cybercriminalité, No. 160.

1386 The drafters of the Convention sur la cybercriminalité tried to approach the problems related to the need of immediate action from law enforcement agencies on the one hand side and the importance of ensuring safeguards on the other hand side 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 sur la cybercriminalité 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."

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 prestataire 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 prestataire 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.

Conformément à l'Art. 18, sous section 1 a) de la Convention sur la cybercriminalité, les prestataires de services qui ont conservé les données peuvent être mis dans l'obligation de les divulguer.

L'Art. 18 de la Convention sur la cybercriminalité n'est pas seulement applicable après qu'une injonction de conservation conformément à l'Art. 16 de la Convention sur la cybercriminalité ait été émise.[1387] Cette disposition est un instrument général que les autorités de police peuvent utiliser. Si le destinataire de l'injonction de produire transfère volontairement les données requises, les autorités de police ne sont pas limitées à la saisie du matériel mais peuvent également appliquer l'injonction de produire moins qui est moins exigeante. Comparée à la saisie proprement dite du matériel, l'injonction de soumettre les informations pertinentes est généralement moins exigeante. Son application est donc particulièrement pertinente lorsque les investigations technico-légales n'exigent pas l'accès au matériel.

Outre l'obligation de soumettre les données informatiques, l'Art. 18 de la Convention sur la cybercriminalité permet aux autorités de police d'ordonner la soumission des données relatives aux abonnés. Cet instrument d'enquête est d'une grande importance dans les enquêtes basées sur l'IP. Si les autorités de police peuvent identifier une adresse IP qui a été utilisée par l'auteur lorsqu'il a commis l'infraction, elles devront identifier cette personne[1388] qui a utilisé l'adresse IP au moment de l'infraction. Conformément à l'Art. 18, sous-

---

1387 *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1388 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 does only enable 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.

section 1 b) de la Convention sur la cybercriminalité, un prestataire de services est obligé de soumettre les données relatives aux abonnés énumérées à la sous-section 3 de l'Art. 18.[1389]

Dans les cas où les autorités de police remontent jusqu'à un auteur d'infraction ayant besoin d'un accès immédiat pour identifier le parcours suivi par la communication qui a été transmise, l'Art. 17 leur permet d'ordonner la 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 prestataires 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 prestataires 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 il est indiqué ci-dessus, la Convention sépare strictement l'obligation de conserver des données à la demande de celles de les divulguer aux autorités compétentes.[1390] L'Art. 17 établit un classement précis car il combine l'obligation d'assurer la conservation des données relatives au trafic dans les cas où un certain nombre de prestataires de services ont été impliqués et celle de divulguer les informations nécessaires afin d'identifier la voie par laquelle la communication a été transmise. Sans cette divulgation partielle, les autorités de police ne pourraient pas dans certains cas, remonter jusqu'à l'auteur lorsque plus d'un fournisseur a été impliqué.[1391] Du fait de la combinaison de deux obligations qui affectent le droit des suspects de différentes façons, il convient d'examiner le point central des sauvegardes liées à cet instrument.

Modèle de Loi du Commonwealth sur l'informatique et les délits liés à l'informatique

On peut trouver des approches similaires dans le modèle de Loi du Commonwealth de 2002.[1392]

Disposition:

> ***Sec. 15***
>
> *Lorsqu'un magistrat est satisfait sur la base d'une demande 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 judiciaires, le magistrat peut ordonner:*

1389 If the offender is using services that do not require a registration or the subscriber information provided by the user are 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).

1390 *Gercke*, The Convention sur la cybercriminalité, Multimedia und Recht 2004, page 802.

1391 "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 sur la cybercriminalité, No. 167.

1392 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(a) qu'une personne sur le territoire du [Etat prenant les dispositions], qui contrôle un système informatique produise à partir de données informatiques spécifiées ou d'une impression ou d'autres sorties intelligibles de ces données; et

(b) qu'un prestataire de services Internet du [Etat prenant les dispositions] produise des informations sur des personnes qui sont abonnées ou qui d'une autre façon utilisent le service; et

(c)[1393] *qu'une personne sur le territoire du [Etat prenant les dispositions] qui a accès à un processus d'un système informatique spécifié et compile des données informatiques spécifiées à partir du système et les donne à une personne spécifiée.*

Sec. 16[1394]

Si un officier de police est satisfait que les données stockées dans un système informatique sont raisonnablement demandées 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) la voie par laquelle la communication a été transmise.

Sec. 17

(1) Si un officier de police est satisfait que:

(a) les données stockées dans un système informatique sont raisonnablement demandées 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 demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.

6.2.5 Conservation des données

Une obligation de conservation des données oblige le prestataire de services Internet à sauvegarder des données relatives au trafic pendant une certaine période de temps.[1395] La mise en œuvre d'une obligation de conservation de données est une approche visant à éviter les difficultés mentionnées ci-dessus concernant l'accès à des

---

1393 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.

1394 The Modèle de loi du Commonwealth 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.

1395 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:

ttp://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

données relatives au trafic avant qu'elles soient supprimées. La Directive de l'Union européenne sur la conservation de données[1396] est un exemple d'une telle approche.

> ***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 prestataires 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 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 de services de communication concernés, par des prestataires 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.*
>
> ***Article 4 – Accès aux données***
>
> *Les Etats 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 Etat membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables 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 Etats 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:*

[1396] 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.

(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 Etats membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une durée minimale de six mois et d'une durée 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 Etat membre veille à ce que les prestataires 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 autorisée 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 Etats 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 clés concernant toute communication sur l'Internet seront couvertes par cette Directive a suscité beaucoup de critiques de la part d'organisations de droit de l'homme.[1397] Cela pourrait, à son tour, conduire à une révision de la Directive et de sa mise en œuvre par des conseils constitutionnels.[1398] En outre, dans sa conclusion de l'affaire Productores de Música de España (Promusicae) contre Telefónica de España[1399], l'Avocat général Juliane Kokott, conseiller auprès de la Cour européenne de justice, a souligné qu'il

---

1397 See for example: Briefing for the Members of the European Parliament on Data Retention, available at: http://www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf; Regarding the concerns related to a 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.

1398 See: Heise News, 13,000 determined to file suit against data retention legislation, 17.11.2007, available at: http://www.heise.de/english/newsticker/news/99161/from/rss09.

1399 Case C-275/06.

était douteux que l'obligation de conservation de données puisse être mise en œuvre sans violation des droits fondamentaux.[1400] Des difficultés concernant la mise en œuvre de telles règlementations avait déjà été signalées par le G8 en 2001.[1401]

Mais la critique n'est pas limitée à ce seul aspect. Une autre raison pour laquelle la conservation de données s'est avérée moins efficace dans la lutte contre la cybercriminalité tient au le fait que cette obligation peut être contournée. Les manières les plus faciles de contourner l'obligation de conservation de données incluent:

- l'utilisation de différents terminaux Internet publics ou de services de données de téléphones mobiles prépayés qui n'exigent pas d'inscription, et[1402]
- l'utilisation de services de communications anonymes qui sont (au moins en partie) exploités dans des pays qui ne connaissent pas l'obligation de conservation des données.[1403]

Si les auteurs d'infractions utilisent des terminaux publics différents ou des services prépayés de données par téléphonie mobile pour lesquels ils n'ont pas besoin d'enregistrer les données stockées par les fournisseurs, l'obligation de conservation de données conduira seulement les autorités de police vers les prestataires de services mais pas vers les véritables auteurs d'infractions.[1404]

De plus, les auteurs d'infractions peuvent contourner l'obligation de conservation de données en utilisant des serveurs de communications anonymes.[1405] Dans ce cas, les autorités de police peuvent être à même de prouver le fait que l'auteur a utilisé un serveur de communications anonyme mais à cause du manque d'accès aux données relatives au pays où est installé le serveur de communications anonymes, elles ne pourront pas prouver la participation de l'auteur à la commission d'une infraction pénale.[1406]

En ce qui concerne le fait qu'il est très facile de contourner cette disposition, la mise en place de la législation relative à la conservation de données dans l'Union européenne est couplée à la crainte que ce processus exige des mesures annexes pour assurer l'efficacité de cet instrument. Les éventuelles mesures additionnelles pourraient inclure l'obligation de s'enregistrer avant l'utilisation de services en ligne[1407] ou l'interdiction de l'utilisation de technologies de communication anonymes.[1408]

1400 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 does usually but not invariably follow the advisors conclusion.

1401 In a G8 Meeting in Tokyo experts discussed the advantaged 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.

1402 Regarding the challenges for law enforcement agencies related to the use of means of anonymous communication see above: Chapter 3.2.12.

1403 Regarding the technical discussion about traceability and anonymity see: CERT Research 2006 Annual Report, page 7 et seq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

1404 An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1405 See: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention sur la cybercriminalité, LOLAE Law Review, 2002, page 91 –available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

1406 Regarding the impact of use of anonymous communication technology on the work of law enforcement agencies see above: Chapter 3.2.12.

1407 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1408 Regarding the protection of the use of anonymous mean of communication by the United States constitution *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention sur la cybercriminalité, LOLAE Law Review, 2002, page 82 – available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

6.2.6 Perquisition et saisie

Bien que de nouveaux instruments d'enquête, comme la collecte en temps réel de données relatives au contenu et l'utilisation de logiciels de télé-expertise légale en informatique pour identifier les auteurs d'infractions soient actuellement à l'étude ou déjà mis en œuvre dans certains pays, la perquisition et la saisie demeurent l'un des plus important instrument d'enquête.[1409] Dès que l'auteur d'une infraction est identifié et que les autorités de police saisissent son équipement TI, les experts en investigation numérique légale peuvent analyser les matériels et collecter les preuves nécessaires pour engager les poursuites.[1410]

La possibilité de remplacer ou de modifier la procédure de perquisition et saisie fait actuellement l'objet de discussions dans certains pays européens et aux Etats-Unis[1411] On pourrait éviter la nécessité de pénétrer chez un suspect pour perquisitionner et saisir du matériel informatique en procédant à des recherches en ligne. L'instrument, qui sera présenté avec davantage de détails dans les sections qui suivent, décrit une procédure par laquelle les autorités de police ont accès à l'ordinateur du suspect via l'Internet pour effectuer des recherches secrètes.[1412] Bien que les autorités de police pourraient évidemment profiter du fait que le suspect ne réalise pas que l'enquête est exécutée, l'accès physique à du matériel permet d'avoir recours à des techniques d'enquête plus efficaces.[1413] Cela souligne le rôle important des procédures de perquisition et saisie dans le cadre des enquêtes sur Internet.

Convention sur la cybercriminalité

La plupart des lois procédurales criminelles nationales contiennent des dispositions qui permettent aux autorités de police de perquisitionner et de saisir des objets.[1414] La raison pour laquelle les rédacteurs de la Convention sur la cybercriminalité ont néanmoins inclus une disposition relative à la perquisition et à la saisie est le fait que, souvent, les législations nationales ne couvrent pas les procédures de perquisition et de saisie liées aux données.[1415] Ainsi, certains pays limitent l'application des procédures de saisie à la saisie d'objets physiques.[1416] S'appuyant sur de telles dispositions, les enquêteurs peuvent saisir un serveur entier mais ne peuvent pas saisir uniquement les données pertinentes en les copiant sur le serveur. Cela peut susciter des difficultés lorsque les

---

1409 A detailed overview about 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 seqq.; *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 seqq. 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: http://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.

1410 Regarding the involvement of computer forensic experts in the investigations see above: Chapter 6.2.2.

1411 Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: http://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: http://www.news.com/8301-10784_3-9769886-7.html.

1412 See below: Chapter 6.2.12.

1413 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 it is the only way to ensure that the files on the suspects 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: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

1414 See Explanatory Report to the Convention sur la cybercriminalité, No. 184.

1415 "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 sur la cybercriminalité, 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.

