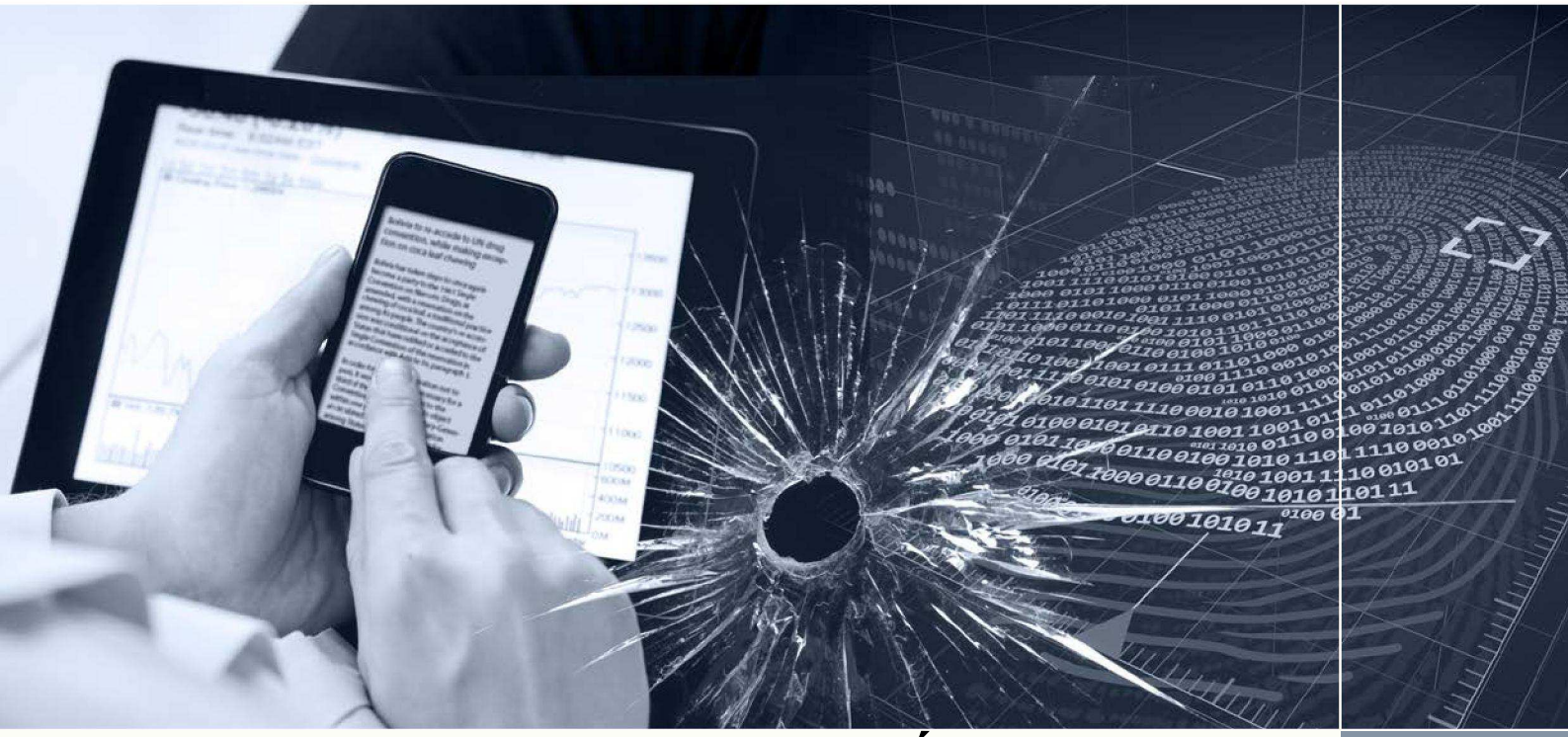
UNODC
United Nations Office on Drugs and Crime



Étude détaillée sur la cybercriminalité

Ébauche — Février 2013

OFFICE DES NATIONS UNIES
CONTRE LA DROGUE ET LE CRIME
Vienne

Étude détaillée sur la Cybercriminalité

Ébauche

Février 2013

UNITED NATIONS
New York, 2013

REMERCIEMENTS

Ce rapport a été préparé pour le groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée par le service d´appui aux conférences, la Direction du crime organisé, la Division des traités, l´ONUDC, sous la supervision de John Sandage (Directeur de la Division des traités), Sara Greenblatt (Chef de la Direction du crime organisé), et Gillian Murray (Coordinatrice principale en matière de cybercriminalité de l´ONUDC et Chef du service d´appui aux conférences).

Équipe chargée de l´étude :

Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (ONUDC)

Consultants :

Ulrich Sieber, Tatiana Tropina, Nicolas von zur Mühlen
(Institut Max Planck de droit pénal étranger et de droit international pénal)

Ian Brown, Joss Wright
(Centre de sécurité informatique et institut internet d'Oxford, Université d´Oxford)

Roderic Broadhurst
(Université nationale australienne)

Kristin Krüger
(Institut Brandenburg pour la sécurité et la société)

Avertissements

Ce rapport est une ébauche préparée pour la seconde réunion du groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée et ne devra pas être cité sans l´accord de l´ONUDC. Ce rapport n´a pas été formellement édité et reste soumis à des modifications rédactionnelles.

Le contenu de ce rapport ne reflète pas nécessairement les vues ou les politiques de l´ONUDC ou des organismes contributeurs et ne suppose pas non plus une ratification de leur part.Les désignations employées et la présentation du matériel dans ce rapport n´impliquent de la part de l´ONUDC aucune prise de position quant au statut juridique des pays, des territoires, des villes ou de leurs autorités, ni quant au tracé de leurs frontières ou limites.

CONTENUS

LISTE DES ABRÉVIATIONS

Abréviations

CERT	Équipe d´intervention informatique d´urgence
CSIRT	Équipe d´intervention en cas d´incident lié à la sécurité informatique
ECHR	Convention européenne pour la Protection des droits de l´homme et des libertés fondamentales
ECtHR	Cour européenne des droits de l´homme
EU	Union européenne
EUROPOL	Office européen de police
G8	Groupe des huit
GDP	Produit intérieur brut
HDI	Indice de développement humain
ICCPR	Pacte international sur les droits civils et politiques
ICCPR-OP2	Deuxième protocole facultatif se rapportant au pacte international sur les droits civils et politiques, visant à abolir la peine de mort
ICERD	Convention internationale sur l´élimination de toutes les formes de discrimination raciale
ICESCR	Pacte international relatif aux droits économiques, sociaux et culturels
ICRMW	Convention internationale des Nations Unies sur la protection des droits de tous les travailleurs migrants et des membres de leurs familles
TIC	Technologie de l´information et des communications
INTERPOL	Organisation internationale de police criminelle
IP	Protocole internet
ISP	Fournisseur de service internet
IT	Technologie de l´information
ITU	Union internationale des télécommunications
NFC	Communication en champ proche
OP-CRC-SC	Convention relative aux droits de l´enfant et Protocole facultatif concernant la vente d´enfants, la prostitution et la pornographie infantiles
P2P	Pair à pair
SCO	Organisation de coopération de Shanghai
SMS	Service de messagerie courte
TRIPS	Accord sur les aspects commerciaux des droits de propriété intellectuelle
UNESCO	Organisation des Nations Unies pour l´éducation, la science et la culture
UNODC	Office des Nations Unies contre la drogue et le crime
UNSC	Conseil de sécurité des Nations Unies
URL	Localisateur de ressources uniformes
USB	Bus universel en série
VGT	Groupe de travail virtuel international
WEF	Forum économique mondial

Liste des instruments régionaux et internationaux et leurs abréviations

Union Africaine, 2012. Projet de Convention relatif à l´établissement d´un cadre juridique pour la cybersécurité en Afrique (**Projet de Convention de l´Union Africaine**).

Marché commun de l´Afrique orientale et australe (COMESA), 2011. Ébauche de projet de loi sur la cybersécurité. (**Ébauche de projet de loi du COMESA**).

Le Commonwealth, 2002. (i) le projet de loi sur l´informatique et les délits liés à l´informatique et (ii) la loi type sur les preuves électroniques (**loi type du Commonwealth**).

La Communauté des états indépendants, 2001. Accord de coopération en matière de lutte contre les infractions liées à l´information informatique (**Accord de la communauté des états indépendants**).

Conseil de l´Europe, 2001. Convention sur la cybercriminalité et protocole additionnel à la Convention sur la cybercriminalité, relatifs à l´incrimination d´actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (**Convention/protocole sur la cybercriminalité du Conseil de l´Europe**).

Conseil de l´Europe, 2007. Convention sur la protection des enfants contre l´exploitation et les abus sexuels (**Convention du Conseil de l´Europe sur la protection des enfants**).

Communauté économique des états de l´Afrique de l´ouest (CEDEAO), 2009. Projet de directive pour lutter contre la cybercriminalité au sein de la Communauté économique des états de l´Afrique de l´ouest (**projet de directive de la CEDEAO**).

Union Européenne, 2000. Directive 2000/31/EC du Parlement européen et du Conseil sur certains aspects juridiques des services de la société d´information et notamment du commerce électronique, dans le marché intérieur (**directive de l´UE en matière de commerce électronique**).

Union Européenne, 2001. Décision-cadre du Conseil 2001/413/JHA relative à la lutte contre la fraude et la contrefaçon des moyens de paiement autre que les espèces (**décision de l´UE relative à la fraude et la contrefaçon**).

Union Européenne, 2002. Directive 2002/58/EC du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (**Directive de l´UE relative à la protection des données**).

Union Européenne, 2005. Décision-cadre du Conseil 2005/222/JHA relative aux attaques visant les systèmes d´information (**décision de l´UE relative aux attaques visant les systèmes d´information**).

Union Européenne, 2006. Directive 2006/24/EC du Parlement européen et du Conseil sur la conservation des données générées ou traitées dans le cadre de la fourniture des services de communications électroniques accessibles au public ou de réseaux publics de communication (**Directive de l´UE relative à la conservation des données**).

Union Européenne, 2010. Proposition COM(2010) 517 de Directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d´information et abrogeant la décision-cadre 2005/222/JHA du Conseil (**Proposition de directive de l´UE relative aux attaques visant les systèmes d´information**).

Union Européenne, 2011. Directive 2011/92/EU du Parlement européen et du Conseil relative à la lutte contre les abus sexuels et l´exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JHA du Conseil (**Directive de l´UE relative à l´exploitation des enfants**).

Union internationale des télécommunications (ITU)/Communauté des Caraïbes (CARICOM)/ Union caraïbe des télécommunications (CTU), 2010. Textes législatifs types en matière de cybercriminalité /crimes électroniques et de preuves électroniques (**UIT/CARICOM/CTU Textes législatifs types**).

Ligue des états arabes, 2010. Convention arabe sur la lutte contre les infractions portant sur les technologies de l´information (**Convention de la Ligue des états arabes**).

Ligue des états arabes, 2004. Loi type arabe sur la lutte contre les infractions portant sur les systèmes de technologies de l´information (**Loi type de la Ligue des états arabes**).

Organisation de coopération de Shanghai, 2010. Accord de coopération dans le domaine de la sécurité de l´information au niveau international (**Accord de l´Organisation de coopération de Shanghai**).

Nations Unies, 2000. Protocole facultatif à la Convention relative aux droits de l´enfant concernant la vente d´enfants, la prostitution et la pornographie infantiles (**Nations Unies OP-CRC-SC**).

Page intentionnellement laissée vierge

INTRODUCTION

La résolution 65/230 de l´Assemblée générale demandait à la Commission pour la prévention du crime et la justice pénale d´établir un groupe intergouvernemental d´experts à composition non limitée, en vue de réaliser une étude approfondie sur la cybercriminalité et les mesures prises par les états membres, la communauté internationale et le secteur privé, y compris en matière d´échange d´informations sur les législations nationales, les meilleures pratiques, l´assistance technique et la coopération internationale.

Dans sa résolution 65/230, l´Assemblée générale a prié la Commission pour la prévention du crime et la justice pénale d´établir, conformément au paragraphe 42 de la Déclaration de Salvador sur les stratégies globales pour faire face aux défis mondiaux : des systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation, un groupe intergouvernemental d´experts à composition non limitée, en vue de réaliser une étude approfondie sur la cybercriminalité et les mesures prises par les états membres, la communauté internationale et le secteur privé, y compris en matière d´échange d´informations sur les législations nationales, les meilleures pratiques, l´assistance technique et la coopération internationale, afin d´examiner les options envisageables pour renforcer les mesures juridiques existantes et pour en proposer de nouvelles à l´échelle nationale ou internationale pour faire face à la cybercriminalité.[1]

Dans sa résolution 67/189, l´Assemblée générale a pris note avec satisfaction du travail effectué par le groupe intergouvernemental d´experts à composition non limitée en vue de réaliser une étude approfondie sur la cybercriminalité, et l´a encouragé à poursuivre ses efforts, afin de terminer son travail et de présenter les conclusions de l´étude à la Commission pour la prévention du crime et la justice pénale en temps voulu.

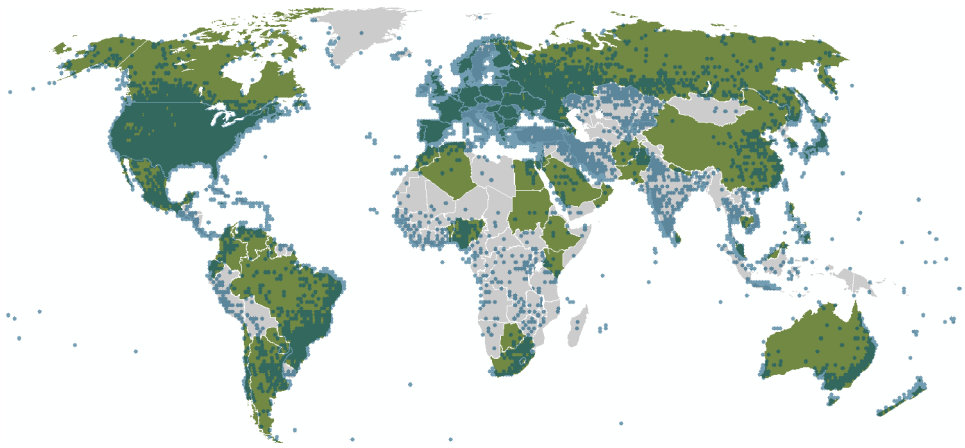
La première session du groupe d´experts s´est tenue à Vienne du 17 au 21 janvier 2011. Lors de cette réunion, le groupe d´experts a examiné et adopté un ensemble de thèmes et une méthodologie pour l´étude.[2]

Les thèmes à examiner dans le cadre d´une étude détaillée sur la cybercriminalité incluaient le problème de la cybercriminalité, les ripostes juridiques à la cybercriminalité, les capacités en matière de justice pénale et de prévention de la criminalité ainsi que d´autres mesures de lutte contre la cybercriminalité, les organisations internationales et l´assistance technique. Ces thèmes principaux furent ensuite divisés en 12 sous-thèmes.[3] Dans cette étude, huit chapitres traitent ces thèmes : (1) Connectivité et cybercriminalité ; (2) la perspective d´ensemble ; (3) Les cadres et la législation ; (4) Incrimination ; (5) Application des lois et enquêtes ; (6) preuves électroniques et justice pénale ; (7) Coopération internationale ; et (8) prévention. La méthodologie de cette étude exige de développer un questionnaire à des fins de collecte et d´analyse de données et de développer une ébauche de texte de l´étude.

1 Résolution 65/230 de l´Assemblée générale, Annexe.
2 E/CN.15/2011/19
3 (1) Phénomène de cybercriminalité ; (2) données statistiques ; (3) défis de la cybercriminalités ; (4) approches communes à la législation ; (5)incrimination ; (6) pouvoirs procéduraux ; (7) coopération internationale ; (8)preuves électroniques ; (9) rôles et responsabilités des prestataires de services et du secteur privé ; (10) prévention de la criminalité, capacités en matière de justice pénale et autres ripostes face à la cybercriminalité ; (11) organisations internationales ; et (12) assistance technique.

L´UNODC a recueilli des informations en conformité avec la méthodologie, et a distribué un questionnaire aux états membres, aux organisations intergouvernementales et aux représentants du secteur privé et des institutions académiques, de février 2012 à juillet 2012. 69 états membres ont transmis des informations avec la distribution régionale suivante : Afrique (11), Amériques (13), Asie (19), Europe (24), et Océanie (2). 40 organisations du secteur privé, 16 organisations académiques et 11 organisations intergouvernementales ont transmis des informations. Le Secrétariat a également examiné plus de 500 documents d´accès. Des détails supplémentaires sur la méthodologie sont inclus dans l´Annexe Cinq de la présente étude.

Réponses des états membres au questionnaire de l´étude (vert) et pénétration d'iinternet (bleu)



Source : réponses au questionnaire de l´étude et élaboration de MaxMind GeoCityLite de l´ONUDC

Comme le demandait la résolution 65/230 de l´Assemblée générale, cette étude a été préparée en vue de « examiner les options envisageables pour renforcer les mesures juridiques existantes et pour en proposer de nouvelles à l´échelle nationale ou internationale pour faire face à la cybercriminalité ». Ce mandat s´inscrit dans le cadre de divers mandats et activités concernant la cybercriminalité et la cybersécurité au sein du système des Nations Unies.[4] À cet égard, l´étude est axée sur les aspects de *prévention de la criminalité* et de *justice pénale* en matière de prévention et de lutte contre la cybercriminalité.

Cette étude représente un aperçu des efforts réalisés en matière de prévention de la criminalité et de justice pénale, pour prévenir et combattre la cybercriminalité.

Elle offre une perspective globale, souligne les enseignements tirés des efforts passés et des efforts actuels, et présente des options possibles pour de futures ripostes. Bien que le titre de l´étude soit la « cybercriminalité », cette étude a une pertinence particulière pour *tous* les délits. Étant donné que le monde évolue vers une société hyper connectée avec un accès universel à l´internet, il est difficile de concevoir un « délit informatique », et peut être n´importe quel délit, n´impliquant pas des preuves électroniques liées à la connectivité à internet. Une telle évolution pourrait requérir des changements fondamentaux dans l´approche de l´application de la loi, le recueil des preuves, et les mécanismes de coopération internationale en matière pénale.

4 Y compris le travail dans le cadre des progrès dans le domaine de l´information et les télécommunications dans le cadre de la sécurité internationale. Voir A/RES/66/24.

Principales conclusions et options

La résolution 65/230 de l´Assemblée générale demandait au groupe intergouvernemental d´experts de réaliser une étude approfondie sur le problème de la cybercriminalité en vue d´examiner les options envisageables pour renforcer les mesures juridiques existantes et pour en proposer de nouvelles à l´échelle nationale ou internationale pour faire face à la cybercriminalité. Cette partie présente les principales conclusions et options de cette étude.

Principales conclusions

- Les principales conclusions de l´étude concernent les thèmes suivants :
  - l´impact de la fragmentation au niveau international et la diversité des lois nationales sur la cybercriminalité dans le contexte de la coopération internationale ;
  - une dépendance envers les moyens traditionnels de coopération internationale formelle dans des affaires pénales impliquant la cybercriminalité, et les preuves électroniques pour tous les délits ;
  - Lle rôle de la localisation des preuves ;
  - l´harmonisation des cadres juridiques nationaux ;
  - la capacité en matière de justice pénale et d´application de la loi ;
  - les activités de prévention de la cybercriminalité.

Cette étude a examiné le problème de la cybercriminalité du point de vue des gouvernements, du secteur privé, des universités et des organisations internationales. Huit chapitres présentent ces résultats et abordent les thèmes de connectivité à internet et de cybercriminalité ; de la perspective globale de la cybercriminalité ; des structures et de la législation contre la cybercriminalité ; de l´incrimination de la cybercriminalité ; de l´application de la loi et des enquêtes sur la cybercriminalité ; de la justice pénale et des preuves électroniques ; de la coopération internationale dans des affaires pénales impliquant la cybercriminalité ; et la prévention de la cybercriminalité.

Les principales conclusions de ces thèmes sont présentées ci-après et plus détaillées dans le résumé analytique qui fait suite à la présente partie :

(a) la fragmentation au niveau international et la diversité des lois nationales contre la cybercriminalité, peuvent être en corrélation avec l´existence de multiples instruments ayant une portée géographique et des thèmes différents. Les instruments reflètent légitimement les différences socio-culturelles et régionales mais l´étendue des divergences des pouvoirs procéduraux et des dispositions en matière de coopération internationale peuvent entraîner l´émergence dans le pays de « groupements » de coopération qui ne conviennent pas toujours en raison de la nature globale de la cybercriminalité ;

(b) la dépendance envers des moyens traditionnels de coopération internationale formelle dans des affaires de cybercriminalité ne permet pas d´offrir l´intervention opportune requise pour obtenir des preuves électroniques volatiles. Étant donné qu´un nombre croissant de délits implique des preuves électroniques géo réparties, cela deviendra un problème non seulement dans des cas de cybercriminalité, mais pour tous les délits en général ;

(c) dans un monde d´informatique en nuage et de centres de données, le rôle de la localisation des preuves doit être revu, afin d´obtenir un consensus sur les questions concernant l´accès direct des autorités répressives aux données extraterritoriales ;

(d) l´analyse des cadres juridiques nationaux disponibles indique un manque d´harmonisation des principaux délits de cybercriminalité, des pouvoirs d´enquêtes et de la recevabilité des preuves électroniques. Les lois internationales sur les droits de l´homme représentent un important point de référence externe en matière d´incrimination de dispositions procédurales ;

(e) les autorités d´application de la loi, les procureurs et le système judiciaire des pays en développement, nécessitent un appui et une assistance technique complète, durable et à long terme afin d´enquêter et de lutter contre la cybercriminalité ;

(f) les activités de prévention de la cybercriminalité doivent être renforcées dans tous les pays, avec une approche holistique qui implique des initiatives de sensibilisation, des partenariats public-privé et l´intégration de stratégies contre la cybercriminalité avec une perspective plus large de cybersécurité.

Options pour renforcer les mesures juridiques existantes et pour en proposer de nouvelles à l´échelle nationale et internationale pour faire face à la cybercriminalité

- Les options pour renforcer les mesures juridiques existantes et pour en proposer de nouvelles à l´échelle nationale pour faire face à la cybercriminalité incluent :
  - le développement de dispositions internationales types ;
  - le développement d´un instrument multilatéral de coopération internationale concernant les preuves électroniques dans des affaires pénales ;
  - le développement d´un instrument multilatéral complet relatif à la cybercriminalité ;
  - fournir un niveau accru d´assistance technique aux pays en développement afin de prévenir et de lutter contre la cybercriminalité.

Les options présentées sont apportées par les réponses fournies par les pays à une question figurant dans le questionnaire de l´étude relative aux options qui devraient être envisagées pour renforcer les mesures juridiques existantes et pour en proposer de nouvelles à l´échelle nationale pour faire face à la cybercriminalité, ainsi que par les principales conclusions.

En réponse à cette question, les pays ont proposé une gamme de possibilités. La majorité des options suggérées concernent des domaines tels que : l´harmonisation des lois ; l´adhésion à des instruments régionaux ou internationaux existants contre la cybercriminalité ; le développement de nouveaux instruments juridiques internationaux ; le renforcement des mécanismes de coopération internationale et d´obtention de preuves extraterritoriales dans la pratiqueet le renforcement des capacités des institutions de justice pénale et d´application de la loi.[1]

Plusieurs pays ont précisé qu´un mécanisme rapide pour les procédures de coopération internationale dans des affaires pénales de cybercriminalité devrait être développé. Certains pays ont suggéré que cela pourrait être fait en renforçant les réseaux informels de police existants. D´autres pays ont proposé, pour ce faire, de développer davantage les voies formelles de coopération internationales existantes, y compris les accords bilatéraux et multilatéraux. Certains pays ont souligné que toutes les options devraient être mises en œuvre en conformité avec les normes internationales des droits de l´homme, y compris les droits concernant la liberté d´expression et la vie privée.

1 Questionnaire de l´étude sur la cybercriminalité. Q11.

Certains pays ont suggéré que l´adhésion à la Convention du Conseil de l´Europe sur la cybercriminalité favoriserait la coopération internationale et l´harmonisation des lois nationales contre la cybercriminalité. Certains pays ont recommandé que soit développé un nouvel instrument juridique international contre la cybercriminalité. D´autres pays ont signalé que l´harmonisation des législations devrait être promue en développant des dispositions juridiques internationales types au niveau des Nations Unies. Certains pays ont recommandé de développer des normes internationales relatives aux données extraterritoriales dans les enquêtes des services de détection et de répression, afin d´éclaircir les relations entre ces enquêtes et les principes de souveraineté nationale. Certains pays ont suggéré de renforcer l´assistance technique en matière de prévention et de lutte contre la cybercriminalité fournie aux autorités chargées de la justice, des poursuites et de l´application des lois. Sur la base des propositions formulées par les états membres et des principales conclusions, l´étude constate que les options envisageables pour renforcer les mesures juridiques existantes et pour en proposer de nouvelles à l´échelle nationale ou internationale pour faire face à la cybercriminalité peuvent inclure un ou plusieurs des points suivants :

(a) le développement de dispositions internationales types relatives à l´incrimination des principaux actes de cybercriminalité, afin d´aider les états à éliminer l´impunité en adoptant des éléments communs d´infractions :

(i) les dispositions pourraient maintenir l´approche des instruments existants pour ce qui concerne les infractions contre la confidentialité, l´intégrité et la disponibilité des données et des systèmes informatiques ;

(ii) les dispositions pourraient également couvrir les infractions « classiques » perpétrées ou facilitées par l´utilisation d´un système informatique, si les approches existantes d´incrimination sont considérées insuffisantes ;

(iii) les dispositions pourraient traiter des domaines qui ne sont pas couverts par les instruments existants, comme l´incrimination du SPAM ;

(iv) les dispositions pourraient être développées en conformité avec les normes internationales les plus avancées sur les droits de l´homme pour ce qui concerne l´incrimination, avec notamment des traités fondés sur la protection du droit à la liberté d´expression ;

(v) l´utilisation de telles dispositions par les états minimiserait les problèmes de double incrimination lors de la coopération internationale.