1416 Explanatory Report No. 184.

informations pertinentes sont stockées sur un serveur avec les données de centaines d'autres utilisateurs et qui ne seraient plus disponibles après que les autorités de police aient saisi ce serveur. Un autre exemple de l'insuffisance des procédures classiques de perquisition et de saisie de biens tangibles est le cas où les autorités de police ne connaissent pas l'emplacement physique du serveur mais peuvent y accéder via Internet.[1417]

L'Art. 19, sous-paragraphe 1 de la Convention sur la cybercriminalité vise à établir un instrument qui permette la perquisition de systèmes informatiques qui soient aussi efficaces que les procédures classiques de perquisition.[1418]

> ***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.*

Bien que la procédure de perquisition et saisie soit un instrument qui est fréquemment utilisé par les enquêteurs, de nombreuses difficultés accompagnent son application dans le cadre des enquêtes de cybercriminalité.[1419] L'une des principales difficultés est que les ordres de perquisition sont souvent limités à certains lieux (par exemple, le domicile du suspect).[1420] En ce qui concerne la perquisition de données informatiques, il peut apparaître, pendant l'enquête, que le suspect n'a pas stocké ces données sur les disques durs locaux mais sur un serveur extérieur auquel il accède via Internet.[1421] L'utilisation de serveurs Internet pour le stockage et le traitement de données est une pratique de plus en plus répandue chez les utilisateurs d'Internet ("informatique en nuages"). L'un des avantages du stockage d'informations sur un serveur Internet est que l'on peut y accéder à partir de n'importe quel endroit avec une connexion Internet. Pour veiller à ce que les enquêtes soient exécutées de manière efficace, il est important de maintenir une certaine souplesse dans leur exécution. Si les enquêteurs découvrent que des informations intéressantes sont stockées sur un autre système informatique, ils doivent pouvoir étendre leurs recherches à ce système.[1422] La Convention sur la cybercriminalité traite de cette question dans son Art. 19 sous-paragraphe 2.

1417 Regarding the difficulties of online-search procedures see below: Chapter 6.2.12.

1418 "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 sur la cybercriminalité, No. 187.

1419 *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1420 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

1421 The importance of being able to extend the search to connected computer systems was already addressed by the Council of Europe Recommendation No. R (95) 13 of he 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: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

1422 In this context it is important to keep in mind the principle of National Sovereignty. If the information are stored on a computer system outside the territory an extension of the search order could violate this principle. The drafters of the Convention sur la cybercriminalité 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 sur la cybercriminalité, No. 193. With regard to this issue see as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

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.

Une autre difficulté est liée à la saisie des données informatiques. Si les enquêteurs parviennent à la conclusion que la saisie du matériel utilisé pour stocker les informations est inutile ou inadéquate, ils peuvent avoir besoin d'autres instruments leur permettant de poursuivre leurs procédures de perquisition et saisie concernant des données informatiques stockées.[1423] Les instruments nécessaires ne sont pas limités à la copie des données pertinentes.[1424] De plus, il existe un certain nombre de mesures secondaires qui sont nécessaires pour maintenir l'efficacité requise pour la saisie du système informatique proprement dit. L'aspect le plus important est de maintenir l'intégrité des données copiées.[1425] Si les enquêteurs n'ont pas l'autorisation de prendre les mesures nécessaires pour assurer l'intégrité des données copiées, ces dernières peuvent ne pas être acceptées comme preuves dans le cadre de poursuites judiciaires.[1426] Après que les enquêteurs aient copié des données et pris les mesures nécessaires pour maintenir leur intégrité, ils doivent décider de la façon de traiter les données d'origine. Du fait que les enquêteurs ne déplaceront pas le matériel pendant la procédure de saisie, les informations restent en général dans ce matériel. Dans le cadre d'investigations liées à des contenus illégaux[1427] (par exemple pédopornographie) les investigateurs ne pourront pas, notamment, laisser les données dans le serveur. Ils ont donc besoin d'un instrument qui les autorise à retirer les données ou au moins à s'assurer qu'on ne peut plus y accéder.[1428] La Convention sur la cybercriminalité traite des questions évoquées ci-dessus à l'Art. 19, sous-paragraphe 3.

Article 19 – Perquisition et saisie de données informatiques stockées

[…]

1423 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1424 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 seqq.

1425 "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.

1426 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.

1427 See above: Chapter 2.5.

1428 One possibility to prevent access to the information without deleting them is the use encryption technology.

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.

Une autre difficulté concerne les ordres de perquisition de données informatiques; en effet, les autorités de police éprouvent parfois des difficultés à trouver l'emplacement des données. Elles sont fréquemment stockées dans des systèmes informatiques hors du territoire national spécifique. Même lorsque l'on connaît l'emplacement exact, le volume de données stockées empêche souvent de procéder à des enquêtes rapides.[1429] Dans de tels cas, il devient très difficile de mener à bien de telles enquêtes car elles s'inscrivent dans un contexte international et doivent donc s'appuyer sur une coopération à ce niveau.[1430] Même lorsque les enquêtes sont liées à des systèmes informatiques situés à l'intérieur des frontières nationales et que les enquêteurs ont identifié l'hébergeur qui exploite les serveurs où l'auteur de l'infraction a stocké les données pertinentes, ils risquent de se trouver face à des difficultés lorsqu'il s'agit d'identifier l'emplacement exact des données. Il est très vraisemblable que même les petits et moyens hébergeurs possèdent des centaines de serveurs et des milliers de disques durs. Très souvent, les enquêteurs ne pourront identifier l'emplacement exact avec l'aide de l'administrateur du système qui est responsable de l'infrastructure des serveurs.[1431] Même lorsqu'ils peuvent identifier le lecteur de disque spécifique, des mesures de protection risquent de les empêcher de chercher les données en cause. Les rédacteurs de la Convention ont décidé de traiter cette question en mettant en œuvre une mesure de coercition pour faciliter la perquisition et la saisie des données informatiques. L'Art. 19, sous-paragraphe 4, permet aux enquêteurs d'obliger un administrateur de systèmes à aider les autorités de police. Bien que l'obligation de suivre l'ordre de l'enquêteur soit limitée aux informations nécessaires et au soutien relatif à ce cas, cet instrument change la nature des procédures de perquisition et saisie. Dans de nombreux pays, les ordres de perquisition et saisie obligent uniquement les parties visées par l'enquête à tolérer la poursuite, elles n'ont pas à apporter un soutien actif à l'enquête. Lorsque des personnes qui ont des connaissances spéciales qui sont nécessaires aux enquêteurs, la mise en œuvre de la Convention sur la cybercriminalité modifiera la situation de deux façons différentes. En premier lieu, elles devront fournir les informations nécessaires aux enquêteurs. En second lieu, l'obligation de fournir, raisonnablement, un soutien aux enquêteurs dispensera ces

---

1429 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

1430 The fact, that the law enforcement agencies are able to access certain data, that are stored outside the country through a computer system in their territory does not automatically legalise 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 trans-border 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.

1431 "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 computer 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.

personnes de leurs obligations ou ordres contractuels donnés par les superviseurs.[1432] La Convention ne définit pas le terme "raisonnable" mais le Rapport explicatif signale que raisonnable: "*peut inclure la divulgation d'un mot de passe ou d'une autre mesure de sécurité aux autorités chargées de l'enquête*". Mais en général elle ne couvre pas "*la divulgation du mot de passe ou d'une autre mesure de sécurité*" si cela était accompagné d'une "*menace inacceptable à la vie privée d'autres utilisateurs ou au caractère confidentiel d'autres données dont la recherche n'est pas autorisée*".[1433]

> ***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.*

Modèle de Loi du Commonwealth sur l'informatique et les délits liés à l'informatique

On peut trouver des approches similaires dans le modèle de Loi du Commonwealth de 2002.[1434]

> ***Sec. 11.***
>
> *Dans cette 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.*
>
> ***Sec. 12***[1435]
>
> *(1) Lorsqu'un magistrat est satisfait, sur la base de [informations obtenues sous serment] [affidavit] que l'on peut raisonnablement [soupçonner] [croire] qu'il peut se trouver quelque part un objet ou des données informatiques:*
>
> *(a) qui peuvent être une évidence substantielle apportant la preuve d'une infraction; ou*
>
> *(b) qui ont pu être acquises par une personne à la suite d'une infraction;*

1432 "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.

1433 Explanatory Report to the Convention on Cybercrime, No. 202.

1434 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1435 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 dat

le magistrat [peut] [devra] lancer un mandat autorisant un officier [des autorités de police], avec l'assistance qui pourrait s'avérer nécessaire, à pénétrer dans l'endroit pour y faire une perquisition et une saisie de l'objet ou des données informatiques..

Sec. 13[1436]

(1) Une personne qui est en possession ou qui contrôle un support de stockage de données informatiques ou un système informatique qui est l'objet d'une perquisition au titre de la section 12 doit permettre, et assister si nécessaire, la personne chargée de la perquisition:

(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 passible, sur condamnation, d'une peine de prison d'une durée maximale de [période] ou d'une amende maximale de [montant] ou des deux.

6.2.7 Injonction de produire

Même lorsqu'une obligation comme celle qui figure à l'Art. 19, sous-paragraphe 4 de la Convention sur la cybercriminalité, n'est pas mise en œuvre dans une législation nationale, les prestataires de services coopèrent souvent avec les autorités de police pour éviter une influence négative sur leurs entreprises. Si, par suite d'un manque de coopération du prestataire, les enquêteurs ne trouvent pas les données ou les dispositifs de stockage qu'ils doivent perquisitionner et saisir, il est vraisemblable qu'ils devront saisir plus de matériel qu'il est en général nécessaire. Les prestataires de services apporteront donc généralement leur aide aux enquêteurs et fourniront les données pertinentes sur demande des autorités de police. La Convention sur la cybercriminalité contient des instruments qui permettent aux enquêteurs de s'abstenir d'injonction de perquisition si la personne, qui possède les données recherchées, les présente aux enquêteurs.[1437]

Bien que les efforts conjoints des autorités de police et des prestataires de services, même lorsqu'il n'y a pas de base juridique, semblent être un exemple positif de partenariat public/privé, on relève un certain nombre de difficultés liées à une coopération non réglementée. Outre les questions de protection de données, la préoccupation principale concerne le fait que les prestataires de services pourraient violer leurs obligations contractuelles avec leurs clients s'ils répondent à une demande de soumettre certaines données qui ne repose pas sur une base juridique suffisante.[1438]

1436 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 ist constitutional or common law protections against self -incrimination.*

1437 Regarding the motivation of the drafters see Explanatory Report to the Convention on Cybercrime, No. 171

1438 "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.

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 prestataire 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'Art. 18 contient deux obligations. Sur la base de l'Art. 18, sous-paragraphe 1a), quiconque (y compris un prestataire de services) est obligé de soumettre des données informatiques spécifiées qui sont la possession ou sous le contrôle d'une personne. Contrairement au sous-paragraphe 1b), l'application de cette disposition n'est pas limitée à des données spécifiques. Le terme "possession" exige que la personne ait un accès physique au dispositif de stockage de données où sont stockées les informations spécifiées.[1439] L'application de cette disposition est étendue par le terme "contrôle". Des données sont dites sous le contrôle d'une personne lorsque cette dernière n'a pas d'accès physique mais qu'elle gère les informations. C'est le cas, par exemple, lorsque le suspect a stocké des données pertinentes sur un système de stockage en ligne éloigné. Dans le Rapport explicatif, les rédacteurs de la Convention signalent néanmoins que la simple capacité technique à accéder à distance à des données stockées ne constitue pas nécessairement un contrôle.[1440] L'application de l'Art. 18 de la Convention sur la cybercriminalité est donc limitée aux cas où le degré de contrôle du suspect va au-delà de la possibilité potentielle d'accéder à ces données.

Le sous-paragraphe 1b) contient une injonction de produire qui est limitée à certaines données. Sur la base de l'Art. 18, sous-paragraphe 1b), les enquêteurs peuvent ordonner à un prestataire de services de produire les informations relatives aux abonnés. Ces informations peuvent être nécessaires pour identifier l'auteur d'une infraction. Si les enquêteurs peuvent découvrir l'adresse IP qui a été utilisée par l'auteur de l'infraction, ils doivent établir le lien entre cette adresse et une personne.[1441] Dans la plupart des cas, l'adresse IP conduit seulement au prestataire de services Internet qui a fourni l'adresse IP à l'utilisateur. Avant de permettre l'utilisation d'un service, le prestataire de services Internet exige en général de l'utilisateur qu'il s'enregistre avec ses informations d'abonné.[1442] Dans ce contexte, il est important de souligner que l'Art. 18 de la Convention sur la cybercriminalité ne met en œuvre ni une obligation de conservation de données[1443] ni une obligation pour les prestataires de services d'enregistrer les informations relatives aux abonnés.[1444] L'Art. 18, sous-paragraphe 1b) permet aux enquêteurs d'ordonner au prestataire de services de produire ses informations relatives aux abonnés.