(b) le développement de dispositions internationales types concernant les pouvoirs d´enquêtes pour les preuves électroniques, afin que les états disposent des outils de procédure nécessaires pour enquêter sur des délits mettant en cause des preuves électroniques :

(i) les dispositions pourraient s´inspirer de l´approche des instruments existants, y compris les ordonnances de conservation rapide des données et les ordonnances d´obtention de données stockées et de données en temps réel ;

(ii) les dispositions pourraient offrir une orientation sur la portée des pouvoirs traditionnels tels que la perquisition et la saisie des preuves électroniques ;

(iii) les dispositions pourraient offrir une orientation sur l´application de mesures appropriées, basées sur des lois internationales sur les droits de l´homme ainsi que sur des traités fondés sur la protection de la vie privée, contre les techniques d´enquêtes intrusives.

(c) le développement de dispositions types relatives à la compétence, afin de disposer de fondements de compétence communs et efficaces dans des affaires pénales de cybercriminalité :

(i) les dispositions pourraient inclure des bases comme celles qui sont issues du principe de la territorialité objective et de la doctrine des effets substantiels ;

(ii) les dispositions pourraient inclure une orientation pour traiter des questions de compétence concurrente.

(d) le développement de dispositions types relatives à la coopération internationale en matière de preuves électroniques, pour les inclure dans des instruments bilatéraux ou multilatéraux, ainsi qu´un traité type des Nations Unies révisé sur l´entraide judiciaire, en conformité avec les suggestions du guide de discussion du treizième congrès pour la prévention du crime et la justice pénale :

(i) les dispositions pourraient se focaliser sur des mécanismes pratiques de coopération pouvant être incorporés aux instruments existants, afin de conserver et de fournir des preuves électroniques en temps opportun dans des affaires pénales ;

(ii) les dispositions pourraient inclure l´obligation d´établir des points focaux pour des réponses rapides en matière de preuves électroniques et des échéances convenues pour les réponses.

(e) le développement d´un instrument multilatéral de coopération internationale concernant les preuves électroniques dans des affaires pénales, afin de disposer d´un mécanisme international de coopération en temps opportun pour conserver et obtenir des preuves électroniques :

(i) en complémentarité avec les traités internationaux de coopération existants, un tel instrument pourra porter essentiellement sur un mécanisme permettant de demander une conservation rapide des données pour une période déterminée ;

(ii) l´instrument peut également inclure des dispositions spécifiques de coopération pour des mesures d´enquêtes supplémentaires, et cela inclut la transmission de données stockées et le recueil de données en temps réel ;

(iii) le champ d´application devra être défini mais ne devrait pas être limité à la « cybercriminalité » ou aux « délits liés à l´informatique » ;

(iv) l´instrument pourrait requérir une réponse dans un délai déterminé et établir des canaux de communication entre les points focaux, en s´appuyant sur les initiatives 24/7 existantes plutôt qu´en faisant double emploi avec ces initiatives ;

(v) l´instrument pourrait inclure des garanties traditionnelles de coopération internationale, ainsi que les exclusions appropriées en matière des droits de l´homme.

(f) le développement d´un instrument complet multilatéral sur la cybercriminalité, afin d´établir une approche internationale en matière d´incrimination, de pouvoirs procéduraux, de juridiction et de coopération internationale :

(i) l´instrument pourrait inclure des éléments de toutes les options susmentionnées sous une forme contraignante et multilatérale ;

(ii) l´instrument pourrait s´inspirer des principales similitudes de la gamme actuelle d´instruments régionaux et internationaux contraignants et non contraignants.

(g) le renforcement des partenariats nationaux, régionaux et internationaux, y compris avec le secteur privé et les institutions académiques, afin de fournir une assistance technique accrue aux pays en développement pour prévenir et combattre la cybercriminalité :

(i) l´assistance technique fournie pourrait s´appuyer sur des normes développées à partir des dispositions types comme le mentionnent les options ci-dessus ;

(ii) l´assistance technique fournie pourrait se focaliser sur les prestations des multiples parties prenantes, y compris des représentants du secteur privé et des institutions académiques.

Page intentionnellement laissée vierge

RÉSUMÉ ANALYTIQUE

Connectivité et cybercriminalité

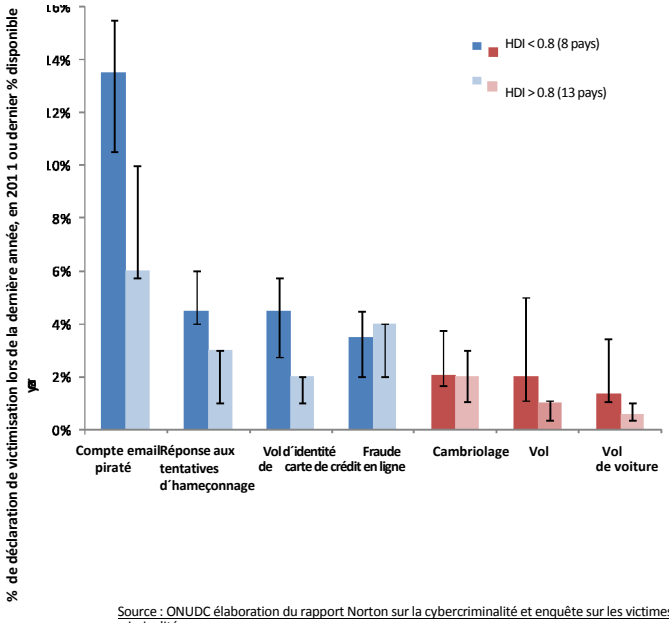
En 2011, au moins 2,3 milliards de personnes, l´équivalent de plus d´un tiers de la population mondiale, a eu accès à l´internet. Plus de 60 % de tous les utilisateurs de l´internet se trouvent dans des pays développés et 45 % de tous les utilisateurs de l´internet ont moins de 25 ans. D´ici à l´année 2017, on estime que près de 70 % de la population mondiale aura un abonnement au haut débit. D´ici à l´année 2020, les dispositifs en réseau (« l´internet des objets ») seront 6 fois plus nombreux que les personnes, et cela transformera les conceptions actuelles de l´internet. Dans le monde hyper connecté de demain il sera difficile de concevoir un « délit informatique », et peut être n´importe quel délit, n´impliquant pas des preuves électroniques liées à la connectivité du protocole internet (IP).

Les définitions de la cybercriminalité dépendent surtout des fins recherchées en utilisant ce terme. Un nombre limité d´actes contre la confidentialité, l´intégrité et la disponibilité des données et des systèmes informatiques représentent l´essentiel de la cybercriminalité. Toutefois, des actes liés à l´informatique commis pour un profit personnel ou financier, ou pour porter préjudice, y compris des formes de crimes liés à l´identité et les actes liés au contenu informatique (tous ceux qui sont inclus dans le sens le plus large du terme « cybercriminalité ») ne facilitent pas l´établissement des définitions légales du terme global. Certaines définitions sont requises pour les principaux actes de cybercriminalité. Cependant, une « définition » de la cybercriminalité n´est pas essentielle pour d´autres finalités, comme lorsqu´il s´agit de définir la portée des pouvoirs en matière de coopération internationale et d´enquêtes spécialisées, qui concernent surtout les preuves électroniques pour tout délit, au-delà d´un concept vaste et artificiel de la « cybercriminalité ».

La perspective globale

Dans de nombreux pays, l´explosion de la connectivité globale est survenue à un moment de transformations économiques et démographiques, avec une disparité croissante des revenus, une contraction des dépenses du secteur privé et une liquidité financière réduite. Au niveau global, les organismes d´application de la loi répondants de l´étude signalent des niveaux croissants de cybercriminalité, car les individus et les groupes criminels organisés, motivés par les profits et les gains personnels exploitent de nouvelles

La cybercriminalité et la victimisation classique relative au crime



Source : ONUDC élaboration du rapport Norton sur la cybercriminalité et enquête sur les victimes de la criminalité.

possibilités criminelles. On estime que plus de 80 % des actes de cybercriminalité proviennent d´activités organisées, et il existe des marchés noirs de cybercriminalité établis dans des cycles de création des logiciels malveillants, des infections informatiques, des gestions de botnet (réseau de machines), la récupération des données financières ou personnelles, la vente de données financières et leur encaissement. Les auteurs de délits de cybercriminalité ne nécessitent plus des habilités ou des techniques complexes. Dans le contexte des pays en développement, notamment, ont émergé des sous-cultures de jeunes qui commettent des fraudes financières liées à l´informatique, et l´implication de certains d´entre eux dans la cybercriminalité débute vers la fin de leur adolescence.

Globalement, les actes de cybercriminalité sont amplement répartis entre des infractions de nature financière et des infractions liées au contenu informatique, et incluent également des actes contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques. Les entreprises du secteur privé et les gouvernements ont des perceptions variables des menaces et des risques relatifs. Actuellement les statistiques des infractions enregistrées par la police ne représentent pas une base solide pour établir des comparaisons transnationales, même si ces statistiques sont souvent importantes pour les stratégies au niveau national. Deux tiers des pays considèrent que leurs systèmes de statistiques policières sont insuffisants pour consigner les délits de cybercriminalité. Les taux de cybercriminalité enregistrés par la police sont davantage associés au niveau de développement des pays et à la capacité de la police spécialisée, plutôt qu´aux taux de criminalité sous-jacents.

Les enquêtes de victimisation représentent une base de comparaison plus fiable. Elles démontrent que la victimisation individuelle relative à la cybercriminalité est significativement plus élevée que les formes classiques de criminalité. Les taux de victimisation concernant les fraudes de cartes de crédit en ligne, les vols d´identité, les réponses aux tentatives d´hameçonnage et l´accès non autorisé à un compte email, varient entre 1 et 17 % de la population en ligne dans 21 pays du monde entier, alors que les taux pour les délits classiques de cambriolage, de vol et de vol de voitures sont inférieurs à 5 % dans ces mêmes pays. Les taux de victimisation relative à la cybercriminalité sont plus élevés dans les pays dont le niveau de développement est plus bas, et cela démontre qu´il est nécessaire de renforcer les efforts de prévention dans ces pays.

Les entreprises du secteur privé en Europe signalent des taux de victimisation similaires –entre 2 et 16 % – avec des actes comme la violation de données par intrusion ou hameçonnage. Les outils criminels choisis pour ces délits, comme les botnets, ont une portée mondiale. Plus d´un million d´adresses IP uniques fonctionnaient au niveau global comme des serveurs de contrôle et de commandes de botnets en 2011. Les gouvernements sont également préoccupés par le contenu d´iinternet. Du matériel devant être supprimé comme la pornographie infantile et les discours de haine, mais également les contenus liés aux critiques et aux diffamations à l´égard du gouvernement, soulèvent des préoccupations relatives aux lois sur les droits de l´homme dans certains cas. On estime qu´environ 24 % du trafic global d´internet enfreint le droit d´auteur, en téléchargeant avec du matériel partagé en pair à pair (P2P) et cela est particulièrement fréquent dans des pays d´Afrique, d´Amérique du sud et d´Asie du sud et de l´ouest.