A première vue, la différence entre "données informatique", au sous-paragraphe 1a) et "informations relatives aux abonnés", au sous-paragraphe 1b) ne semble pas nécessaire puisque les informations relatives aux abonnés qui sont stockées sous forme numérique sont également couvertes par le sous-paragraphe 1a). La première raison de cette différenciation est liée aux définitions différentes de "données informatiques" et "informations relatives aux abonnés". Contrairement à l'expression "données informatiques", l'expression "informations

---

1439 Explanatory Report to the Convention on Cybercrime, No. 173.

1440 "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.

1441 Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication see above: Chapter 3.2.12.

1442 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.

1443 See above: Chapter 6.2.5.

1444 Explanatory Report to the Convention on Cybercrime, No. 172.

relatives aux abonnés" n'exige pas que ces informations soient stockées en tant que données informatiques. L'Art. 18, sous-paragraphe 1b), de la Convention sur la cybercriminalité permet aux autorités législatives compétentes de produire des informations qui sont conservées dans un format non numérique.[1445]

> ***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 prestataire 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 de la distinction entre "données informatiques" et "informations relatives aux abonnés" est le fait qu'elle permet aux législateurs de mettre en œuvre différentes exigences en ce qui concerne l'application des instruments.[1446] Il est possible, par exemple, de mettre en œuvre des exigences plus strictes[1447] pour une injonction de produire se rapportant au sous-paragraphe 1b) car cet instrument permet aux autorités de police d'accéder à tout type de données informatiques, y compris à des données relatives au contenu.[1448] La différence entre la collecte en temps réel de données relatives au trafic (Art. 20)[1449] et la collecte en temps réel de données relatives au contenu (Art. 21)[1450] montre que les rédacteurs de la Convention ont réalise qu'en fonction de la nature des données en question, les autorités de police ont accès à différentes sauvegardes qui doivent être mises

---

1445 These can for example be information that were provided on a classic registration form and kept by the provider as paper records.

1446 The Explanatory Report does even point 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"

1447 For example the requirement of a court or

1448 The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 20) shows that the drafters of the Convention realised that the instruments are

1449 See below: Chapter 6.2.9.

1450 See below: Chapter 6.2.10.

en œuvre.[1451] Avec la différence entre "données informatiques" et "informations relatives aux abonnés", l'Art. 18 de la Convention sur la cybercriminalité permet aux états signataires de développer un système similaire de sauvegardes graduées en ce qui concerne l'injonction de produire.[1452]

Modèle de Loi du Commonwealth sur l'informatique et les délits liés à l'informatique

On peut trouver des approches similaires dans le modèle de Loi du Commonwealth de 2002.[1453]

> ***Sec. 15***
>
> *Lorsqu'un magistrat est satisfait, sur la base d'une demande faite par l'officier de police, que des données informatiques spécifiées, ou une impression d'autres informations, sont requises raisonnablement aux fins d'une enquête criminelle ou de poursuites criminelles, il peut ordonner:*
>
> *(a) qu'une personne sur le territoire de [Etat prenant les dispositions] qui contrôle un système informatique produit à partir du système des données informatiques spécifiées ou une impression ou une autre forme de sortie intelligible de ces données; et*
>
> *(b) qu'un prestataire de services Internet dans [Etat prenant les dispositions] produit des informations sur des personnes qui sont abonnées ou qui autrement utilisent le service; et*
>
> *(c)[1454] qu'une personne sur le territoire de [Etat prenant les dispositions] qui a accès à un processus de système informatique spécifié et qui compile des données informatiques spécifiées à partir du système et les transmet à une personne spécifiée.*

6.2.8 Collecte en temps réel de données informatiques

Dans de nombreux pays, la surveillance téléphonique est un instrument qui est utilisé dans le cadre d'enquêtes sur des crimes capitaux.[1455] De nombreuses infractions impliquent l'usage du téléphone, en particulier du téléphone mobile, soit au moment de la préparation soit au moment de la commission de l'infraction. En cas de trafic de stupéfiants, en particulier, la surveillance des conversations entre auteurs peut être essentielle pour la réussite de l'enquête. Cet instrument permet aux enquêteurs de collecter des informations précieuses bien que limitées aux informations échangées par les lignes téléphoniques/téléphones surveillés. Si l'auteur utilise d'autres moyens d'échange, par exemple, lettres ou lignes non surveillées, les enquêteurs ne pourront pas

---

1451 Art. 21 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»). Unlike this Art. 20 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.

1452 Regarding the advantages of a graded system of safeguards see above: Chapter 6.2.3.

1453 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1454 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.

1455 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: http://www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

enregistrer les conversations. Généralement, la situation est la même lorsqu'il s'agit de conversations directes sans utilisation de téléphones.[1456]

Aujourd'hui, l'échange de données a remplacé les conversations téléphoniques classiques. L'échange de données ne se limite pas à des courriels ou à des transferts de fichiers. Un volume croissant de communications se fait en ayant recours aux technologies basées sur les protocoles Internet (Voix sur IP).[1457] D'un point de vue technique, un appel téléphonique "Voix sur IP" ressemble beaucoup plus à un échange de courriel qu'à un appel téléphonique classique utilisant le fil et l'interception de ce type d'appel implique des difficultés exceptionnelles.[1458]

Vu que de nombreux délits informatiques impliquent l'échange de données, la capacité à aussi bien intercepter ces processus qu'à utiliser des données liées aux opérations d'échange peut devenir une exigence essentielle pour la réussite des enquêtes. L'application des dispositions de surveillance téléphonique existantes ainsi que des dispositions liées à l'utilisation de données relatives au trafic des communications dans les enquêtes de cybercriminalité s'avère difficile dans certains pays. Les difficultés rencontrées sont liées à des questions techniques[1459] et à des questions juridiques. D'un point de vue juridique, l'autorisation d'enregistrer une conversation téléphonique n'inclut pas nécessairement l'autorisation d'intercepter les processus de transferts de données.

La Convention sur la cybercriminalité vise à combler les lacunes existantes concernant l'aptitude des autorités de police à surveiller les processus de transferts de données.[1460] Dans cette perspective, la Convention sur la cybercriminalité fait la distinction entre deux sous-ensembles de surveillance de transferts de données. L'Art. 20 autorise les enquêteurs à collecter des données relatives au trafic. L'expression "données relatives au trafic" est définie à l'Art. 1d) de la Convention sur la cybercriminalité.

> ***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 utilisée dans la plupart des législations nationales dans ce domaine.[1461]

1456 In these cases other technical solutions for the 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 seqq.

1457 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 http://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.

1458 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: http://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 http://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.

1459 Especially the missing technical preparation of Internet Providers to collect the relevant data in real-time.

1460 Explanatory Report to the Convention on Cybercrime, No. 205.

1461 ABA International Guide to Combating Cybercrime, page 125.

6.2.9 Collecte de données relatives au trafic

Convention sur la cybercriminalité

Eu égard au fait que la définition de "données relatives au trafic" varie d'un pays à l'autre[1462], les rédacteurs de la Convention sur la cybercriminalité ont décidé de définir cette expression de façon à améliorer l'application de la disposition correspondante dans le cadre d'enquêtes internationales. L'expression "données relatives au trafic" désigne des données qui sont produites par des ordinateurs pendant les opérations d'acheminement d'une communication de son origine à sa destination. Chaque fois qu'un utilisateur se connecte à l'Internet, télécharge des courriels ou ouvre un site Internet, des données relatives au trafic sont produites. En ce qui concerne les enquêtes de cybercriminalité, les données relatives au trafic et liées aux origines et aux destinations les plus pertinentes sont les adresses IP qui identifient le correspondant d'une communication dans le cas d'une communication sur Internet.[1463]

Contrairement à l'expression "données relatives au contenu", l'expression "données relatives au trafic" couvre uniquement les données produites pendant un transfert de données mais ne couvre pas les données transférées proprement dites. Bien que l'accès aux données relatives au contenu puisse être nécessaire dans certains cas, car elle permet aux autorités de police d'analyser la communication d'une manière beaucoup plus efficace, les données relatives au trafic jouent un rôle important dans les enquêtes de cybercriminalité.[1464] Alors que l'accès aux données relatives au contenu permet aux autorités de police d'analyser la nature des messages des fichiers échangés, les données relatives au trafic peuvent être nécessaires pour identifier un auteur d'infraction. Dans les cas de pédopornographie, les données relatives au trafic permettent, par exemple, aux enquêteurs d'identifier une page du web où l'auteur de l'infraction télécharge des images de pédopornographie. En surveillant les données relatives au trafic produites pendant l'utilisation de services Internet, les autorités de police peuvent identifier l'adresse IP du serveur et peuvent alors essayer de déterminer son emplacement 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 prestataire 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*

1462 ABA International Guide to Combating Cybercrime, page 125.

1463 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.

1464 "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 as well: ABA International Guide to Combating Cybercrime, page 125; Gercke, Preservation of User Data, DUD 2002, 577 et seq.

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 prestataire 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'Art. 20 contient deux approches différentes concernant la collecte de données relatives au trafic, toutes deux étant supposées être mises en œuvre.[1465]

- La première consiste à mettre en œuvre une obligation pour les prestataires de services Internet de permettre aux autorités de police de collecter directement les données pertinentes. Cela nécessite en générale l'installation d'une interface que les autorités de police peuvent utiliser pour accéder aux infrastructures des prestataires de services Internet.[1466]
- La seconde approche consiste à permettre aux autorités de police d'obliger les prestataires de services Internet à collecter des données à la demande de ces autorités. Cette disposition permet aux enquêteurs d'utiliser les capacités techniques existantes et les connaissances dont disposent généralement les prestataires. L'une des intentions sous-jacente de cette combinaison des deux approches est de s'assurer que si les fournisseurs des services n'ont pas les technologies en place pour enregistrer les données, les autorités de police doivent être en mesure d'effectuer les enquêtes (sur la base de l'Art. 20, sous-paragraphe 1b)) sans l'aide des fournisseurs.[1467]

La Convention sur la cybercriminalité n'a pas été rédigée avec une préférence pour une technologie spécifique et n'a pas non plus l'intention d'élaborer des normes pour accompagner le besoin d'investissements financiers élevés pour l'industrie concernée.[1468] Dans cette perspective, l'Art. 20, sous-paragraphe 1a), de la Convention sur la cybercriminalité apparaît comme la meilleure solution. Toutefois, la recommandation figurant dans l'Art. 20, sous-paragraphe 2, montre que les rédacteurs de la Convention étaient conscients du fait que certains pays risqueraient d'avoir des difficultés à mettre en œuvre une législation qui permettrait aux autorités de police d'effectuer directement leurs enquêtes.

L'une des grandes difficultés des enquêtes, basées sur l'Art. 20, est l'utilisation de moyens de communication anonymes. Comme cela a déjà été expliqué[1469], les auteurs d'infractions peuvent utiliser des services sur Internet qui permettent des communications anonymes. Si l'auteur d'une infraction utilise un service de communication anonyme comme le logiciel TOR[1470], les enquêteurs ne sont pas, dans la plupart des cas, en mesure d'analyser comme il convient les données relatives au trafic et d'identifier les correspondants de la

---

1465 "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.

1466 The Convention does not define technical standards regarding the design of such interface. Explanatory Report to the Convention on Cybercrime, No. 220.

1467 Explanatory Report to the Convention on Cybercrime, No. 223.

1468 "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.

1469 See above: Chapter 3.2.12.

1470 Tor is a software that enables users to protect against traffic analysis. For more information about the software see http://tor.eff.org/.

communication. L'auteur de l'infraction peut atteindre un résultat similaire en utilisant des terminaux Internet publics.[1471]

Par rapport aux procédures classiques de perquisition et saisie, l'un des avantages de la collecte de données relatives au trafic est le fait que le suspect d'une infraction ne réalise pas nécessairement qu'une enquête se déroule.[1472] Cela limite ses possibilités de manipuler ou de supprimer des preuves. Pour s'assurer que les auteurs d'infractions ne sont pas informés par le prestataire de services des investigations en cours, l'Art. 20, sous-section 3, aborde cette question et oblige les Etats signataires à mettre en œuvre une législation qui oblige les prestataires de services à s'assurer qu'ils protègent la confidentialité des enquêtes en cours. Pour le prestataire de services, cette obligation est associée à l'avantage qu'il est libéré de l'obligation[1473] d'informer les utilisateurs.[1474]

La Convention sur la cybercriminalité a été conçue pour améliorer et harmoniser les législations en ce qui concerne les questions liées à la cybercriminalité.[1475] A cet égard, il est important de souligner que sur la base du texte figurant dans la Convention à l'Art. 21, cette provision ne s'applique pas uniquement aux infractions liées à la cybercriminalité mais à toute infraction. En ce qui concerne le fait que l'utilisation de communications électroniques peut être pertinente non seulement dans les cas de cybercriminalité, l'application de cette disposition hors des infractions de cybercriminalité peut être utile dans le cadre des enquêtes. Ainsi, cela permettrait aux autorités de police d'utiliser des données relatives au trafic qui sont générées pendant l'échange de courriels entre auteurs d'une infraction dans le cas de la préparation d'une activité criminelle classique. L'Art. 14, sous-paragraphe 3, permet aux Parties de faire une réserve et de limiter l'application de cette disposition à certaines infractions.[1476]

1471 An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this 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
http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1472 This advantage is also relevant for remote forensic investigations. See below: Chapter 6.2.12.