Législation et structures

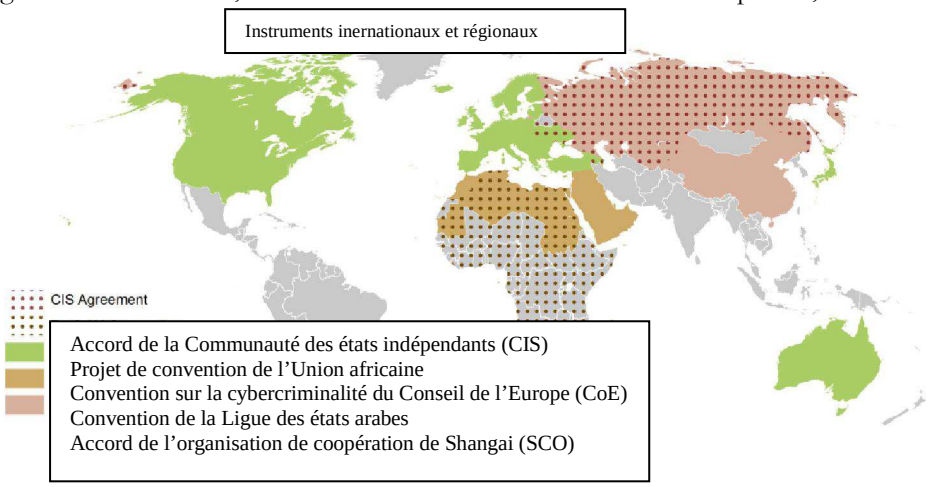
Les mesures juridiques ont un rôle clef dans la prévention et la lutte contre la cybercriminalité. Elles sont nécessaires dans tous les domaines, y compris en matière d´incrimination, de pouvoirs procéduraux, de juridiction, de coopération internationale et en ce qui concerne la responsabilité des prestataires de services internet. Au niveau national, les nouvelles lois (ou les lois prévues) et les lois existantes sur la cybercriminalité concernent généralement l´incrimination et visent à établir des délits spécialisés pour les principaux actes de cybercriminalité. Toutefois, les pays reconnaissent de plus en plus la nécessité d´une législation dans d´autres domaines. En comparaison avec les lois existantes, les nouvelles lois ou les lois prévues contre la cybercriminalité abordent plus fréquemment la question des mesures d´enquêtes, la juridiction, les preuves électroniques et la coopération internationale. Globalement, moins de la moitié des pays ayant répondu au questionnaire considèrent que les cadres de droit pénal et procédural sont suffisants, bien que cela masque d´importantes différences régionales. Alors que plus de deux tiers des pays en Europe considèrent que la législation est suffisante, la situation est inversée en Afrique, dans les Amériques, en Asie

et en Océanie, où plus de deux tiers des pays considèrent que la législation est partiellement suffisante ou insuffisante. Seulement la moitié des pays, qui ont signalé que la législation était insuffisante, a également signalé de nouvelles lois ou des lois prévues, et ont ainsi souligné un besoin urgent de consolider les législations dans ces régions.

Des progrès significatifs concernant la promulgation d´instruments régionaux et internationaux visant à lutter contre la cybercriminalité sont survenus lors de la dernière décennie. Ceci inclut des instruments contraignants et non contraignants.

On peut mentionner cinq catégories, avec des instruments développés dans le cadre de, ou inspirés par : (i) le Conseil de l´Europe ou l´Union Européenne, (ii) la Communauté des états indépendants ou l´Organisation de coopération de Shanghai, (iii) les organisations intergouvernementales africaines, (iv) la Ligue des états arabes, et (v) les Nations Unies. Un significatif enrichissement mutuel existe entre tous les instruments, notamment en ce qui concerne les concepts et les approches développés dans la Convention sur la cybercriminalité du Conseil de l´Europe. Une analyse des articles de 19 instruments multilatéraux pertinents en matière de cybercriminalité révèle des dispositions essentielles communes, mais également des divergences significatives dans des importants domaines abordés.

Globalement 82 pays ont signé et /ou ratifié un instrument contraignant sur la cybercriminalité.[1] Outre la mise en œuvre et l´adhésion formelle, les instruments multilatéraux sur la cybercriminalité ont influencé indirectement les législations nationales, en servant de modèle à des états non parties, ou en influençant la législation des états parties dans d´autres pays. L´adhésion à un instrument multilatéral sur la cybercriminalité cause la perception d´une suffisance accrue du droit procédural et pénal national, et cela indique que les dispositions multilatérales actuelles dans ces domaines sont généralement considérées comme efficaces. Pour plus de 40 pays qui ont fourni des informations, la Convention sur la cybercriminalité du Conseil de l´Europe est l´instrument multilatéral le plus utilisé pour le développement de la législation en matière de cybercriminalité. De plus des instruments multilatéraux inclus dans d´autres « catégories » ont été utilisés dans près de la moitié des pays.



Un tiers des pays qui ont répondu au questionnaire considèrent que leur législation est totalement ou hautement harmonisée avec les pays considérés comme importants dans le cadre de la coopération internationale. Toutefois, cela varie au niveau régional, avec des niveaux plus élevés d´harmonisation dans les Amériques et en Europe. Ceci peut être dû dans certaines régions à l´utilisation d´instruments multilatéraux, fondamentalement conçus pour jouer un rôle dans l´harmonisation. La fragmentation au niveau international et la diversité des lois nationales, pour ce qui concerne l´incrimination des actes de cybercriminalité, les bases juridictionnelles et les mécanismes de coopération, peuvent être en corrélation avec l´existence de multiples instruments ayant une portée géographique et des thèmes différents. Les instruments et les régions reflètent actuellement des divergences provenant de différences juridiques et constitutionnelles sous-jacentes, ainsi que des conceptions différentes en matière de droits et de vie privée.

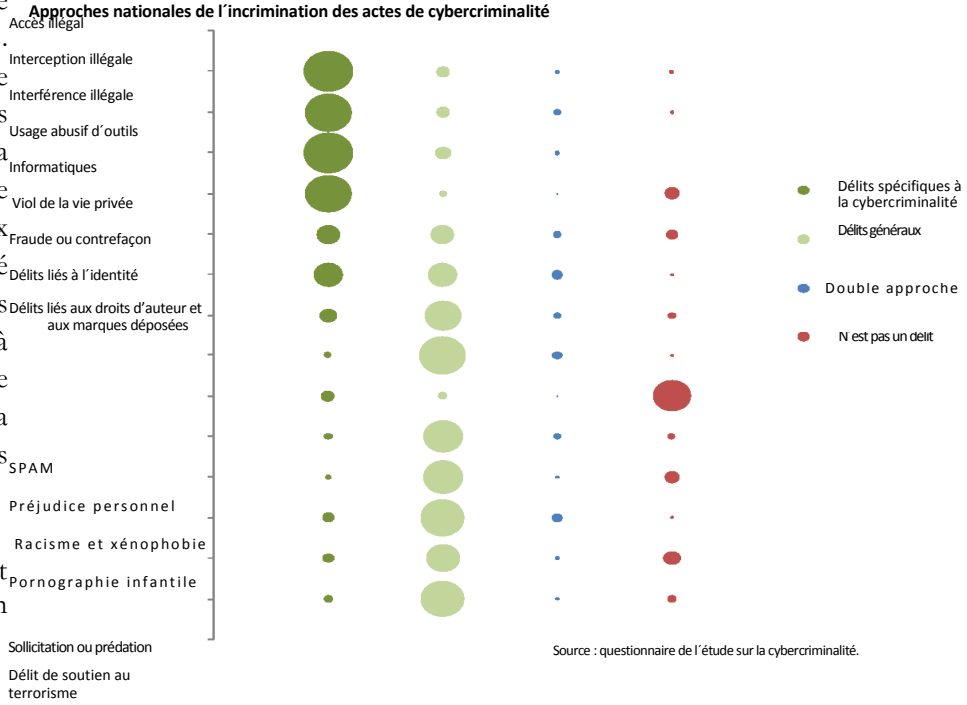
1 Un ou plusieurs : Convention sur la Cybercriminalité du Conseil de l´Europe, la Convention sur la lutte contre les infractions liées aux technologies de l´information de la Ligue des états arabes, l´Accord de coopération en matière de lutte contre les infractions liées à l´information informatique de la Communauté des états indépendants, ou l´Accord dans le domaine de la sécurité de l´information au niveau international de l´Organisation de coopération de Shanghai.

2 La source primaire a été analysée pour 97 états membres, y compris 56 états qui ont répondu au questionnaire, et dont la distribution régionale est la suivante : Afrique (15), Amériques (22), Asie (24), Europe (30), et Océanie (6).

Incrimination

Les informations sur les lois pénales en matière de cybercriminalité ont été recueillies par le biais du questionnaire de l´étude ainsi que par une analyse des sources primaires des législations en vigueur réalisée par le Secrétariat.[2] Le questionnaire de l´étude mentionnait 14 actes généralement inclus dans le concept de la cybercriminalité.[3] Les pays qui ont répondu au questionnaire ont décrit une incrimination généralisée de ces 14 actes, à l´exception des délits de SPAM et dans une certaine mesure des délits relatifs à l´usage abusif des outils informatiques, au racisme et à la xénophobie, et à la sollicitation ou à la prédation sexuelle des enfants en ligne. Ceci reflète un certain consensus de base sur les conduites coupables en matière de cybercriminalité. Les pays signalent peu de délits additionnels, non mentionnés dans le questionnaire. Ils concernent principalement les contenus informatiques, l´incrimination de matériel obscène, les paris en ligne, et les marchés illicites en ligne, de drogues et de personnes, par exemple. Pour les 14 actes, les pays ont signalé l´utilisation de délits spécifiques pour les principaux actes de cybercriminalité contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques. Pour d´autres formes de cybercriminalité, des délits généraux (non spécifiques à la cybercriminalité) ont été le plus souvent utilisés. Les deux approches ont été mentionnées pour les infractions liées à l´informatique impliquant une violation de la vie privée, la fraude ou la falsification et les infractions liées à l´identité.

Approches nationales de l´incrimination des actes de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité.

Alors qu´existe un haut niveau de consensus en matière d´incrimination, une analyse détaillée des dispositions du droit primaire révèle des approches divergentes. Les délits qui impliquent un accès illégal aux données et aux systèmes informatiques diffèrent quant à l´objet du délit (données, système ou information), et pour ce qui concerne l´incrimination du « seul fait » d´accéder ou l´exigence de plusieurs tentatives pour considérer qu´un dommage ou une perte a été causé. L´intention requise pour qu´il y ait un délit diffère également dans les approches pour l´incrimination de l´interférence des données ou des systèmes informatiques. La plupart des pays requiert que l´interférence soit intentionnelle, alors que d´autres incluent l´interférence imprudente. En ce qui concerne l´interférence des données informatiques, la conduite constituant une interférence va du fait d´endommager ou effacer au fait d´altérer, de supprimer, de saisir ou de transmettre les données. L´incrimination de l´interception illégale varie en fonction du fait que le délit se limite ou ne se limite pas à la transmission des données non publiques, et en fonction du fait que le délit se limite à l´interception « à l´aide de moyens techniques ». Tous les pays n´incriminent pas l´usage abusif d´outils informatiques. Pour les pays qui le font, les différences surgissent en fonction du fait que le délit couvre la possession, la diffusion ou l´utilisation d´un software (tel qu´un logiciel malveillant) et/ou les codes d´accès à l´ordinateur (comme les mots de passe de la victime). En matière de coopération internationale, ces différences peuvent avoir un impact sur les constats de double incrimination entre les pays.

3 Accès illégal a un système informatique ; accès illégal, interception ou acquisition de données informatiques ; interférence illégale de données ou de systèmes informatiques ; utilisation abusive d´outils informatiques ; viol de la vie privée ou des mesures de protection des données ; fraude ou falsification liée à l´informatique ; délit lié à l´informatique concernant l´identité ; délit lié à l´informatique relatif aux droits d´auteur et aux marques déposées ; actes liés à l´informatique causant un préjudice personnel ; actes liés à l´informatique impliquant du racisme ou de la xénophobie ; la production, la distribution ou la possession de pornographie infantile liée à l´informatique ; la sollicitation ou la prédation sexuelle des enfants liée à l´informatique ; actes d´appui au délit de terrorisme liés à l´informatique.

Plusieurs pays ont adopté des délits spécifiques de cybercriminalité dans des cas de fraude liée à l´informatique, de falsification et des délits liés à l´identité. D´autres pays amplifient des dispositions générales sur la fraude ou le vol, ou dépendent de délits qui couvrent les éléments constitutifs – comme l´accès, l´interférence et la falsification des données, dans le cas des délits concernant l´identité. Certains délits liés au contenu, notamment ceux qui concernent la pornographie infantile, sont amplement incriminés. Toutefois, il existe des différences quant à la définition d' « enfant », des limitations relatives au matériel « visuel » ou l´exclusion du matériel simulé et des actes couverts. Même si la majorité des pays incluent, par exemple, la production et la distribution de pornographie infantile, il existe de grandes variations en ce qui concerne l´incrimination de l´accès et de la possession. En matière d´atteinte aux droits d´auteur et aux marques déposées liée à l´informatique, les pays signalent généralement l´application d´infractions pénales générales pour des actes commis délibérément et à une échelle commerciale.

L´utilisation croissante des médias sociaux et les contenus créés par les usagers d´internet ont donné lieu à ce que les gouvernements prennent des mesures de nature réglementaire, et cela inclut l´utilisation du droit pénal et des appels au respect de la liberté d´expression. Les pays qui ont répondu au questionnaire signalent des limites variables pour ce qui concerne la liberté d´expression, y compris en matière de diffamation, d´outrage, de menaces, d´incitation à la haine, d´insulte aux sentiments religieux, de matériel obscène et de porter atteinte à l´état. L´élément socio-culturel de certaines limitations se reflète non seulement dans la législation nationale mais également dans les instruments multilatéraux. Certains instruments régionaux contre la cybercriminalité, par exemple, incluent une vaste gamme de délits relatifs à la violation à la moralité publique, au matériel pornographique, et aux valeurs ou aux principes religieux ou familiaux.

Les lois internationales sur les droits de l´homme servent à la fois d´arme et de bouclier, en requérant l´incrimination de formes extrêmes d´expression, alors qu´elles protègent d´autres formes d´expression. Certaines prohibitions sur la liberté d´expression, comme l´incitation au génocide, l´appel à la haine constituant une incitation à la discrimination, l´hostilité ou la violence, l´incitation au terrorisme et la propagande en faveur de la guerre, sont exigées aux états parties aux instruments internationaux pertinents relatifs aux droits de l´homme. Pour d´autres, la « marge d´appréciation » accorde aux pays de la latitude pour déterminer les limites acceptables de la liberté d´expression en conformité avec leurs propres cultures et traditions juridiques. Toutefois, le droit international relatif aux droits de l´homme interviendra à un certain moment. Les lois pénales sur la diffamation, les insultes et l´outrage à autorité,, par exemple, qui s´appliquent à la liberté d´expression en ligne, feront face à un seuil élevé de limites pour démontrer que les mesures sont proportionnées, appropriées et aussi peu invasives que possible. Si le contenu est illégal dans un pays mais s´il est légal de le produire et de le diffuser dans d´autres pays, les états devront se concentrer sur les mesures de justice pénale dans la juridiction nationale à l´encontre des personnes qui accèdent à ce contenu, plutôt que sur un contenu produit hors du pays.

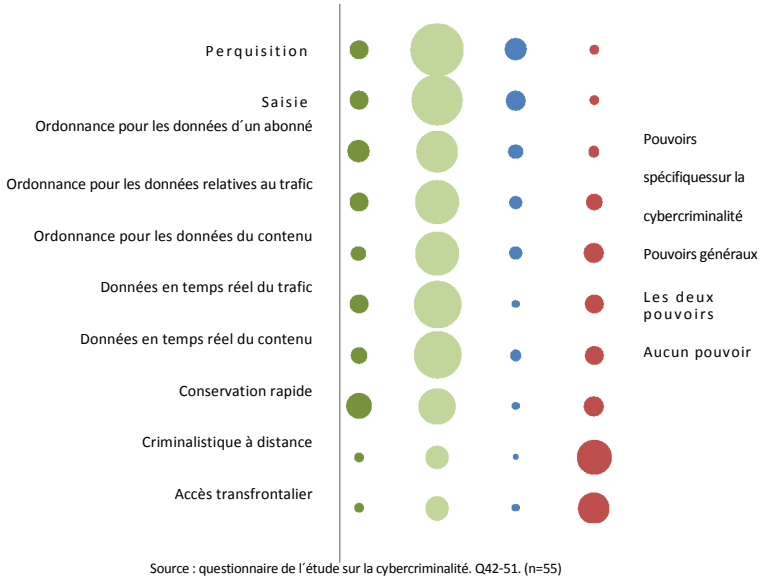
Application des lois et enquêtes

Plus de 90 % des pays qui ont répondu au questionnaire signalent que les autorités d´application de la loi prennent généralement connaissance des actes de cybercriminalité par le biais de rapports présentés par des personnes ou des entreprises qui en sont victimes. Ces pays estiment que la proportion actuelle de la victimisation de la cybercriminalité signalée à la police dépasse 1 %. Une enquête globale du secteur privé suggère que 80 % des personnes qui sont victimes des principaux délits de cybercriminalité ne signalent pas le délit à la police. La sous-déclaration provient d´un manque de sensibilisation en matière de victimisation et de mécanismes de signalement, de la honte et l´embarras ressentis par la victime, et des risques perçus pour leur réputation dans le cas des entreprises. Les autorités dans toutes les régions du monde mettent l´accent sur les initiatives prises, afin d´augmenter les signalements, y compris en ligne ou par le biais de systèmes d´assistance téléphonique pour le signalement, des campagnes publiques de sensibilisation, de liaison avec le secteur privé, et de l´amélioration de la communication et du partage d´informations de la police. Une réponse aux incidents de cybercriminalité doit toutefois être accompagnée d´enquêtes tactiques à long et moyen terme qui se concentrent sur les marchés criminels et les architectes du système criminel. Les autorités d´application de la loi des pays développés se sont engagées dans ce domaine, avec des unités infiltrées qui visent les délinquants sur les sites de réseautage social, les forums de discussion, les messageries instantanées et les services pairs à pairs. Les difficultés des enquêtes sur la cybercriminalité proviennent des innovations criminelles des délinquants, des difficultés d´accès aux preuves électroniques, et des limitations logistiques, en matière de capacité et de ressources internes. Les suspects utilisent

fréquemment des techniques d´anonymisation et d´obfuscation, et les nouvelles techniques se frayent rapidement un chemin auprès d´un vaste public délinquant par le biais des marchés criminels en ligne.

Les enquêtes sur la cybercriminalité menées par les autorités d´application de la loi requièrent la fusion de techniques traditionnelles et de nouvelles techniques policières. Bien que les pouvoirs traditionnels permettent de mettre en œuvre certains mesures d´enquêtes, de nombreuses dispositions de procédure ne se transposent pas aisément d´une approche spatiale et orientée objet à une approche impliquant le stockage de données électroniques et le flux de données en temps réel. Le questionnaire de l´étude mentionne dix mesures d´enquêtes sur la cybercriminalité, allant de la perquisition et la saisie aux pouvoirs spécialisés, comme la conservation des données informatiques.[4] Les pays signalent généralement l´existence de pouvoirs généraux (non spécifiques en matière de cybercriminalité) pour les mesures d´enquêtes. Certains pays signalent également une cyber législation spécifique notamment pour garantir une conservation rapide des données informatiques et pour obtenir des données enregistrées d´abonnés. Plusieurs pays ont signalé l´absence de pouvoirs légaux pour des mesures de pointe, comme la criminalistique informatique à distance. Alors que les pouvoirs traditionnels de procédures peuvent s´appliquer aux situations de cybercriminalité, dans de nombreux cas une telle approche peut également entraîner des incertitudes juridiques et des difficultés relatives à la légalité des preuves recueillies, et donc à la recevabilité des preuves. De plus, les approches nationales en matière de pouvoirs d´enquêtes sur la cybercriminalité ont une base commune moindre qu´en matière d´incrimination de nombreux actes de cybercriminalité.

Approches nationales des mesures d´enquêtes pour la cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité. Q42-51. (n=55)

Indépendamment de la forme juridique des pouvoirs d´enquêtes, toutes les autorités qui ont répondu au questionnaire utilisent la perquisition et la saisie pour l´appropriation physique du matériel informatique et la capture des données informatiques. La majorité des pays utilisent également des ordonnances pour que les fournisseurs de services internet leur transmettent les données informatiques stockées. Toutefois, à l´extérieur de l´Europe près d´un tiers des pays signalent des difficultés pour contraindre les tierces parties à fournir des informations dans une enquête. Environ les trois quarts des pays utilisent des mesures d´enquêtes spécialisées, telles que la collecte des données en temps réel ou la conservation rapide des données. L´utilisation des mesures d´enquêtes exige habituellement un minimum de preuves préliminaires ou le signalement d´un acte de cybercriminalité. Des mesures plus intrusives, comme celles concernant la collecte de données en temps réel ou l´accès au contenu des données, requièrent souvent des preuves du fait de commettre un acte grave, ou de démontrer une cause probable ou des motifs raisonnables.

4 Perquisition pour le matériel ou les données informatiques ; saisie du matériel ou des données informatiques ; ordonnance pour les données des abonnés ; ordonnance pour les données de trafic stockées, collecte des données de trafic en temps réel ; collecte des données du contenu en temps réel ; conservation rapide des données informatiques ; utilisation d´outils de criminalistique à distance ; et accès transfrontalier à des données ou des systèmes informatiques.

Les autorités d´application de la loi et les fournisseurs de services internet ont une interaction particulièrement complexe. Les fournisseurs de services détiennent les informations des abonnés, la facturation, certains journaux de connexion, des informations relatives à la localisation (comme les données de la tour de téléphonie cellulaire pour les fournisseurs de services de téléphonie mobile), et le contenu des communications, qui peuvent représenter des preuves électroniques essentielles d´un délit. Les obligations légales nationales, la rétention des informations du secteur privé et les politiques de divulgation varient beaucoup selon le pays, le type d´industrie et de données. Les pays ont signalé qu´ils utilisent souvent des ordonnances du tribunal pour que les fournisseurs de services leurs transmettent des preuves. Cependant, dans certains cas, les autorités d´application de la loi sont à même d´obtenir directement les données stockées des abonnés, des données de trafic ou des données de contenu. À cet égard, les organisations du secteur privé signalent souvent une politique principale qui exige une procédure légale en bonne et due forme pour divulguer des données, mais également dans certaines circonstances une observation volontaire des demandes présentées par les autorités d´application de la loi. Les relations informelles entre les autorités d´application de la loi et les fournisseurs de services, qui ont été mentionnées par plus de la moitié des pays, facilite le processus d´échange d´informations et de confiance. Les réponses indiquaient qu´il est nécessaire d´équilibrer la vie privée et la procédure régulière, avec une divulgation de la preuve en temps opportun, en veillant à ce que le secteur privé ne devienne pas un obstacle pour les enquêtes.

Les enquêtes sur la cybercriminalité impliquent invariablement des considérations relatives à la vie privée en conformité avec les lois internationales sur les droits de l´homme. Les normes sur les droits de l´homme spécifient que les lois doivent être suffisamment claires et donner des indications adéquates sur les circonstances dans lesquelles les autorités sont habilitées à utiliser des mesures d´enquêtes, et il doit y avoir des garanties adéquates et efficaces contre les abus. Les pays ont mentionné la protection des droits à la vie privée dans les législations nationales, ainsi qu´une gamme de limites et de garanties lors des enquêtes. Cependant, lorsque les enquêtes sont transnationales, l´accès aux données des autorités de détection et de répression étrangères est imprévisible en raison des divergences en matière de niveaux de protection et des potentielles lacunes juridictionnelles des régimes de protection de la vie privée.

Plus de 90 % des pays qui ont répondu au questionnaire ont commencé à mettre en place des structures spécialisées pour enquêter sur la cybercriminalité et sur des délits mettant en cause des preuves électroniques. Cependant, les pays en développement manquent de ressources et de capacités. Les pays avec de bas niveaux de développement disposent de nettement moins de services de police spécialisée, environ 0,2 pour 100 000 utilisateurs nationaux d´internet. Ce taux est de deux à cinq fois plus élevé dans les pays plus développés. Dans les pays moins développés soixante-dix % des officiers spécialisés des services de détection et de répression ont signalé un manque de matériel et d´habilités informatiques, et seulement la moitié reçoit une formation plus d´une fois par année. Plus de la moitié des pays d´Afrique et un tiers des pays d´Amérique qui ont répondu au questionnaire ont signalé que les ressources des services de détection et de répression pour enquêter sur la cybercriminalité étaient insuffisantes. Il est probable que la situation soit pire. Par exemple, l´étude a reçu les réponses de seulement 20 % des 50 pays les moins développés dans le monde. Tous les pays d´Afrique qui ont répondu et plus de 80 % des pays d´Amérique, d´Asie et d´Océanie ont mentionné le besoin d´assistance technique. Le domaine le plus fréquemment cité en matière d´assistance technique était les techniques d´enquêtes générales sur la cybercriminalité. 60 % des pays qui avaient besoin d´une assistance ont indiqué que celle-ci était requise par les services de détection et de répression.

Preuves électroniques et justice pénale

Les preuves sont les faits pertinents au moyen desquels la culpabilité ou l´innocence d´une personne est établie lors d´un procès. Les preuves électroniques comprennent toutes les preuves existant en forme digitale ou électronique. Elles peuvent être stockées ou transitoires. Elles peuvent exister sous la forme de fichiers informatiques, de

transmissions, de journal, de métadonnées ou de données en réseau. La criminalistique numérique se rapporte à la récupération des informations – qui sont souvent volatiles et facilement contaminées –pouvant avoir une valeur probante. Les techniques de criminalistique incluent la création de copies « bit à bit » des informations stockées et effacées, le « blocage d´écriture », afin de garantir que les informations originales ne sont pas altérées, et des « hachages » cryptographiques de fichiers, ou des signatures digitales, qui peuvent révéler des changements dans les informations. Pratiquement tous les pays ont mentionné des capacités de criminalistique numérique. Cependant, divers pays, de toutes les régions du monde, ont signalé un nombre insuffisant d´experts en criminalistique, des différences entre les capacités existantes au niveau fédéral et au niveau étatique, un manque d´outils criminalistiques et des retards causés par d´immenses quantités de données à analyser. La moitié des pays a signalé que les suspects utilisent le cryptage et cela rend difficile l´accès à ce type de preuves et cela prend beaucoup de temps sans la clé de décryptage. Dans la plupart des pays, les autorités des services de détection et de répression sont chargées d´analyser les preuves électroniques. Cependant, les procureurs doivent voir et comprendre les preuves électroniques, afin de monter un cas pour le procès. Tous les pays d´Afriques et un tiers des pays localisés dans d´autres régions signalent que les procureurs n´ont pas les ressources nécessaires pour cela. Les habilités informatiques du parquet sont typiquement inférieures à celles des enquêteurs. Globalement environ 65 % des pays qui ont répondu mentionnent des formes de spécialisation du parquet en matière de cybercriminalité. Seulement 10 % des pays mentionnent des services judiciaires spécialisés. La grande majorité des cas de cybercriminalité est traitée par des juges non spécialisés, qui, dans 40 % des pays, ne reçoivent aucun type de formation en matière de cybercriminalité. La formation judiciaire en matière de lois sur la cybercriminalité, de recueil des preuves, et de connaissance basique et avancée en informatique, représente une priorité particulière.