1473 Such obligation might be legal or contractual.

1474 Explanatory Report to the Convention on Cybercrime, No. 226.

1475 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.»

1476 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.

Modèle de Loi du Commonwealth sur l'informatique et les délits liés à l'informatique

On peut trouver des approches similaires dans le modèle de Loi du Commonwealth de 2002.[1477]

> *(1) Si un officier de police est satisfait 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 spécifiée; et*
>
> *(b) autorise et assiste un officier de police spécifié à collecter ou à enregistrer ces données.*
>
> *(2) Si un magistrat est satisfait sur la base de [informations données sous serment] [affidavit] qu'il existe des motifs valables [de suspecter] que les données relatives au trafic sont demandées raisonnablement 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 spécifiées pendant une période spécifiée par l'application de moyens techniques.*

6.2.10 Interception de données relatives au contenu

Convention sur la cybercriminalité

A part le fait que l'Art. 21 traite des données relatives au contenu, sa structure est similaire à celle de l'Art. 20. La possibilité d'intercepter des échanges de données peut être importante lorsque les autorités de police savent déjà qui sont les correspondants des communications mais qu'elles n'ont pas d'informations sur le type de données échangées. L'Art. 21 leur donne la possibilité d'enregistrer des communications de données et d'analyser leur contenu.[1478] Cela inclut les fichiers téléchargés à partir de sites Internet ou les systèmes de partage de fichiers, les courriels envoyés ou reçus par l'auteur de l'infraction et les conversations en ligne.

> ***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 prestataire 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*

1477 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1478 One possibility to prevent law enforcement agencies to analyse 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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

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 prestataire 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 au cas des données relatives au trafic, la Convention sur la cybercriminalité ne donne pas de définition des données relatives au contenu. Comme elle l'indique, l'expression "données relatives au contenu" se réfère au contenu des communications.

Exemples de données relatives au contenu dans le cadre d'enquêtes de cybercriminalité:

- Objet d'un courriel;
- Contenu d'un site web qui a été ouvert par le suspect;
- Contenu d'une conversation VoIP.

L'une des difficultés les plus importantes que rencontrent les enquêtes effectuées conformément à l'Art. 21 est le recours aux technologies de cryptage.[1479] Comme cela a déjà été expliqué en détail, leur utilisation peut permettre aux auteurs d'infractions de protéger les contenus échangés de telle manière qu'il est impossible pour les autorités de police d'y accéder. Si la victime chiffre le contenu qu'elle transfère, les auteurs d'infractions ne peuvent qu'intercepter les communications chiffrées mais ne peuvent pas analyser leur contenu. Sans avoir accès à la clé de chiffrement des fichiers utilisée, le déchiffrement risque de prendre beaucoup de temps.[1480]

Modèle de Loi du Commonwealth sur l'informatique et les délits liés à l'informatique

On peut trouver des approches similaires dans le modèle de Loi du Commonwealth de 2002.[1481]

Interception de communications électroniques

18. (1) Si un [magistrat] [juge] est satisfait, sur la base des informations [obtenues sous serment] [affidavit] qu'il existe des motifs valables [pour suspecter] [pour penser] que le contenu de communications électroniques est requis raisonnablement aux fins d'une enquête criminelle, le magistrat [peut] [devra]:

(a) ordonner à un prestataire de services Internet dont les services sont disponibles dans [Etat prenant les dispositions] par l'utilisation de moyens techniques de collecter ou enregistrer ou autoriser ou assister les autorités compétentes à 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.

1479 Regarding the impact of encryption technology on computer forensic and criminal investigations see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge see below: Chapter 6.2.11.

1480 *Schneier*, Applied Cryptography, Page 185.

1481 "Model Law on Computer and Computer Related Crime», LMM(02)17; The Model Law is available at: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

6.2.11 Réglementation concernant les technologies de chiffrement

Comme il est expliqué ci-dessus, les auteurs d'infractions peuvent également gêner l'analyse des données relatives au contenu en utilisant des technologies de chiffrement. Il existe divers produits logiciels qui permettent aux utilisateurs de protéger efficacement les fichiers ainsi que les processus de transfert de données contre des accès non autorisés.[1482] Si les suspects ont utilisé un tel produit et que les autorités chargées des enquêtes n'ont pas accès à la clé de chiffrement des fichiers utilisée, le déchiffrement demandé peut prendre beaucoup de temps.[1483]

L'utilisation de technologies de chiffrement par les auteurs d'infractions est un défi pour les autorités de police.[1484] Il existe diverses approches nationales et internationales[1485] pour résoudre ce problème.[1486] Du fait des différentes estimations de la menace posée par les technologies de chiffrement, il n'existe, jusqu'à présent, aucune approche internationale largement acceptée pour traiter de ce sujet. Les solutions les plus courantes sont les suivantes:

- Dans les enquêtes criminelles, les autorités de police doivent avoir reçu l'autorisation de briser le chiffrement si nécessaire.[1487] Sans ces autorisations ou sans avoir la possibilité de lancer une injonction de produire, les autorités chargées des enquêtes ne seront pas en mesure de collecter les preuves nécessaires. En outre, ou en tant qu'option, les enquêteurs peuvent être autorisés à utiliser des logiciels enregistreurs de frappes pour intercepter un mot de passe d'un fichier chiffré afin de briser le chiffrement.[1488]
- Réglementation limitant les performances des logiciels de chiffrement en limitant la longueur des clés.[1489] Selon l'importance de cette limitation, cela permettrait aux enquêteurs de briser la clé dans un délai raisonnable. Ceux qui s'opposent à une telle solution craignent que les limitations permettent non seulement aux enquêteurs de briser un chiffrement mais aussi à des espions économiques d'essayer d'accéder à des informations commerciales chiffrées.[1490] De plus, cette restriction empêcherait simplement l'auteur de l'infraction d'utiliser un chiffrement plus puissant si de tels outils logiciels

---

1482 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1483 *Schneier*, Applied Cryptography, Page 185.

1484 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:

1485 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. "

1486 For more information see Koops, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

1487 The need for such authorisation if for example mentioned 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.»

1488 This topic was discussed in the decision of the United States 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 the law enforcement agencies to make use of a software to record the key strokes on the suspects computer (key logger) 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 http://www.epic.org/crypto/scarfo/opinion.html.

1489 Export limitations for encryption software that is able process 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.

1490 The limitation of the import of such powerful software is even characterised 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: http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

n'étaient pas disponibles. En premier lieu, cela nécessiterait l'existence de normes internationales pour empêcher les producteurs d'outils de chiffrements puissants d'offrir leurs logiciels aux pays qui n'ont pas de restrictions à proprement parler concernant la longueur des clés. Dans tous les cas, les auteurs d'infractions pourraient développer, relativement facilement, leurs propres logiciels de chiffrement qui ne limiteraient pas la longueur des clés.

- L'obligation d'établir un système de mise en dépôt de clés ou une procédure de récupération de clés pour des produits de chiffrement puissants.[1491] Avec de telles règlementations, les utilisateurs continueraient à utiliser des technologies de chiffrement puissantes et les enquêteurs pourraient accéder aux données pertinentes en forçant les utilisateurs à soumettre les clés aux autorités spéciales qui détiennent les clés et qui les fournissent aux enquêteurs, si nécessaires.[1492] Ceux qui s'opposent à une telle solution craignent que les auteurs d'infractions aient accès aux clés ainsi présentées et aux informations secrètes pour le décryptage. En outre, ces auteurs pourraient relativement facilement contourner la réglementation en développant leurs propres logiciels de chiffrement qui ne nécessiteraient pas la remise des clés aux autorités.
- L'injonction de produire est une autre approche.[1493] Cette expression désigne l'obligation de divulguer une clé utilisée pour chiffrer des données. La mise en œuvre d'un tel instrument a été examinée lors de la réunion du G8 à Denver en 1997.[1494] Un certain nombre de pays ont mis en œuvre ces obligations[1495]. En Inde, la Sec. 69 de la Loi sur les technologies de l'information de 2000 est un

---

1491 See: *Lewis*, Encryption Again, available at: http://www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

1492 The key escrow system was promoted by the United States Government and implemented in France for a period of 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.

1493 See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 et seq.

1494 "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.", http://www.g7.utoronto.ca/summit/1997denver/formin.htm.

1495 See for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: http://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, Artikel 37, available at: http://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: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: http://www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: http://www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: http://www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative a l'echange electronique de donnees 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 http://www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: http://www.info.gov.za/gazette/acts/2002/a70-02.pdf;Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: http://www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

exemple de mise en œuvre nationale.[1496] La Sec. 49 de la Loi de 2000 sur la réglementation des pouvoirs d'enquête au Royaume-Uni est un exemple d'une telle obligation[1497]:

Sec. 49.

(1) Cette section s'applique lorsqu'aucune information protégée

(a) est devenue la propriété 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 faire;

(b) est devenue la propriété de quiconque au moyen de l'exercice d'un pouvoir conféré par la loi d'intercepter des communications, ou est susceptible de le faire;

(c) est devenue la propriété 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 en tant que résultat d'une notification adressée au titre de la Sec. 22 (4), ou est susceptible de le faire;

(d) est devenue la propriété 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 faire; ou

(e) est devenue la propriété par tout moyen légitime n'impliquant pas l'exercice de pouvoirs conférés par la loi, de tous services d'information, de la police, ou des douanes, ou est susceptible d'entrer en possession d'un quelconque de ces services, de la police ou des douanes.

(2) Si quiconque ayant l'autorisation appropriée au titre du "schedule 2" estime 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 sécuriser l'exercice effectif 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, la personne ayant cette autorisation peut, en notifiant celle qu'elle croit posséder la clé, impose une exigence de divulgation concernant les informations protégées.

(3) une exigence de divulgation concernant les informations protégées si nécessaire pour des motifs conformes à cette sous-section si cela est nécessaire-

---

1496 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.

1497 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: http://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.

(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 comme quoi 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 permettre une période de mise en conformité raisonnable dans toutes les circonstances.

Pour s'assurer que la personne obligée de divulguer la clé respecte l'injonction et remet réellement la clé, la Loi de 2000 sur les pouvoirs d'enquête du Royaume-Uni contient une disposition qui criminalise le fait de ne pas se conformer à l'injonction.

Sec. 53.

(1) Quiconque ayant reçu une notification au titre de la Sec. 49 a été jugé coupable d'une infraction si, en toute connaissance de cause, conformément à ladite notification, ne fait 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 qui 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, ce sera un moyen de défense pour cette personne de prouver:

(a) qu'il n'était pas raisonnablement facile pour elle de divulguer la clé requise selon la remise de la notification au titre de la section 49 avant le moment où elle a été requise conformément à cette notification de divulguer la clé; mais

(b) qu'elle a divulgué la clé immédiatement après le moment où cela 'était 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 2006 sur la Réglementation des pouvoirs d'enquête oblige le suspect d'une activité criminelle à coopérer avec les autorités de police. Trois grandes préoccupations sont liées à cette réglementation:

- Une préoccupation générale liée au fait que l'obligation conduit à un conflit potentiel avec les droits fondamentaux d'un suspect par rapport à l'auto-incrimination.[1498] Au lieu de laisser l'enquête aux autorités compétentes, le suspect doit coopérer activement à l'enquête. Dans de nombreux pays, la forte protection contre l'auto-incrimination soulève jusqu'à présent la question de savoir jusqu'où une telle réglementation peut aller pour devenir un modèle de solution pour résoudre les difficultés liées aux technologies du chiffrement.
- Une autre préoccupation est liée au fait que la perte de la clé peut conduire à une enquête criminelle. Bien que la criminalisation exige que l'auteur de l'infraction refuse, en toute connaissance de cause, de divulguer la clé, la perte de cette dernière risque de mettre en cause les personnes utilisant une clé de chiffrement dans une poursuite judiciaire non voulue. Mais surtout, la Sec. 53, sous-paragraphe 2, interfère potentionnellement avec la charge de la preuve.[1499]
- Il existe des solutions techniques qui permettent aux auteurs d'infractions de contourner l'obligation de divulguer la clé utilisée pour chiffrer des données. On citera à titre d'exemple de contournement de l'obligation, l'utilisation par l'auteur de l'infraction d'un logiciel de chiffrement basé sur le principe de "possibilité de déni plausible".[1500]

6.2.12 Téléinvestigation numérique légale

Comme il est expliqué ci-dessus, la recherche de preuves dans l'ordinateur d'un suspect nécessite un accès physique au matériel concerné (système informatique et support de stockage extérieur). Cette procédure s'accompagne en général du besoin d'accéder à l'appartement, à la maison ou au bureau du suspect. Dans ce cas, ce dernier saura qu'une enquête est en cours au moment même où les enquêteurs commencent leur

---

1498 Regarding the discussion about the protection against self-incrimination under the 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, Issue1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: http://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: http://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: http://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: http://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: http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe about self-incrimination, in particular with regard to the European Convention on Human Right (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.