Plus de 60 % des pays ayant répondu, n´établissent aucune différence juridique entre les preuves électroniques et les preuves physiques. Bien que les approches varient, plusieurs pays considèrent ceci comme une bonne pratique, car cela garantit une recevabilité équitable de tous les autres types de preuves. Plusieurs pays à l´extérieur de l´Europe n´admettent pas les preuves électroniques, et ainsi les poursuites de la cybercriminalité et de tout autre délit impliquant des informations électroniques deviennent irréalisables. Même si en général les pays n´ont pas de règles de preuve distinctes en matière de preuves électroniques, certains pays mentionnent des principes comme : la règle de la meilleure preuve, la pertinence de la preuve, la règle du ouï dire, l´authenticité et l´intégrité, qui peuvent tous s´appliquer aux preuves électroniques. Plusieurs pays mentionnent les difficultés d´attribuer des actes à une personne déterminée et signalent que cela dépend souvent de preuves circonstancielles.

Les difficultés auxquelles font face les enquêteurs et les procureurs signifient que les taux relatifs aux auteurs d´un cyberdélit traduits en justice sont bas. Le taux des suspects identifiés en raison d´une infraction enregistrée par la police est comparable aux délits de pornographie infantile par rapport à d´autres délits sexuels. Toutefois, les personnes identifiées en raison d´une infraction enregistrée et suspectes d´avoir commis des actes tels que l´accès et la fraude ou la falsification liée à l´informatique représentent 25 délits sur 100. Très peu de pays peuvent fournir des données sur les personnes poursuivies ou condamnés. Les calculs relatifs aux délits de cybercriminalité dans un pays montrent que la proportion des personnes condamnées pour ces infractions est significativement inférieure au nombre de personnes condamnées pour des délits « classiques ».

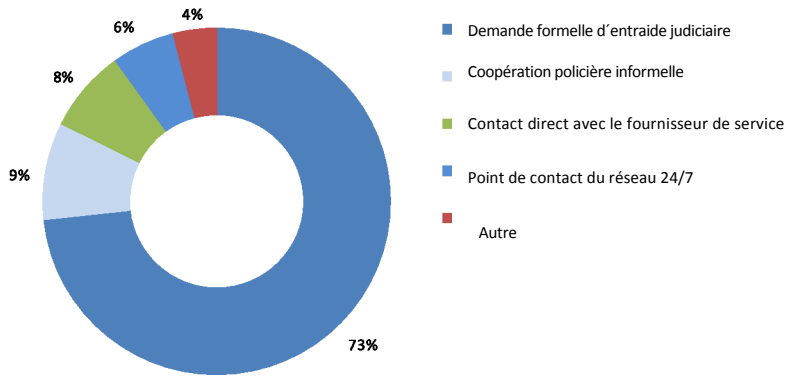
Coopération internationale

Les pays qui ont répondu au questionnaire de l´étude signalent qu´entre 30 et 70 % des actes de cybercriminalité impliquent une dimension transnationale, et met en jeu des questions d´enquêtes transnationales, de souveraineté, de juridiction, de preuves extraterritoriales et de la nécessité de la coopération internationale. La dimension transnationale des délits de cybercriminalité surgit lorsqu´un effet ou un élément important du délit se trouve dans un autre territoire, ou si une partie du *modus operandi* du délit a eu lieu dans un autre territoire. Le droit international prévoit certaines bases de juridiction sur ces actes, y compris des formes de juridiction fondée sur le territoire et de juridiction fondée sur la nationalité. Certaines de ces bases sont également incluses dans les instruments multilatéraux sur la cybercriminalité. Alors que tous les pays d´Europe

considèrent que leurs législations nationales fournissent un cadre juridique suffisant pour l´incrimination et la poursuite des actes de cybercriminalité extraterritoriale, près d´un tiers à un quart des pays localisés dans d´autres régions du monde signalent des cadres juridiques insuffisants. Dans plusieurs pays, les dispositions reflètent l´idée que le délit « complet » doit avoir été commis dans le pays pour faire valoir la juridiction territoriale. Des liens territoriaux peuvent être faits par le biais des effets ou des éléments de l´acte, ou de la localisation des données ou des systèmes informatiques utilisés pour commettre le délit. Les conflits de juridiction qui peuvent surgir sont généralement résolus avec des consultations formelles et informelles entre les pays. Les réponses fournies par les pays ne révèlent actuellement aucun besoin de formes additionnelles de juridictions sur la dimension putative du cyberespace. Les formes de juridiction fondée sur le territoire et de juridiction fondée sur la nationalité sont pratiquement toujours en mesure de garantir une connexion suffisante entre les actes de cybercriminalité et au moins un État.

Les formes de coopération internationale incluent l´extradition, l´entraide judiciaire, la reconnaissance mutuelle des jugements étrangers et la coopération policière informelle. En raison de la nature volatile des preuves électroniques, la coopération internationale en matière pénale dans le domaine de la cybercriminalité requiert des réponses en temps opportun et la capacité de requérir des mesures d´enquêtes spécialisées, comme la conservation des données informatiques. L´utilisation des formes traditionnelles de coopération prédomine lorsqu´il s´agit d´obtenir des preuves extraterritoriales dans des affaires de cybercriminalité, et plus de 70 % des pays ont signalé l´utilisation de demandes formelles d´entraide judiciaire à cette fin. Dans le cadre de la coopération formelle, près de 60 % des demandes utilisent les instruments bilatéraux comme base juridique. Les instruments multilatéraux sont utilisés dans 20 % des cas. Les délais de réponse des mécanismes formels est de plusieurs mois pour les demandes d´extradition et d´entraide judiciaire, et ce délai complique la collecte de preuves électroniques volatiles. Soixante % des pays d´Afrique, d´Amérique et d´Europe, et 20 % des pays d´Asie et d´Océanie, mentionnent des voies pour les demandes urgentes. Toutefois, leur impact sur le délai de réponse n´est pas clair. Des modalités de coopération informelle sont possibles pour près des deux tiers des pays, bien que peu de pays aient une politique relative à l´utilisation de ces mécanismes. Les initiatives concernant la coopération informelle et visant à faciliter la coopération formelle, comme les réseaux 24/7, offrent un potentiel important pour des délais de réponse plus rapides. Ils sont cependant peu utilisés, et représentent environ trois % du nombre total de cas de cybercriminalité traités par les autorités répressives du groupe de pays déclarants.

Moyens d´obtenir des preuves extraterritoriales



Source : questionnaire de l´étude sur la cybercriminalité .Q105. (n=56, r=221)

Les modalités formelles et informelles de coopération sont conçues pour gérer le processus de consentement de l´état relatif à des enquêtes menées par des services répressifs étrangers qui affectent la souveraineté d´un état. Cependant, les enquêteurs ont de plus en plus accès, sciemment ou non, à des données extraterritoriales lors de la collecte de preuves, sans le consentement de l´état où ces données sont physiquement situées. Cette situation survient en raison des technologies de l´informatique en nuage impliquant le stockage des données dans de multiples centres de données dans divers emplacements géographiques. La « localisation » des données, bien qu´il soit techniquement possible de la connaître, devient de plus en plus artificielle, dans la mesure où même les demandes traditionnelles d´entraide judiciaire sont souvent adressées au pays où se trouve le siège du fournisseur de services, plutôt qu´au pays où se trouve physiquement le centre de données. L´accès direct aux données extraterritoriales des services répressifs étrangers peut avoir lieu lorsque les enquêteurs utilisent la connexion en direct existante du dispositif d´un suspect, où lorsque les enquêteurs utilisent des identifiants d´accès aux données légalement obtenues.

Les enquêteurs des services répressifs peuvent parfois obtenir des données des fournisseurs de services extraterritoriaux par le biais d´une demande directe informelle, bien que les fournisseurs de services requièrent généralement une procédure légale en bonne et due forme. Les dispositions pertinentes existantes sur l´accès « transfrontalier » incluses dans la Convention sur la Cybercriminalité du Conseil de l´Europe et la Convention sur la lutte contre les infractions portant sur les technologies de l´information de la Ligue des états arabes ne couvrent pas ces situations de manière adéquate, car elles se basent sur le « consentement » de la personne qui est légalement autorisée à divulguer ces données et sur la connaissance présumée de la localisation des données au moment de l´accès ou de la réception.

La situation actuelle de la coopération internationale est exposée à l´émergence de groupements de pays ayant les procédures et les pouvoirs nécessaires pour coopérer entre eux, mais limités, pour tous les autres pays, aux modalités « traditionnelles » de coopération internationale qui ne tiennent pas compte des spécificités des preuves électroniques et de la nature globale de la cybercriminalité. Ceci est particulièrement vrai pour la coopération dans le cadre des mesures d´enquêtes. L´absence d´une approche commune, y compris parmi les instruments multilatéraux sur la cybercriminalité, signifie que les demandes de mesures, comme, par exemple, la rapide conservation des données hormis les pays soumis à des obligations internationales de garantir ce service et de les mettre à disposition sur demande, peuvent ne pas être facilement satisfaites. L´inclusion de ce pouvoir dans le projet de Convention sur la cybersécurité de l´Union Africaine pourrait contribuer à combler cette lacune. Globalement, les divergences sur la portée des dispositions relatives à la coopération dans les instruments bilatéraux et multilatéraux, une absence d´obligation en matière de délai de réponse, une absence d´accords relatifs à l´accès direct autorisé aux données extraterritoriales, les multiples réseaux informels des services d´application de la loi, et les variations de garanties en matière de coopération, représentent des difficultés non négligeables pour une coopération internationale efficace pour ce qui concerne les preuves électroniques dans des affaires pénales.

Prévention de la cybercriminalité

La prévention des délits inclut des stratégies et des mesures qui visent à réduire les risques de commettre des délits, et à atténuer les potentiels effets nocifs sur les personnes et la société. Près de 40 % des pays qui ont répondu ont signalé l´existence de politiques ou de lois nationales sur la prévention de la cybercriminalité. Des mesures sont en cours dans près de 20 % des pays. Les pays ont souligné que les bonnes pratiques en matière de prévention de la cybercriminalité incluent la promulgation de la législation, un leadership efficace, le développement de la capacité d´application de la loi et de justice pénale, l´éducation et la sensibilisation, le développement d´une solide base de connaissance, et la coopération entre le gouvernement, les communautés, le secteur privé et au niveau international. Plus de la moitié des pays a signalé l´existence de stratégies contre la cybercriminalité. Dans plusieurs cas les stratégies contre la cybercriminalité sont incorporées aux stratégies de cybersécurité. Près de 70 % de tous les pays ont mentionné des stratégies nationales qui incluaient des éléments de sensibilisation, de coopération internationale et de capacité d´application de la loi. À des fins de coordination, les organismes de poursuites et d´application de la loi sont le plus souvent signalés comme les principales institutions de lutte contre la cybercriminalité.

Les enquêtes, y compris dans les pays développés, démontrent que la plupart des utilisateurs d´internet prend maintenant des précautions basiques de sécurité. L´importance constante des campagnes de sensibilisation publiques, y compris celles qui abordent les menaces émergentes et celles qui visent des audiences spécifiques, comme, par exemple, les enfants, a été soulignée par les gouvernements, les entités du secteur privé et les institutions académiques. L´éducation fournie aux utilisateurs est plus efficace si elle est combinée à des systèmes qui

aident les utilisateurs à accomplir leurs objectifs de manière sûre. Si le coût d´usage est plus élevé que le bénéfice direct des usagers, les personnes ont de petits incitatifs pour suivre les mesures de sécurité. Les entités du secteur privé signalent également que la sensibilisation des employés et des utilisateurs doit être intégrée dans une approche holistique de la sécurité. Les principes fondamentaux et les bonnes pratiques incluent la responsabilité d´agir en conscience, des pratiques et des politiques sur la gestion des risques, le leadership au niveau du conseil d´administration, et la formation du personnel.

Deux tiers des répondants du secteur privé ont effectué des évaluations de risques en matière de cybercriminalité et la plupart a signalé l´utilisation de techniques de cybersécurité comme les pare-feu, la conservation des preuves digitales, l´identification du contenu, la détection des intrusions, et la surveillance et le contrôle du système. Ils ont cependant mentionné qu´il était préoccupant que les petites et moyennes entreprises ne prennent pas suffisamment de mesures pour protéger les systèmes, en supposant de manière erronée qu´elles ne seront pas une cible.

Les cadres règlementaires ont un rôle important à jouer dans la prévention de la cybercriminalité, pour ce qui concerne le secteur privé en général et les fournisseurs de services en particulier. Près de la moitié des pays a adopté des lois sur la protection des données, avec des exigences spécifiques relatives à la protection et l´utilisation des données personnelles. Certains de ces régimes incluent des exigences spécifiques relatives aux fournisseurs de services internet et à d´autres fournisseurs de communications électroniques. Bien que les lois sur la protection des données exigent que les données personnelles soient éliminées dès qu´elles ne s´avèrent plus nécessaires, certains pays ont fait des exceptions à des fins d´enquêtes pénales, en demandant à des fournisseurs de services internet de stocker des types spécifiques de données pour un certain temps. Plusieurs pays développés ont également des règles qui exigent que les organisations notifient les violations de données aux individus et aux organismes de règlementation. Les fournisseurs de services iinternet ont généralement une responsabilité limitée en tant que « simples conduits » de données. Les modifications du contenu transmis accroissent la responsabilité, ainsi que la connaissance réelle ou présumée d´une activité illégale. D´autre part, des mesures expéditives prises après la notification réduisent la responsabilité. S´il existe des possibilités techniques pour les fournisseurs de services de filtrer le contenu d´internet, les restrictions en matière d´accès à internet sont soumises à des exigences de proportionnalité et de prévisibilité en conformité avec les lois internationales sur les droits de l´homme qui protègent le droit de rechercher, recevoir et transmettre des informations.

Les partenariats public-privé sont essentiels pour la prévention de la cybercriminalité. Près de la moitié de tous les pays a mentionné l´existence de partenariat. Ceux-ci sont créés en nombre égal par le biais d´accords informels et sur des bases légales. Les entités du secteur privé sont le plus souvent impliquées dans des partenariats, suivies par les institutions académiques et les organisations régionales et internationales. Les partenariats sont souvent utilisés pour faciliter l´échange d´informations sur les tendances et les menaces, mais également dans le cadre des mesures et des activités de prévention dans des cas spécifiques. Dans le contexte de certains partenariats public-privé, les entités du secteur privé ont pris des approches proactives pour enquêter et prendre des mesures légales contre des opérations de cybercriminalité. Ces mesures complètent les mesures prises par les services répressifs et peuvent aider à atténuer les préjudices causés aux victimes. Les institutions académiques jouent différents rôles dans la prévention de la cybercriminalité, avec la prestation de services d´éducation et de formation aux professionnels, le développement de politiques et de lois, et des travaux sur les normes techniques et le développement de solutions. Les universités disposent et fournissent des experts en cybercriminalité, des équipes d´intervention informatique d´urgence (CERT) et des centres de recherche spécialisés.

Page intentionnellement laissée vierge

CHAPITRE PREMIER : la connectivité et la cybercriminalité

Ce chapitre examine les effets de la révolution de la connectivité globale en matière de cybercriminalité, et reconnait dans la cybercriminalité un défi contemporain croissant provoqué par une série de facteurs socio-économiques sous-jacents. Il examine les définitions de la cybercriminalité et en conclut que si certaines définitions sont requises pour les « principaux » actes de cybercriminalité, le concept global n´est pas adapté en tant que notion juridique.

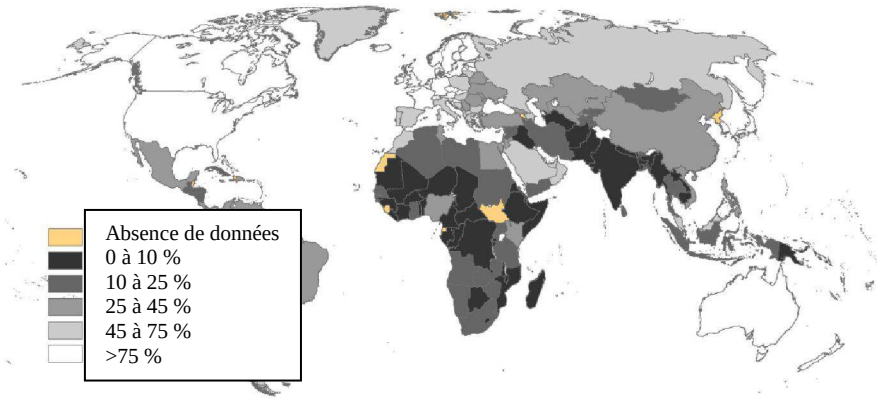
1.1 La révolution de la connectivité globale

Principaux résultats :

- en 2011, plus d´un tiers du total de la population mondiale avait accès à l´internet ;
- plus de 60 % du total des utilisateurs d´internet se trouvait dans des pays développés, et 45 % du total des utilisateurs d´internet avait moins de 25 ans ;
- on estime que le taux d´abonnement au haut débit atteindra 70 % du total de la population mondiale d´ici à l´année 2017 ;
- on estime que les dispositifs en réseau (l´internet des objets) seront 6 fois plus nombreux que les personnes, et cela transformera les conceptions actuelles de l´internet ;
- dans le monde hyper connecté de demain il sera difficile de concevoir un « délit informatique », et peut être n´importe quel délit, n´impliquant pas des preuves électroniques liées à la connectivité du protocole internet (IP).

En 2011, **au moins 2,3 milliards de personnes, l´équivalent de plus d´un tiers de la population mondiale, ont eu accès à l´internet. Les pays développés jouissent de niveaux plus élevés d´accès à l´internet (70 %) que les pays en développement (24 %). Cependant, le nombre absolu d´utilisateurs d´internet dans les pays en développement dépasse déjà de loin celui des pays développés. 62 % du nombre** total des utilisateurs d´internet se trouvait dans des pays en développement en 2011.

Dans les pays développés et les pays en développement, il y a plus de jeunes utilisateurs que des utilisateurs plus âgés en ligne puisque 45 % de tous les utilisateurs de l´internet ont moins de 25 ans[1] – un segment démographique qui correspond également à une tranche d'âge présentant un risque particulier de commettre une infraction pénale.[2]

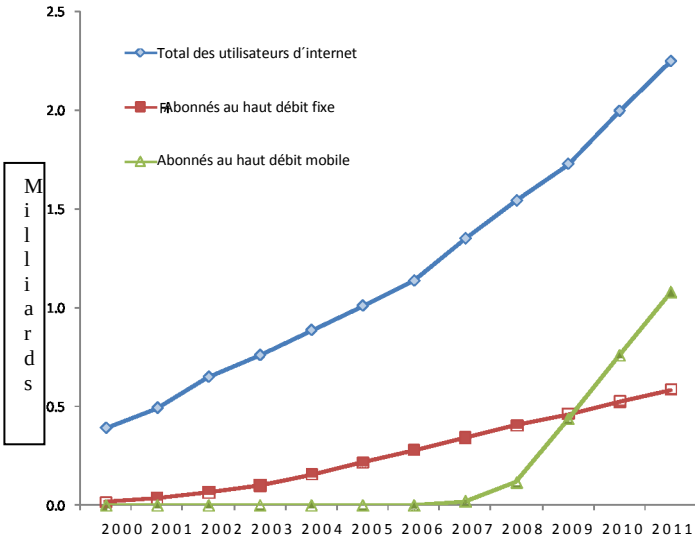


Source : élécommunications dans le monde /indicateurs des TIC 2012

La croissance de l´accès mobile à l´internet

Il existe environ 1,2 milliard d´abonnement au haut débit mobile. Ceci représente le double des abonnements au haut débit sur lignes fixes, et correspond à environ 16 % de la population globale.[3] En 2009, le volume du trafic de données mobiles globales a dépassé le volume du trafic de voix mobile. Le trafic de données mobiles globales en 2011 était quatre fois plus élevé que le trafic de voix mobile.[4]

Figure 1.2 : connectivité globale à l´internet 2000 - 2011



Source : UIT Télécommunications dans le monde. Indicateurs des TIC 2012

L´Afrique et les états arabes montrent des ratios particulièrement élevés entre le haut débit mobile et le haut débit fixe, qui reflètent le lancement des services et des réseaux 3G+ mobiles à haute vitesse dans ces régions, conjugué à la croissance des dispositifs portables, y compris les smartphones et les tablettes électroniques. D´ici à l´année 2017, on estime que la technologie mobile GSM/EDGE[5] couvrira plus de 90 % de la population mondiale, et que 85 % de la population aura accès à la technologie mobile WCDMA/HSPA[6], avec un débit pouvant atteindre 2Mb par seconde. Les prévisions suggèrent que le nombre d´abonnement au haut débit mobile atteindra cinq milliards d´ici à l´année 2017. En 2011, le nombre de dispositifs en réseau – appelés « l´internet des objets » – a dépassé le nombre total de la population mondiale. D´ici à l´année 2020, les dispositifs en réseau seraient 6 fois plus nombreux que les personnes connectées, et cela transformera les conceptions actuelles de l´internet.[7] Alors que les personnes connectées ont actuellement un ou deux dispositifs connectés à l´internet (en général un ordinateur et un téléphone intelligent), d´ici à l´année 2015 cela pourrait être sept dispositifs connectés à l´internet.[8] Dans « l´internet des objets, » des objets tels que des appareils ménagers, des véhicules, des compteurs électriques et des compteurs d´eau, des médicaments ou même des effets personnels comme des vêtements, pourraient avoir la capacité d´avoir une adresse IP assignée, de s´identifier eux-mêmes et de communiquer en utilisant des technologies comme RFID et NFC.[9]

---

1 Union internationale des télécommunications, 2012. *Mesurer la société de l´information, et base de données sur les indicateurs des télécommunications /TIC dans le monde.*
Voir également Moore, R., Guntupalli, N.T., et Lee, T., 2010. Contrôle parental et activités en ligne : Examen des facteurs qui influent pour qu´un jeune devienne la victime d´un harcèlement en ligne. *Journal international de cybercriminologie,* 4(1&2) :685–698.

2 Commission européenne, 2012. *Eurobaromètre spécial 390 : rapport sur la Cybersécurité.* Voir également Fawn, T. et Paternoster, R., 2011. Victimisation de la cybercriminalité : un examen des facteurs au niveau individuel et conjoncturel. *Journal international de cybercriminologie,* 5(1) :773-793, 782.

3 Union internationale des télécommunications, 2012. *Mesurer la société de l´information, et base de données sur les indicateurs des télécommunications /TIC dans le monde.*

4 Ericsson, 2012. Rapport sur le marché et le trafic.

5 Système mondial de communications mobiles/taux de données améliorées pour l´évolution globale GSM ou EGPRS.

6 accès multiple par répartition de codes à large bande/accès par paquets à haute vitesse.

7 Union internationale des télécommunications, 2012. *L´état du haut débit en 2012 : atteindre l´inclusion numérique pour tous.*

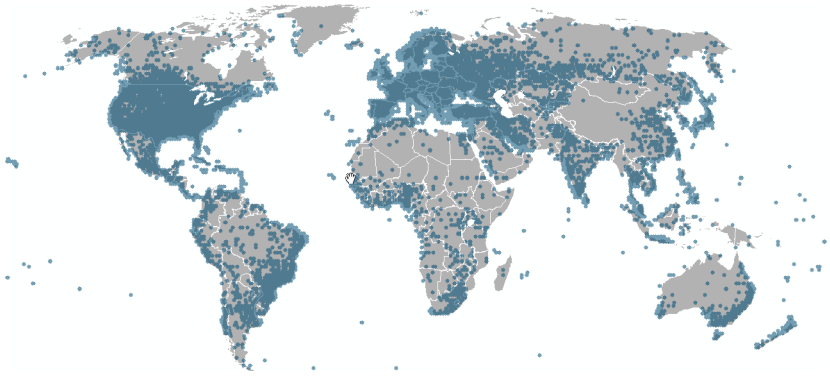
8 Commission européenne, 2012. *Agenda numérique : consultation de la Commission sur les règles concernant les dispositifs connectés sans fil – l´iinternet des objets ».* Disponible sur :
http ://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTGovernance

9 Identification par radiofréquence et communication en champ proche.

La fracture numérique persistante

Les inégalités en matière d´accès à l´internet sont clairement illustrées en recensant les géolocalisations des adresses IP globales. Ceci fournit une estimation raisonnable de la couverture géographique de l´internet. Alors que la densité des adresses IP suit en grande mesure la densité de la population globale, de nombreux emplacements peuplés dans les pays en développement montrent une faible disponibilité de connexion à l´internet. Des disparités en Asie méridionale et orientale, en Amérique centrale et en Afrique notamment démontrent l´actuelle fracture numérique. Vers la moitié de l´année 2012, 341 millions de personnes en Afrique subsaharienne vivaient à plus de 50 km d´un réseau terrestre de fibres optiques– un nombre supérieur à la population des États-Unis d´Amérique.[10] Comme l´a signalé la Commission sur les larges bandes pour le développement numérique établie par l´UIT et l´UNESCO, les régions qui ne sont pas connectées à l´internet perdent une occasion sans précédent de bien-être social et d´opportunités économiques. La Banque mondiale estime qu´une augmentation de 10 % du taux de pénétration du haut débit pourrait apporter, en moyenne, une augmentation de 1,38 % de la croissance du PIB des pays à revenu faible et intermédiaire.[11]

Figure 1.3 : géolocalisation des IP(2012)



Source : ONUDC élaboration de MaxMind GeoCityLite.