1499 In this context see as well: Walker, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: http://www.bileta.ac.uk/01papers/walker.html.

1500 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.

perquisition.[1501] Ces informations risquent d'entrainer un changement de comportement.[1502] Par exemple, si l'auteur d'une infraction a attaqué des systèmes informatiques en vue de tester ses capacités et de participer ensuite à la préparation d'une plus grande série d'attaques avec des complices, la procédure de perquisition risque d'empêcher les enquêteurs d'identifier les autres suspects car il est très vraisemblable que l'auteur de l'infraction cessera de communiquer avec eux.

Pour éviter la détection d'enquêtes en cours, les autorités de police exigent un instrument qui leur permette d'accéder aux données informatiques stockées sur l'ordinateur du suspect, et qui puisse être utilisé secrètement pour la surveillance des appels téléphoniques.[1503] Un tel instrument devrait permettre aux autorités de police d'accéder à distance à l'ordinateur du suspect et de rechercher des informations. Actuellement, la question de savoir si oui ou non de tels instruments sont nécessaires est au centre d'un débat intensif.[1504] Déjà en 2001, des rapports signalaient qu'aux Etats-Unis le FBI développait un outil d'enregistrement des frappes dans le cas d'enquêtes liées à Internet et appelé la "lanterne magique".[1505] En 2007, des rapports étaient publiés indiquant qu'aux Etats-Unis des autorités de police utilisaient des logiciels pour remonter jusqu'au suspect utilisant des moyens de communication anonymes.[1506] Ces rapports se référaient à des mandats de perquisition lorsque le recours à un outil appelé CIPAV[1507] était demandé.[1508] Après que la Cour fédérale en Allemagne ait décidé que

---

1501 A detailed overview about the elements of search procedures as well as the challenges of carrying them ot 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 seqq.; *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 seqq.

1502 Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an on going investigation based on Art. 20 confidential see above: Chapter 6.2.9.

1503 There are disadvantages related to remote investigations. 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 it is the only way to ensure that the files on the suspects 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: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

1504 Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: http://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: http://www.news.com/8301-10784_3-9769886-7.html.

1505 See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: https://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: http://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: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: http://www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; Abreu, FBI confirms "Magic Lantern» project exists, 2001, available at: http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

1506 See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: http://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: http://www.heise-security.co.uk/news/92950.

1507 Computer and Internet Protocol Address Verifier.

les dispositions de la législation de procédures criminelles existante ne permettaient pas aux enquêteurs d'utiliser à distance des logiciels d'investigation numérique légale afin de perquisitionner secrètement l'ordinateur d'un suspect, un débat s'est instauré sur la nécessité d'amender les législations existantes dans ce domaine.[1509] Durant ce débat, des informations ont été publiées selon lesquelles des autorités chargées d'enquêtes avaient utilisé à distance et illégalement des logiciels d'investigation numérique légale à propos de deux enquêtes.[1510]

Divers concepts de "logiciels de téléinvestigation numérique légale" et en particulier leurs fonctions possibles ont été examinés.[1511] Dans une perspective théorique, ce logiciel pourrait avoir les fonctions suivantes:

- Fonction de perquisition – Cette fonction permettrait aux autorités de police de perquisitionner des contenus illégaux et de collecter des informations sur des fichiers stockés dans un ordinateur.[1512]
- Enregistrement – Les enquêteurs pourraient enregistrer des données qui sont traitées sur le système informatique du suspect sans y être stockées en permanence. Si par exemple, le suspect utilise des services Voice over IP pour communiquer avec d'autres suspects, le contenu des conversations n'est, en général, pas stocké.[1513] Le logiciel de téléinvestigation numérique légale pourrait enregistrer les données traitées pour les conserver à l'intention des enquêteurs.
- Enregistreur de frappes – Si le logiciel de téléinvestigation numérique légale contient un module pour l'enregistrement des frappes, ce module pourrait être utilisé pour enregistrer des mots de passe que le suspect utilise pour chiffrer des fichiers.[1514]
- Identification – Cette fonction pourrait permettre aux enquêteurs de prouver la participation du suspect à une infraction criminelle même s'il a utilisé des services de communication anonymes qui empêchent les enquêteurs d'identifier l'auteur de l'infraction en remontant jusqu'à l'adresse IP utilisée.[1515]

1508 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: http://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: http://www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV fort he first time, Heise Security News, 19.07.2007, available at: http://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: http://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: http://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.

1509 Regarding the discussion in Germany see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: http://www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: http://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: http://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: http://www.spiegel.de/international/germany/0,1518,502955,00.html.

1510 See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: http://www.tagesspiegel.de/politik/;art771,1989104.

1511 For an overview see *Gercke*, Secret Online Search, Computer und Recht 2007, page246 et seq.

1512 The search function was in 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: http://www.edri.org/edrigram/number5.3/online-searches.

1513 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 http://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.

1514 This 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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

- Activation de périphériques – Le logiciel de téléinvestigation pourrait être utilisé pour activer une webcam ou un micro à des fins d'observation de pièces.[1516]

Bien que les fonctions possibles de ce logiciel semblent très utiles pour les enquêteurs, il est important de signaler qu'il existe un certain nombre de difficultés juridiques et techniques liées à l'utilisation d'un tel logiciel. D'un point de vue technique, les aspects suivants doivent être pris en considération:

- Difficultés en ce qui concerne les processus d'installation – Le logiciel doit être installé sur le système informatique du suspect. La propagation de logiciels malveillants prouve qu'il est possible d'installer le logiciel sur l'ordinateur d'un utilisateur d'Internet sans sa permission. Mais la différence principale entre un virus et un logiciel de téléinvestigation numérique légale est le fait que ce dernier doit être installé sur un système informatique spécifique (l'ordinateur du suspect) alors qu'un virus vise à infecter un nombre maximum d'ordinateurs sans qu'il soit nécessaire de se focaliser sur un système informatique spécifique. Il existe un certain nombre de techniques permettant de transmettre ce logiciel sur l'ordinateur du suspect. Par exemple: installation avec accès physique au système informatique; installation du logiciel sur un site Internet en vue de son téléchargement; accès en ligne au système informatique en contournant les mesures de sécurité; et dissimulation du logiciel dans le flux de données généré pendant des activités sur Internet, pour n'en mentionner que quelques-unes[1517] Du fait des mesures de protection telles que les logiciels de détection de virus et les murs pare-feu dont sont équipés la plupart des ordinateurs, toutes les méthodes d'installation à distance comportent des difficultés pour les enquêteurs.[1518]
- Avantage de l'accès physique – Pour conduire certaines analyses (par exemple l'inspection physique de supports de traitement de données), il faut accéder au matériel. De plus, le logiciel de téléinvestigation numérique légale ne permet aux enquêteurs que d'analyser des systèmes informatiques connectés à l'Internet.[1519] En outre, il est difficile de maintenir l'intégrité du système informatique du suspect.[1520] Pour toutes ces raisons, le logiciel de téléinvestigation numérique légale ne peut pas, en général, remplacer l'examen physique du système informatique du suspect.

De plus, un certain nombre d'aspects juridiques doit être pris en considération avant de mettre en œuvre une disposition qui autorise les enquêteurs à installer ce logiciel. Les sauvegardes prévues dans les codes de procédures criminelles ainsi que dans les constitutions de nombreux pays limitent les fonctions potentielles de tels logiciels. Outre les aspects nationaux, l'installation d'un logiciel de téléinvestigation numérique légale risque de violer les principes de souveraineté nationale.[1521] Lorsque le logiciel est installé sur un notebook qui est ensuite sorti du pays, il peut permettre aux enquêteurs de procéder à des enquêtes criminelles dans un pays étranger sans avoir reçu l'autorisation nécessaire des autorités responsables.

1515 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.

1516 Regarding this functions see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 et seq.

1517 Regarding the possible ways for an infection of a computer system by a spyware see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: http://www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

1518 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 a detection of the remote forensic software this could go along with serious risks for the computer security. For more information see *Gercke*, Computer und Recht 2007, page 249.

1519 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 do just have access to the computer system via a remote forensic software.

1520 With regard to the importance of maintaining the 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: https://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1521 National Sovereignity is a fundamental principle in International Law. See Roth, State Sovereignity, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

6.2.13 Demande d'autorisation

Les auteurs d'infractions peuvent agir de façon à compliquer les enquêtes. En plus de l'utilisation de logiciels qui permettent les communications anonymes[1522], l'identification peut être rendue compliquée si le suspect utilise des terminaux Internet publics ou des réseaux sans fil ouverts. Des restrictions sur la production de logiciels qui permettent aux utilisateurs de cacher leur identité et sur la mise à disposition du public de terminaux d'accès à Internet qui n'exigent pas d'identification pourraient permettre aux autorités de police de conduire leurs enquêtes avec davantage d'efficacité. C'est en Italie que l'on trouve un exemple d'approche visant à restreindre l'utilisation des terminaux publics pour commettre des infractions pénales avec l'Art. 7[1523] du Décret 144[1524], qui est devenu loi en 2005 (Legge No 155/2005).[1525] Cette disposition oblige quiconque ayant l'intention de proposer un accès public à l'Internet (par exemple cafés Internet ou universités[1526]) à demander une autorisation. De plus, cette personne est obligée de demander l'identité de ses clients avant de les autoriser à utiliser ces services. En ce qui concerne le fait qu'une personne privée qui configure un point d'accès sans fil n'est en général pas couverte par cette obligation, la surveillance peut être facilement contournée si les auteurs d'infractions utilisent des réseaux privés non protégés pour cacher leur identité.[1527]

On peut se demander si les mesures prises pour améliorer les enquêtes justifient la restriction d'accès à Internet et aux services de communications anonymes. Le libre accès à l'Internet est aujourd'hui reconnu comme un aspect important du droit au libre accès à l'information qui est protégé par les constitutions d'un certain nombre de pays. Il est vraisemblable que la demande d'identité aura des conséquences sur l'utilisation d'Internet car les utilisateurs craindront toujours que leur utilisation d'Internet soit surveillée. Même lorsque les utilisateurs savent que leurs activités sont légales, cette situation peut néanmoins avoir une influence sur leurs interactions et leur utilisation d'Internet.[1528] Parallèlement, les auteurs d'infractions qui veulent empêcher leur identification peuvent facilement contourner la procédure d'identification. Ils peuvent, par exemple, utiliser des cartes de téléphone prépayées achetées à l'étranger et qui n'exigent pas d'identification pour accéder à l'Internet.

6.3 Coopération internationale

6.3.1 Introduction

Un nombre de plus en plus élevé d'infractions liées à la cybercriminalité prend une dimension internationale.[1529] Comme cela a été signalé auparavant, l'une des raisons sous-jacente à ce phénomène est le fait qu'il n'est pas

---

1522 See above: Chapter 3.2.12.

1523 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 licensce by 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.

1524 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1525 For more details see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 et seq.

1526 *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

1527 Regarding the related challenges see: *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime» in Cybercrime & Security, IIA-2, page 6 et seq.

1528 *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: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

1529 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: http://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.

nécessaire que l'auteur de l'infraction soit présent physiquement à l'endroit où un service est proposé.[1530] Généralement, il n'est donc pas nécessaire que les auteurs d'infractions soient présents sur le leu où se trouve la victime. D'une manière générale, les enquêtes en matière de cybercriminalité vont de pair avec le besoin d'une coopération internationale.[1531] L'une des demandes principales formulée par les enquêteurs à propos d'enquêtes transnationales est une réaction immédiate de la part de leurs homologues dans le pays où se trouve l'auteur de l'infraction.[1532] A cet égard, les instruments d'entraide classiques ne répondent pas, dans la plupart des cas, aux exigences relatives de rapidité des enquêtes sur Internet.[1533] La Convention sur la cybercriminalité traite de l'importance croissante de la coopération internationale dans ses Art. 23 – Art. 35. On trouve également une autre approche dans le Projet de Convention de Stanford.[1534]

6.3.2 Principes généraux relatifs à la coopération internationale

L'Art. 23 de la Convention sur la cybercriminalité définit trois principes généraux relatifs à la coopération internationale en matière d'enquête de cybercriminalité chez les membres.

> ***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.*

En premier lieu, dans le cadre d'enquêtes internationales, les membres sont supposés coopérer dans la plus grande mesure du possible. Cette obligation reflète l'importance de la coopération internationale dans les enquêtes de cybercriminalité. En outre, l'Art. 23 dispose que les principes généraux ne s'appliquent pas uniquement aux enquêtes de cybercriminalité mais à toutes les enquêtes où doivent être recueillies des preuves sous forme électronique. Cela couvre les enquêtes de cybercriminalité ainsi que les enquêtes. Si, dans une affaire de meurtre, le suspect a utilisé un service de courriel à l'étranger, l'Art. 23 est applicable en ce qui concerne les enquêtes nécessaires eu égard aux données stockées par l'hébergeur.[1535] Le troisième principe stipule que les dispositions traitant de coopération internationale ne remplacent pas les dispositions des accords internationaux en ce qui concerne l'assistance juridique réciproque et l'extradition ou les dispositions pertinentes des législations nationales applicables à la coopération internationale. Les rédacteurs de la Convention sur la cybercriminalité ont insisté sur le fait que l'entraide doit en général s'appuyer sur l'application des traités pertinents et arrangements similaires d'entraide. En conséquence, la Convention n'entend pas créer un régime général séparé concernant l'entraide. C'est donc uniquement lorsque les traités, les lois et les arrangements

---

1530 See above: Chapter 3.2.7.

1531 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: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

1532 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

1533 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."

1534 See below: Chapter 6.3.9.

1535 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).

existants ne contiennent pas déjà de telles provisions que chaque Partie doit établir une base juridique lui permettant d'assurer son rôle au titre de la coopération internationale telle qu'elle est définie par la Convention.[1536]

6.3.3 Extradition

L'extradition de ressortissants demeure l'un des aspects les plus difficiles de la coopération internationale.[1537] Les demandes d'extradition conduisent très souvent à des conflits entre la nécessité de protéger le citoyen et celle de contribuer aux enquêtes en cours dans un pays étranger. L'Art. 24 définit les principes de l'extradition. Contrairement à l'Art. 23, cette disposition est limitée aux infractions mentionnées dans la Convention et ne s'appliquent pas aux cas mineurs (privation de liberté pour une période d'une durée maximale d'au moins un an[1538]). Pour éviter de tels conflits qui pourraient survenir eu égard à la possibilité des Parties de faire des réserves, l'Art. 24 est basé sur le principe de la double incrimination.[1539]

> ***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 passibles dans la législation des deux Parties concernées par une peine privative de liberté pour une période d'une durée 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.*

1536 If for example two countries involved in a cybercrime investigation already do have bilateral agreements in place that contain the relevant instruments, this agreement will remain a valid basis for the international cooperation.

1537 Regarding the difficulties related to the dual criminality principle see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 et seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

1538 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.

1539 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 seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

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.

6.3.4 Principes généraux relatifs à l'entraide

En ce qui concerne l'entraide, l'Art. 25 complète les principes de l'Art. 23. L'une des règlementations les plus importantes figurant à l'Art. 25 est le paragraphe 3 qui souligne l'importance de la rapidité des communications pour les enquêtes de cybercriminalité.[1540] Comme cela a été signalé précédemment, un certain nombre d'enquêtes de cybercriminalité effectué au niveau national échoue car elles sont trop longues et les données importantes sont donc effacées avant que l'on ait pu prendre des mesures procédurales pour les conserver.[1541] Les enquêtes qui nécessitent une entraide juridique demandent généralement encore plus de temps du fait des exigences formelles chronophages de la communication des autorités de police. La Convention traite ce problème en insistant sur l'importance de pouvoir autoriser l'utilisation de moyens rapides de communication.[1542]

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 Etat requis l'exige. 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

---

1540 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."

1541 See above: Chapter 3.2.10.

1542 See Explanatory Report to the Convention on Cybercrime, No. 256.

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.

Lors d'enquêtes de cybercriminalité effectuées au niveau national, on peut découvrir des liens avec des infractions se rapportant à un autre pays. Si les autorités de police se livrent par exemple à des enquêtes de pédopornographie, elles peuvent trouver des informations sur des pédophiles d'autres pays qui ont participé à l'échange de matériels pédopornographiques.[1543] L'Art. 26 expose les réglementations nécessaires aux autorités de police pour qu'elles informent leurs homologues étrangers sans mettre en danger leurs propres enquêtes.[1544]

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.

L'une des règlementations les plus importantes de l'Art. 26 est liée la confidentialité des informations. Concernant le fait que certaines enquêtes ne peuvent être exécutées avec succès que si l'auteur de l'infraction n'est pas au courant des enquêtes qui se déroulent, l'Art. 26 permet à la Partie qui transmet des informations de demander la confidentialité concernant ces dernières. Si cette confidentialité ne peut être garantie, la Partie qui fournit les informations peut refuser de le faire.

6.3.5 Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Tout comme l'Art. 25, l'Art. 27 repose sur l'idée que l'entraide juridique devrait être assurée par l'application des traités et arrangements similaires pertinents au lieu de se référer uniquement à la Convention. Les rédacteurs de la Convention ont décidé de ne pas établir un régime séparé d'entraide obligatoire dans la Convention.[1545] Si d'autres instruments sont déjà en place, les Art. 27 et 28 ne sont pas pertinents dans le cadre d'une demande concrète. Ce n'est que lorsque d'autres règlementations ne sont pas applicables que les Art. 27 et 28 proposent un ensemble de mécanismes qui peuvent être utilisés pour répondre aux demandes d'entraide.

1543 This information often leads to successful international investigations. For an overview about 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: http://www.ecpat.se/upl/files/279.pdf.

1544 Similar instruments can be found in other Council of Europe Convention. 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. The Council of Europe Conventions are available at: http://www.coe.int.

1545 See Explanatory Report to the Convention on Cybercrime, No. 262.

Les aspects les plus importants réglementés par l'Art. 27 sont notamment les suivants:

- obligation de désigner un point de contact pour répondre aux demandes d'entraide juridique[1546];
- exigence de communication directe entre les points de contact pour éviter de longues procédures[1547]; et,
- création d'une base de données par le Secrétaire général du Conseil de l'Europe avec tous les points de contact.

En outre, l'Art. 27 définit les limites en ce qui concerne les demandes d'entraide. Les Parties à la Convention peuvent notamment refuser la coopération:

- en ce qui concerne les infractions politiques; et/ou,
- si l'on considère que la coopération pourrait être préjudiciable à sa souveraineté, sa sécurité, l'ordre public ou autres intérêts essentiels.

Les rédacteurs de la Convention ont vu la nécessité de permettre aux Parties de refuser de coopérer dans certains cas, d'une part, mais, d'autre part, ont fait remarquer que les Parties devraient accepter le refus de coopération avec retenue pour éviter tout conflit avec les principes exposés précédemment.[1548] Il est donc particulièrement important de définir avec précision l'expression "autres intérêts essentiels". Le Rapport explicatif de la Convention sur la cybercriminalité signale que cela pourra être le cas lorsque la coopération conduit à des difficultés fondamentales pour la Partie requise.[1549] Dans la perspective des rédacteurs, les préoccupations liées à des législations inadéquates en matière de protection des données ne présentent pas un intérêt majeur.[1550]

6.3.6 Entraide en matière de mesures provisoires

Les Art. 28 – 33 sont un reflet des instruments de procédure de la Convention sur la cybercriminalité.[1551] La Convention sur la cybercriminalité contient un certain nombre d'instruments procéduraux conçus pour améliorer les enquêtes chez les Etats membres.[1552] En ce qui concerne le principe de souveraineté nationale[1553], ces instruments ne peuvent être utilisés que pour des enquêtes au niveau national.[1554] Si les enquêteurs réalisent que les preuves doivent être collectées à l'extérieur de leur territoire, ils doivent faire appel à l'entraide. En plus de l'Art. 18, chacun des instruments définis aux Art. 15- 21 a une disposition correspondante dans les Art. 28 -33

1546 Regarding the 24/7 network points of contact see below: Chapter 6.3.8.

1547 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.»

1548 See Explanatory Report to the Convention on Cybercrime, No. 268.

1549 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.»

1550 See Explanatory Report to the Convention on Cybercrime, No. 269.

1551 See above: Chapter 6.2.

1552 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).

1553 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

1554 An exemption is Art. 32 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).

qui permet aux autorités de police d'appliquer les instruments procéduraux sur demande d'une autorité de police étrangère.

Instrument procédural	Disposition correspondante du ML
Article 16 – Conservation rapide de données informatiques stockées[1555]	Article 29
Article 17 – Conservation et divulgation rapides de données relatives au trafic[1556]	Article 30
Article 18 – Injonction de produire[1557]	
Article 19 – Perquisitions et saisies de données informatiques stockées[1558]	Article 31
Article 20 – Collecte en temps réel de données relatives au trafic[1559][9]	Article 33
Article 21 – Interception de données relatives au contenu[1560]	Article 34

6.3.7 Accès transfrontalier à des données stockées

Outre le simple reflet des dispositions procédurales, les rédacteurs de la Convention se sont interrogés pour savoir dans quelles circonstances les autorités de police sont autorisées à accéder à des données informatiques qui ne sont ni stockées sur leur territoire ni sous le contrôle d'une personne se trouvant sur leur territoire. Ils n'ont pu se mettre d'accord que sur deux cas de scénarios où une enquête devrait être exécutée par une autorité de police sans avoir à formuler une demande d'entraide.[1561] D'autres accords n'étaient pas possibles[1562] et même la solution trouvée reste critiquée par des Etats membres du Conseil de l'Europe.[1563]

Les deux cas pour lesquels les autorités de police sont autorisées à accéder à des données stockées hors de leur territoire concernent:

- des informations accessibles au public; et/ou
- l'accès avec le consentement d'une personne légalement autorisée.

> ***Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public***
>
> *A 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*

1555 See above: Chapter 6.2.4

1556 See above: Chapter 6.2.4.

1557 See above: Chapter 6.2.7.

1558 See above: Chapter 6.2.6.

1559 See above: Chapter 6.2.9.

1560 See above: Chapter 6.2.410.

1561 See Explanatory Report to the Convention on Cybercrime, No. 293.

1562 "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.

1563 See below in this chapter.

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.

D'autres situations ne sont pas couvertes par l'Art. 32 mais elles ne sont pas non plus exclues.[1564]

L'Art. 32 dispose que si les données pertinentes sont accessibles au public, les autorités de police étrangères sont autorisées à accéder à ces informations. On citera, comme exemple d'informations accessibles au public celles que l'on trouve sur des sites Internet sans contrôle d'accès (comme des mots de passe). Si les enquêteurs, contrairement à tout autre utilisateur, ne sont pas autorisés à accéder à ces sites Internet, cela risque de gêner sérieusement leurs travaux. La première situation traitée par l'Art. 32 est donc largement acceptée.

La seconde situation à propos de laquelle les autorités de police sont autorisées à accéder à des données informatiques stockées hors de leur territoire se présente lorsque les enquêteurs ont obtenu le consentement légitime et volontaire de la personne légalement autorisée à leur divulguer ces données. Cette autorisation fait l'objet de vives critiques.[1565] Il existe de bons arguments contre une telle réglementation. Le plus important est le fait qu'en établissant la seconde exemption, les rédacteurs de la Convention violent la structure dogmatique du régime d'entraide. Avec l'Art. 18, les rédacteurs de la Convention autorisent les enquêteurs à ordonner la production de données. Cet instrument ne peut s'appliquer aux enquêtes internationales car il manque la disposition correspondante du Titre 3 de la Convention. Au lieu d'abandonner la structure dogmatique en autorisant les enquêteurs étrangers à contacter directement la personne qui contrôle les données et à demander la production de ces données, les rédacteurs auraient pu simplement mettre en œuvre une disposition correspondante dans le Titre 3 de la Convention.[1566]

6.3.8 Réseaux de contacts 24/7

Les enquêtes de cybercriminalité exigent souvent une réaction immédiate.[1567] Comme cela a été expliqué auparavant, c'est notamment le cas lorsqu'il s'agit de données relatives au trafic nécessaires à l'identification d'un suspect, car elles sont souvent supprimées dans un délai assez court.[1568] Pour accélérer les enquêtes internationales, la Convention européenne sur la cybercriminalité souligne qu'il est important d'autoriser le recours à des moyens rapides de communication dans son Art. 25. Pour améliorer encore plus l'efficacité des demandes d'entraide, les rédacteurs de la Convention obligent les Parties à désigner un point de contact pour les demandes d'entraide joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept.[1569] Les rédacteurs de la Convention ont insisté sur le fait que la désignation de points de contact est l'un des instruments les plus importants prévus par la Convention sur la cybercriminalité.[1570]

1564 See Explanatory Report to the Convention on Cybercrime, No. 293.

1565 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

1566 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 the foreign law enforcement agency to order the submission of the relevant data. It can only seek for permission.

1567 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."

1568 See above: Chapter 6.2.4.

1569 The availability 24 hours a day and 7 days a week is especially important with regard to 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: Chapter 3.2.6.

1570 See Explanatory Report to the Convention on Cybercrime, No. 298.

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 du réseau 24/7 est partie du modèle de réseau d'information du G8 institué pour lutter contre la criminalité liée à la haute technologie, accessible 24 heures sur 24.[1571] Avec la création d'un réseau de points de contact 24/7, les rédacteurs de la Convention se sont fixés pour objectif de relever les défis de la cybercriminalité, notamment ceux liés à la vitesse des processus d'échange de données[1572] et qui ont une dimension internationale.[1573] Les Parties à la Convention sont obligées de désigner de tels points de contact et de veiller à ce qu'ils soient capables de mener immédiatement certaines actions et de maintenir le service. Comme il est indiqué à l'Art. 35, sous-paragraphe 3, de la Convention sur la cybercriminalité, cela implique de disposer d'un personnel formé et équipé.

En ce qui concerne le processus de désignation des points de contact et en particulier les principes fondamentaux de cette structure, la Convention donne un maximum de souplesse aux Etats membres. La Convention n'exige ni que l'on crée une nouvelle autorité ni que l'on désigne les autorités existantes auxquelles les points de contact doivent être rattachés. Les rédacteurs de la Convention ont également insisté sur le fait que les réseaux 24/7 ont pour objectif de fournir une assistance technique et légale, ce qui conduira à diverses solutions possibles en ce qui concerne leur mise en œuvre.

Pour ce qui est des enquêtes de cybercriminalité, l'installation des points de contact a deux fonctions principales, à savoir:

- l'accélération des communications en fournissant un point de contact unique; et
- l'accélération des enquêtes en autorisant les points de contact à mener certaines enquêtes immédiatement.

La combinaison de ces deux fonctions permet d'accélérer les enquêtes internationales jusqu'au niveau atteint par les enquêtes nationales.

1571 Regarding the activities of the G8 in the fight against Cybercrime see above: Chapter 5.1.1 . For more information on the 24/7 Network see: 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: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

1572 See above: Chapter 3.2.10.

1573 See above: Chapter 3.2.6.

L'Art. 32 de la Convention sur la cybercriminalité définit les aptitudes minimales requises des points de contact. En plus de l'assistance technique et de la fourniture d'informations juridiques, les tâches principales des points de contact incluent:

- la conservation des données;
- la collecte de preuves; et
- la localisation des suspects.

Dans ce contexte, il est important de souligner de nouveau que la Convention ne désigne pas les autorités qui devraient être responsables du fonctionnement des réseaux de points de contact 24/7. Si le point de contact est sous contrôle d'une autorité qui a compétence pour ordonner la conservation des données[1574] et si un point de contact étranger demande cette conservation, la mesure peut être ordonnée immédiatement par le point de contact local. Si le point de contact dépend d'une autorité qui n'a pas compétence à ordonner la conservation des données proprement dites, il est important que ce point de contact puisse contacter immédiatement les autorités compétentes pour veiller à ce que la mesure soit prise immédiatement.[1575]

Lors de la deuxième réunion du Comité de la Convention sur la cybercriminalité, il a été précisé que la participation de points de contact aux réseaux 24/7 n'exige pas la signature ou la ratification de la Convention.[1576]

6.3.9 La coopération internationale dans le Projet de Convention de Stanford

Les rédacteurs du Projet de Convention de Stanford[1577] ont reconnu l'importance de la dimension internationale de la cybercriminalité et des difficultés associées. Pour relever ces défis, ils ont intégré des dispositions spécifiques qui traitent de la coopération internationale. Ces dispositions couvrent les thèmes suivants:

- Article 6 – Entraide juridique
- Article 7 – Extradition
- Article 8 – Poursuites
- Article 9 – Solutions provisoires
- Article 10 – Droits de la personne accusée
- Article 11 – Coopération en matière de répression pénale

Cette approche présente un certain nombre de similitudes avec la Convention sur la cybercriminalité. La principale différence repose dans le fait que les règlementations figurant dans la Convention sur la cybercriminalité sont plus strictes, plus complexes et définies avec davantage de précision que celles figurant dans le Projet de Convention de Stanford. Comme l'ont signalé les rédacteurs du Projet de Convention de Stanford, l'approche de la Convention sur la cybercriminalité est plus pratique et présente donc des avantages en ce qui concerne son application réelle.[1578] Les rédacteurs du Projet de Convention de Stanford ont décidé d'adopter une approche différente car ils prévoyaient que la mise en œuvre de nouvelles technologies pourrait

---

1574 Regarding the question which authorities should be authorised to order the preservation of data see above: Chapter 6.2.4.

1575 Explanatory Report to the Convention on Cybercrime, No. 301.

1576 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

1577 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: http://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.

1578 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

conduire à quelques difficultés. En conséquence, ils n'ont donné que quelques instructions générales sans davantage les préciser.[1579]

6.4 Responsabilité des prestataires de services Internet

6.4.1 Introduction

Commettre un cybercrime implique automatiquement un certain nombre de personnes et d'activités même si l'auteur de l'infraction a agi seul. Du fait de la structure d'Internet, la transmission d'un simple courriel fait intervenir un certain nombre de fournisseurs de services.[1580] Outre le fournisseur du service de messagerie, la transmission fait intervenir des fournisseurs d'accès ainsi que des routeurs qui font suivre le courrier au destinataire. En ce qui concerne le téléchargement de films contenant de la pédopornographie, la situation est similaire. Le processus de téléchargement implique le fournisseur de contenu qui a téléchargé les images (par exemple, sur un site Internet), l'hébergeur qui a fourni le support de stockage pour le site Internet, les routeurs qui ont acheminé les fichiers vers l'utilisateur et enfin le fournisseur d'accès qui a permis à l'utilisateur d'accéder à l'Internet.

Du fait de l'implication de parties multiples, les prestataires de services Internet ont toujours été au centre des enquêtes portant sur des auteurs qui utilisent les services de FAI pour commettre des infractions.[1581] L'une des raisons principales de cette évolution est le fait que même lorsque l'auteur de l'infraction agit à partir de l'étranger, les fournisseurs situés à l'intérieur des frontières nationales constituent une cible appropriée des enquêtes criminelles sans violer le principe de la souveraineté nationale.[1582]

Le fait que les actes de cybercriminalité peuvent, d'une part, ne pas être commis sans la participation de fournisseurs et que, d'autre part, le fait que les fournisseurs n'ont généralement pas les compétences pour empêcher ces crimes, a conduit à la question de savoir si la responsabilité des prestataires de services Internet devaient être limitée.[1583] La réponse à cette question est critique du point de vue du développement économique de l'infrastructure TIC. Les fournisseurs n'exploiteront leurs services que s'ils peuvent éviter la criminalisation dans leur mode régulier de fonctionnement. De plus, les autorités de police ont également un grand intérêt dans cette question. Leur travail dépend souvent de la coopération des prestataires de services Internet. Cela suscite une question car limiter la responsabilité des prestataires de services Internet pour les actes commis par les utilisateurs pourrait avoir des incidences sur la coopération des FAI et leur soutien aux enquêtes de cybercriminalité ainsi que sur la prévention proprement dite des délits.

6.4.2 L'approche des Etats-Unis

Il existe différentes méthodes pour parvenir à un équilibre entre, d'une part, la nécessité d'impliquer activement les prestataires de services dans les enquêtes et, d'autre part, de limiter les risques de la responsabilité criminelle

---

1579 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1580 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.

1581 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: http://www.okjolt.org/pdf/2004okjoltrev8a.pdf.

1582 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

1583 For an introduction into 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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

pour des actions de tiers.[1584] On trouve un exemple d'approche législative dans la loi américaine 17 U.S.C. §§ 517(a) et (b).

> ***§ 512. Limitations de responsabilité se rapportant à du matériel en ligne***
>
> *(a) Communications sur réseaux numériques transitoires*
>
> *Un prestataire de services n'est pas responsable de la réparation pécuniaire, ou, sauf comme il est prévu à 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 fournit 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, acheminement ou connexion, si –*
>
> *(1) la transmission du matériel a été déclenchée par ou sous 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 anticipés 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 comme il est prévu à 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 à 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 partir de la personne décrite au sous-paragraphe (A), si les conditions exposées au paragraphe (2) sont satisfaites.*

1584 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 the DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights.»

Cette disposition repose sur le DMCA (Digital Millennium Copyright Act) qui a été adopté en 1998.[1585] En créant un régime de refuge, le DMCA excluait la responsabilité des fournisseurs de certains services en cas de violation du droit d'auteur à partir de tiers.[1586] Dans ce contexte, il faut tout d'abord souligner que tous les prestataires de services ne sont pas couverts par cette limitation.[1587] La limitation de responsabilité ne s'applique qu'aux fournisseurs de services[1588] et aux fournisseurs de stockages "caching".[1589] De plus, il est important de souligner que la responsabilité est liée à certaines exigences. En ce qui concerne les fournisseurs de services, ces exigences sont les suivantes:

- la transmission du matériel doit être déclenchée par ou sous l'ordre d'une personne autre que le prestataire de services;
- la transmission doit être faite par un processus technique automatique sans sélection du matériel par le prestataire de services;
- le prestataire de services ne doit pas choisir les destinataires du matériel;
- aucune copie du matériel faite par le prestataire de services pendant le stockage intermédiaire ou provisoire ne doit être conservée sur le système ou sur le réseau, qui soit facilement accessible à quiconque autre que les destinataires visés.

Un autre exemple de limitation de responsabilité des prestataires de services Internet figure dans la loi américaine 47 U.S.C. § 230(c) qui est basé sur la Loi Communications Decency[1590]:

> ***§ 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 –*

1585 Regarding the History of the DMCA and the 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: http://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.

1586 Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq., available at: http://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 http://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.

1587 Regarding the application of the 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: http://www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

1588 17 U.S.C. § 512(a)

1589 17 U.S.C. § 512(b)

1590 Regarding the Communication 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 seqq., available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf.

(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, les lois américaines 17 U.S.C. § 517(a) et 47 U.S.C. § 230(c), ont en commun qu'elles se focalisent sur la responsabilité eu égard aux groupes spéciaux de fournisseurs et des domaines particuliers de la loi. La dernière partie de ce chapitre donnera donc une vue générale de l'approche législative adoptée par l'Union européenne qui a adopté un concept plus large.

6.4.3 Directive de l'Union européenne sur le commerce électronique

La Directive de l'Union européenne sur le commerce électronique[1591] est un exemple d'approche législative visant à réglementer la responsabilité des prestataires de services Internet. Confrontés aux difficultés liées à la dimension internationale de l'Internet, les rédacteurs de cette Directive ont décidé d'élaborer des normes juridiques constituant un cadre juridique propice au développement global de la société d'information, au développement économique global ainsi qu'aux travaux des autorités de police.[1592] La réglementation concernant la responsabilité repose sur le principe de la responsabilité graduée.

Cette Directive contient un certain nombre de dispositions qui limitent la responsabilité de certains prestataires.[1593] Ces limitations sont liées aux différentes catégories de services assurés par le prestataire.[1594] Dans tous les autres cas, la responsabilité n'est pas nécessairement exclue et à moins qu'elle soit limitée par d'autres réglementations, le prestataire est totalement responsable. L'objectif de cette Directive de limiter la responsabilité dans les cas où le prestataire n'a que des moyens réduits pour empêcher les infractions. Les raisons de ces possibilités limitées peuvent être de nature technique. Par exemple, les routeurs sont incapables de filtrer les données qui passent par eux sans perte significative de vitesse et sont à peine capables d'empêcher les échanges de données. Les hébergeurs ont les moyens de retirer des données s'ils sont au courant d'activités criminelles. Cependant, tout comme les routeurs, les gros hébergeurs ne peuvent contrôler toutes les données stockées sur leurs serveurs.

En ce qui concerne leur capacité variable à réellement contrôler les activités criminelles, la responsabilité des hébergeurs et des fournisseurs d'accès est différente. A cet égard, il faut prendre en considération le fait que l'équilibre de la Directive repose sur des normes techniques courantes. Actuellement, il n'existe aucun outil capable de détecter automatiquement des images pornographiques inconnues. Si les progrès techniques se poursuivent dans ce domaine, il pourrait s'avérer nécessaire d'évaluer la capacité technique des prestataires et, si nécessaire, d'ajuster le système.

6.4.4 Responsabilité des fournisseurs d'accès (Directive de l'Union européenne)

Les Art. 12 – Art. 15 définissent le degré de limitation de responsabilité des différents prestataires. Selon l'Art. 12, la responsabilité des fournisseurs d'accès et des opérateurs de routeurs est totalement exclue pour autant qu'ils se conforment aux trois conditions exposées à l'Art. 12. En conséquence, le fournisseur d'accès

---

1591 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 U.S. & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol 31, 2003, pae 325 et seqq., available at: http://www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

1592 See Lindholm/Maennel, Computer Law Review International 2000, 65.

1593 Art. 12 – Art. 15 EU E-Commerce Directive.

1594 With the number of different services covered the E-Commerce Directive aims for a broader regulation than 17 U.S.C. § 517(a). Regarding 17 U.S.C. § 517(a) see above.

n'est généralement pas responsable des infractions pénales commises par ses utilisateurs. Cette exclusion totale de responsabilité ne dégage pas les fournisseurs de l'obligation d'empêcher d'autres infractions si un tribunal ou une autorité administrative leur en donne l'ordre.[1595]

Article 12 – Simple transport ("Mere conduit")

1. Les Etats 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

(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 Etats 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 loi américaine 17 U.S.C. § 517(a).[1596] Ces deux règlementations visent à préciser la responsabilité des prestataires de services et elles établissent un lien entre la limitation de responsabilité et les exigences similaires. La différence principale réside dans le fait que l'application de l'Art. 12 de la Directive de l'Union européenne sur le commerce électronique n'est pas limitée aux violations du droit d'auteur mais exclut la responsabilité pour tout autre type d'infraction.

6.4.5 Responsabilités pour le "caching" (Directive de l'Union européenne)

Dans ce contexte, le terme "caching" sert à décrire le stockage de sites web populaires sur des supports de stockage locaux afin de réduire la bande passante et de conférer davantage d'efficacité à l'accès aux données.[1597] L'une des techniques utilisées pour réduire la bande passante consiste à installer des serveurs mandataires.[1598] Dans ce contexte, un serveur mandataire peut servir des demandes sans contacter le serveur spécifié (le nom de domaine entré par l'utilisateur) en saisissant le contenu sauvegardé sur le support de stockage local à partir d'une requête précédente. Les rédacteurs de la Directive ont reconnu l'importance économique du "caching" et ont décidé d'exclure la responsabilité en ce qui concerne le stockage provisoire automatique si le prestataire se conforme aux conditions définies par l'Art. 13. L'une de ces conditions est qu'il se conforme aux normes largement reconnues concernant l'actualisation de l'information.

1595 See Art. 12 paragraph 3 E-Commerce Directive.

1596 The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq., available at: http://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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

1597 With regard to the traditional caching as well as active caching see: Naumenko, Benefits of Active Caching in the WWW, available at: http://lcawww.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

1598 For more information on Proxy Servers see: *Luotonen*, Web Proxy Servers, 1997.

Article 13 – Forme de stockage dite "caching"

1. Les Etats 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 Etats membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation.

L'Art. 13 de la Directive de l'Union européenne sur le commerce électronique est un autre exemple des similitudes qui existent entre la structure dogmatique américaine et l'approche européenne. L'approche de l'Union européenne est comparable à celle de la loi américaine 17 U.S.C. § 517(b).[1599] Ces deux règlementations visent à préciser la responsabilité des fournisseurs de "caching" et établissent le lien entre les limitations de responsabilité et des exigences similaires. En ce qui concerne la responsabilité des prestataires de services[1600], la différence principale entre les deux approches réside dans le fait que l'application de l'Art. 13 de la Directive de l'Union européenne sur le commerce électronique n'est pas limitée aux violations de droits d'auteur mais exclut la responsabilité en ce qui concerne tout type d'infraction.

6.4.6 Responsabilité de l'hébergeur (Directive de l'Union européenne)

L'hébergeur a une fonction importante dans la commission d'une infraction, notamment en ce qui concerne les contenus illégaux. Les auteurs d'infractions qui mettent en ligne des contenus illégaux ne les stockent généralement pas sur leurs propres serveurs. La plupart des sites Internet sont stockés sur des serveurs qui sont mis à disposition par des hébergeurs. Quiconque souhaite disposer d'une page Internet peut louer une capacité de stockage à un hébergeur pour stocker son site Internet. Quelques hébergeurs proposent même gratuitement des espaces Internet commandités par de la publicité.[1601]

1599 The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq. , available at: http://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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

1600 See above: Chapter 6.4.4.

1601 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.

L'identification de contenus illégaux est un défi pour les hébergeurs. Cela est particulièrement vrai pour les hébergeurs populaires qui proposent de nombreux sites et pour lesquels les recherches manuelles de contenus illégaux sur un aussi grand nombre de sites seraient impossibles. En conséquence, les rédacteurs de la Directive ont décidé de limiter la responsabilité des hébergeurs. Toutefois, contrairement au cas des fournisseurs d'accès, la responsabilité de l'hébergeur n'est pas exclue. Pour autant que l'hébergeur n'a pas de véritable connaissance d'activités illégales ou de contenus illégaux stockés sur ses serveurs, il n'est pas responsable. L'hypothèse que des contenus illégaux puissent être stockés sur ses serveurs n'est pas considérée ici comme étant équivalente à une connaissance réelle du problème. Si l'hébergeur est véritablement au courant d'activités illégales ou de contenus illégaux, il peut seulement éviter d'être responsable en retirant immédiatement les informations illégales.[1602] L'absence de réaction immédiate conduit à la responsabilité de l'hébergeur.[1603]

> ***Article 14 – Hébergement***
>
> *1. Les Etats 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 Etats 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 Etats membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.*

L'Art. 14 ne s'applique pas uniquement aux hébergeurs qui limitent leurs services à la location d'infrastructures techniques de stockage de données. Des services Internet populaires comme les plates-formes d'enchères offrent également des services d'hébergement.[1604]

6.4.7 Exclusion de l'obligation de surveillance (Directive de l'Union européenne)

Avant que la Directive soit mise en œuvre, il n'était pas certain, chez certains Etats membres, que les prestataires puissent être poursuivis sur la base d'une violation de l'obligation de surveillance des activités des utilisateurs. A part la possibilité de conflit avec les règlementations relatives à la protection des données et le secret des télécommunications, une telle obligation causerait, notamment, des difficultés aux hébergeurs qui stockent des milliers de sites Internet. Pour éviter ces conflits, la Directive exclut l'obligation générale de surveiller les informations transmises ou stockées.

> ***Article 15 – Absence d'obligation générale en matière de surveillance***
>
> *1. Les Etats 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*

1602 This procedure is called "notice and takedown».

1603 The hosting provider is quite often in a difficult situation. On the one hand side he needs to react immediately to avoid liability – on the other hand side he has certain obligations with regard to his customers. If he removes legal information that was just on first sight illegal, this could lead to claims for indemnity.

1604 By enabling their customers to offer products they provide the necessary storage capacity for the required information.

stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.

2. Les Etats 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.

6.4.8 Responsabilité en matière d'hyperliens (ECC Autriche)

Les hyperliens jouent un rôle important sur Internet. Ils permettent aux fournisseurs d'hyperliens de guider les utilisateurs vers des informations spécifiques disponibles en ligne. Au lieu de simplement proposer des détails techniques sur la façon d'accéder aux informations (par exemple, en fournissant le nom de domaine du site web où l'information est offerte), les utilisateurs peuvent accéder directement aux informations en cliquant sur l'hyperlien actif. L'hyperlien 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 d'une réglementation sur les hyperliens a fait l'objet d'un vif débat.[1605] Les rédacteurs ont décidé de ne pas obliger les Etats membres à harmoniser leurs législations concernant leurs responsabilités en matière d'hyperliens. Au lieu de cela, ils ont mis en œuvre une procédure de réexamen pour s'assurer qu'était pris en considération le besoin de propositions concernant la responsabilité des fournisseurs d'hyperliens ainsi que les services des outils de localisation.[1606] En attendant que la réglementation de la responsabilité des hyperliens soit modifiée, les Etats membres sont libres d'élaborer des solutions nationales[1607]. Certains pays de l'Union européenne ont décidé d'étudier la responsabilité des fournisseurs d'hyperliens dans le cadre d'une disposition spécialisée.[1608] Ces pays ont basé la responsabilité des fournisseurs d'hyperliens sur les mêmes principes que ceux de la Directive en ce qui concerne la responsabilité des hébergeurs.[1609] Cette approche est la conséquence logique de la situation comparable des hébergeurs et des fournisseurs d'hyperliens. Dans les deux cas, ces fournisseurs contrôlent les contenus illégaux ou au moins le lien vers ces contenus.

La Sec. 17 de la ECC autrichienne[1610] en est un exemple:

Sec. 17 ECC (Autriche) – Responsabilité en matière d'hyperliens

---

1605 *Spindler*, Multimedia und Recht 1999, page 204.

1606 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.

1607 *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

1608 Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

1609 See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

1610 § 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.

(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 il aurait été apparent au prestataire de services que ces activités ou informations étaient illégales; ou

2. après avoir pris connaissance de ces activités ou informations, il a agit rapidement pour retirer le lien électronique.

6.4.9 Responsabilité en matière de moteur de recherche

Les fournisseurs de moteurs de recherche proposent des services de recherche utilisés pour identifier des documents d'intérêt en spécifiant certains critères. Ces moteurs recherchent des documents pertinents qui correspondent aux critères indiqués par l'utilisateur. Ils jouent un rôle important dans le bon développement de l'Internet. Les contenus mis à disposition sur un site web et qui ne sont pas énumérés sur l'index du moteur de recherche ne peuvent être consultés que si la personne souhaitant y accéder connaît l'URL complète. *Introna/Nissenbaum* souligne que "sans vraiment exagérer, on pourrait dire pour exister il faut être indexé par un moteur de recherche".[1611]

Comme pour les hyperliens, la Directive de l'Union européenne ne contient pas de normes qui définissent la responsabilité des opérateurs de moteurs de recherche. En conséquence, certains pays de l'Union européenne ont décidé de traiter la responsabilité des fournisseurs de moteurs de recherche par une disposition spécialisée.[1612] Contrairement au cas des hyperliens, tous les pays n'ont pas basé leurs réglementations sur les mêmes principes.[1613] L'Espagne[1614] et le Portugal ont basé leur réglementation en ce qui concerne la responsabilité des opérateurs de moteurs de recherche sur l'Art. 14 de la Directive alors que l'Autriche[1615] a basé la limitation de responsabilité sur l'Art. 12.

1611 *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, Page 5. Available at: http://www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

1612 Austria, Spain and Portugal. See report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

1613 See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

1614 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 conteni-dos 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.

1615 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.

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.

7 Références juridiques

Convention sur la cybercriminalité du Conseil de l'Europe[1616]

Modèle de Loi du Commonwealth sur l'informatique et les infractions liées à l'informatique[1617]

Projet de Convention de Stanford[1618]

1616 Council of Europe Convention on Cybercrime, available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

1617 Commonwealth Model Law on Computer and Computer Related Crime, available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

1618 Draft Stanford Convention, available at: http://www.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf.

Imprimé en Suisse
Genève, 2009