Il s´est avéré que le haut débit mobile a un impact plus élevé sur la croissance du PIB que le haut débit fixe car cela réduit les inefficacités.[12] Outre la croissance économique, l´internet permet l´accès à des services essentiels pour les plus isolés en matière d´éducation, de santé et de gouvernance électronique.

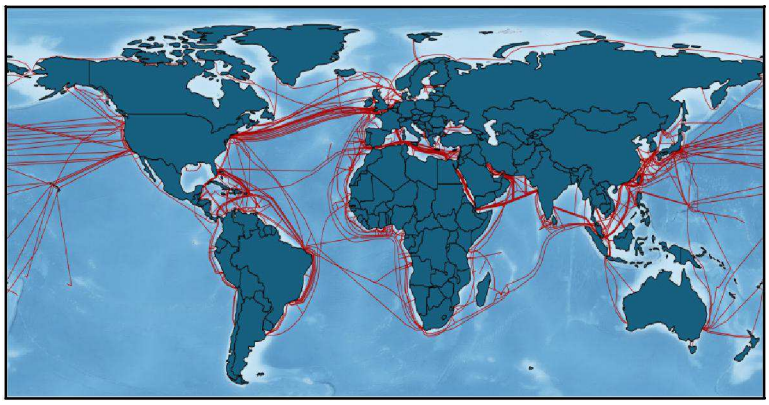
Le rôle du secteur privé

Le secteur privé possède et opère une proportion importante des infrastructures d´internet. L´accès à iinternet exige une infrastructure « passive » de tranchées, de conduits, de fibre optique, de stations de base mobile et de matériel satellitaire. Il exige également une infrastructure « active » consistant en du matériel électronique et un « service » qui consiste en des contenus, des services et des applications.[13] Les grandes ISP mondiales, comme AT&T, NTT Communications, Sprint, Telefonica, et Verizon, possèdent ou louent le transport de fibres optiques inter ou intracontinentales de haute capacité (la dorsale internet) ainsi que d´autres infrastructures essentielles d´internet, comme les commutateurs et les routeurs. Les réseaux ISP sont connectés de manière bilatérale, à des points concentrés (connus comme des points d´interconnexion internet ou IXP). Les principaux réseaux négocient entre eux des *accords d´échange de trafic*, par le biais desquels chacun d´entre eux convient de transporter le trafic des autres – et ceci leur permet de fournir à leurs clients des connexions globales rapides. Le transport de données est payant pour ceux qui n´appartiennent pas au réseau de pairs. Les opérateurs de téléphonie mobile et les ISP locaux possèdent ou gèrent le réseau de cellules radio et de câbles locaux qui assurent le dernier trajet d´internet depuis le serveur jusqu´aux dispositifs portables ou de bureau. L´annexe quatre de cette étude contient des détails supplémentaires sur l´infrastructure d´ internet.

10 Organisation des télécommunications du Commonwealth, 2012. *L´impact socio-économique du haut débit en Afrique subsaharienne : l´avantage du satellite.*.
11 Banque mondiale, 2009. *Informations et communications pour le développement : étendre leur rayon d´action et accroitre leur impact.*
12 Banque mondiale, 2012. *Informations et communications pour le développement : Maximiser la plate-forme mobile.*
13 Union internationale des télécommunications, 2012. *L´état du haut débit en 2012 : atteindre l´inclusion numérique pour tous.*

Les opérateurs internationaux cherchent à établir de vastes bases commerciales, et à maximiser l´efficacité et le rendement des investissements d´infrastructures, et on observe ces dernières années une convergence des technologies de l´information et dela communicationtraditionnellement distinctes, et des services web.[14] les réseaux de télécommunications sont tous en train de devenir des réseaux de données IP, avec des produits standardisés et une interconnectivité plus simple. L´augmentation de l´informatique et du stockage en nuage permettra que les mêmes contenus et services aux utilisateurs soient fournis aux dispositifs des utilisateurs, comme un téléphone portable, un ordinateur de bureau ou une tablette électronique.

Figure 1.4 : câbles sous-marins globaux



Source : ONUDC élaboration des données de http://www.cablemap.info/

La technologie IP réduit généralement le coût des exploitations commerciales de réseau. Toutefois, le coût de la bande passante internationale peut encore varier énormément, en fonction des élasticités de l´offre et de la demande. Jusqu´à ce que, par exemple, le câble sous-marin ACE (de la côte africaine àl'Europe) devienne totalement opérationnel, les pays dAfrique de l´ouest continuent à supporter les coûts de connectivité à internet les plus élevés du monde, car ils dépendent exclusivement de la bande passante commerciale satellitaire. [15]

En tant qu´infrastructure, la croissance d´internet peut être comparée au développement des routes, des chemins de fer et de l´électricité qui dépendent des investissements, de la construction et de la maintenance du secteur privé, mais qui sont régulés et stimulés par les gouvernements nationaux. Par ailleurs, l´internet est souvent considéré comme étant dirigé par le secteur privé. En collaborant avec le secteur privé, les gouvernements peuvent offrir un leadership des politiques publiques et faciliter la croissance d´internet avec des investissements directs pour les infrastructures et les services, en mettant en place des politiques qui promeuvent la concurrence et qui éliminent les obstacles à l´investissement, et en offrant des incitatifs aux entreprises qui déploient des services internet. [16]

1.2 La cybercriminalité contemporaine

Principaux résultats :

- le délit lié à l´informatique est un phénomène établi de longue date, mais la croissance de la connectivité globale est étroitement liée au développement de la cybercriminalité actuelle ;
- les activités de cybercriminalité actuelles utilisent surtout des technologies de l´information et de la communication globalisées pour commettre des actes criminels ayant une portée transnationale ;
- certains cyberdélits sont commis en utilisant des systèmes informatiques autonomes ou fermés, bien que cela soit beaucoup moins fréquent.

14 Forum économique mondial, 2012. *Rapport mondial sur les technologies de l´information2012 : vivre dans un monde hyperconnecté.*

15 Organisation des télécommunications du Commonwealth, 2012. L´impact socio-économique *du haut débit en Afrique subsaharienne : l´avantage du satellite.*.

16 Forum économique mondial, 2012. *Rapport mondial sur les technologies de l´information2012 : vivre dans un monde hyperconnecté.*

Outre ses bénéfices socio-économiques, il ne fait aucun doute que la technologie informatique et l´internet – ainsi que d´autres moyens pour améliorer les interactions humaines – peuvent être utilisés pour réaliser des activités criminelles. Bien que la criminalité informatique ou les délits liés à l´informatique soient un phénomène établi de longue date, la croissance de la connectivité globale est inhérente à la cybercriminalité contemporaine.

Les actes de cybercriminalité qui incluent les dommages physiques causés aux systèmes informatiques et aux données stockées ;[17] l´utilisation non autorisée des systèmes informatiques et la manipulation des données électroniques ;[18] les fraudes informatiques ;[19] et le piratage de logiciel [20] ont été reconnus comme des délits pénaux depuis les années 1960.

En 1994, le Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique signalait que la manipulation informatique ; la falsification informatique ; les dommages ou les modifications des programmes ou des données informatiques ; l´accès non autorisé aux services et aux systèmes informatiques ; et la reproduction non autorisée des programmes informatiques protégés par la loi, étaient des formes courantes de criminalité informatique.[21]

Si de tels actes sont souvent considérés comme des délits à l´échelle locale pour ce qui concerne les systèmes fermés ou autonomes, la dimension internationale de la criminalité informatique et de la législation pénale connexe a été reconnue dès 1979. Une présentation sur la fraude informatique lors du troisième symposium d´Interpol sur les fraudes internationales, qui s´est tenu du 11 au 13 décembre 1979, soulignait que « *la nature de la criminalité informatique est internationale, en raison de l´augmentation constante des communications par téléphones, satellites etc., entre les différents pays* ».[22]

Le concept fondamental de la cybercriminalité contemporaine demeure exactement semblable à l´idée que la technologie globale convergente de la communication et de l´information peut être utilisée pour commettre des actes criminels d´une portée internationale.

Ces actes peuvent inclure tous les délits liés à l´informatique cités précédemment, et bien d´autres encore, comme les délits liés au contenu informatique ou au contenu internet, [23] ou des infractions informatiques pour des bénéfices personnels ou financiers.[24] Comme l´établit le présent chapitre, cette étude ne « définit » pas la cybercriminalité contemporaine comme telle. Elle la caractérise plutôt comme une liste d´actes qui constituent des délits de cybercriminalité. Néanmoins, il est clair que l´accent est mis sur le mauvais usage des TIC à partir d´une perspective globale. Plus de la moitié des pays répondants ont signalé qu´entre 50 et 100 % des actes de cybercriminalité enregistrés par la police incluaient un élément international.[25] Les pays répondants qualifiaient la cybercriminalité de *« phénomène global »* et signalaient que *« les communications en ligne impliquaient invariablement des dimensions internationales ou transnationales »*.[26]

Mettre l´accent sur la connectivité globale n´exclut pas du champ de la cybercriminalité les délits commis sur des systèmes informatiques fermés ou autonomes.[27] Il est intéressant de noter qu´alors que les agents des services répressifs des pays développés signalent généralement une proportion élevée de cyberdélits comprenant un élément transnational, les agents des services répressifs des pays en développement tendent à identifier une proportion beaucoup plus faible – moins de 10 % dans certains cas.[28] Ceci peut indiquer que dans les pays en développement les auteurs de cyberdélits se concentrent davantage sur des victimes locales et sur les systèmes informatiques (probablement autonomes). D´autre part, il est possible que, en raison des problèmes de capacité, les agents des services répressifs des pays en développement identifient, ou entrent rarement en relation avec les fournisseurs de service étrangers ou les potentielles victimes liés à des cas nationaux.

17 Pour ce qui concerne ces difficultés, voir Slivka, R.T., et Darrow, J.W., 1975. Méthodes et Problèmes en matière de sécurité informatique. *Journal Rutgers sur le droit et l´informatique,* 5 :217.

18 Congrès des États Unis, 1977. *Bill S.1766, Loi fédérale sur la protection des systèmes informatiques,* 95ièmeCongrès, 1ère Session., 123 Cong. Rec.20, 953 (1977).

19 Glyn, E.A., 1983. Abus informatique : la criminalité émergente et le besoin de législation. *Journal juridique urbain de Fordham*, 12(1) :73-101.

20 Schmidt, W.E., 1981. Droits de propriété légaux dans les programmes informatiques : l´expérience américaine. *Journal jurimétrique,* 21 :345.

21 Nations Unies, 1994. *Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique.*

22 INTERPOL, 1979. *Troisième symposium d´Interpol sur les fraudes internationales,* Paris 11-13 décembre 1979.

23 En incluant les délits liés à l´informatique concernant le racisme ou la xénophobie, ou la production, la distribution ou la possession de pornographie infantile liée à l´informatique.

24 En incluant les délits liés à l´informatique concernant l´identité et les délits liés à l´informatique relatif aux droits d´auteur et aux marques déposées.

25 Questionnaire de l´étude sur la cybercriminalité Q83.

26 *Ibid.*27 Certaines approches considèrent que la cybercriminalité se restreint aux délits « lié à l´informatique », dans la mesure où un cyberdélit requiert un réseau informatique – et cela exclut donc les délits commis en utilisant un système informatique fermé ou autonome. Bien que mettant l´accent sur la connectivité, la présente étude n´exclut pas du champ de la cybercriminalité les systèmes informatiques fermés ou autonomes. Le terme « cybercriminalité » est donc utilisé pour décrire une gamme de délits qui incluent les délits informatiques classiques ainsi que les délits de réseau.

Néanmoins, la réalité de la connectivité globale doit être considérée comme un élément central de la cybercriminalité contemporaine et, notamment, de la cybercriminalité de demain. Dans la mesure où le trafic Ip et le cyberespace augmentent, [29] où le trafic des dispositifs est supérieur au trafic des dispositifs câblés et où davantage de trafic internet provient de dispositifs autres que des ordinateurs, il devient difficile d´imaginer un délit « informatique » sans l´élément de la connectivité IP. Le caractère personnel des dispositifs mobiles et l´émergence des effets personnels ou des appareils ménagers connectés au réseau IP, signifient que les transmissions et les données électroniques pourraient être générés par, ou devenir partie intégrante de presque toutes les activités humaines – légale ou illégales.

1.3 La cybercriminalité comme un défi croissant

Principaux résultats :

- en raison des difficultés pour essayer de définir et d´identifier la cybercriminalité, les statistiques comparatives transnationales sur la cybercriminalité sont beaucoup plus rares que pour d´autres types de délits ;
- au niveau international, les services répressifs qui ont répondu à l´étude signalent des niveaux croissants de cybercriminalité, car les individus et les groupes criminels organisés, motivés par les profits et les gains personnels exploitent de nouvelles possibilités criminelles ;
- la cybercriminalité attire de plus en plus l´attention publique car il y a une augmentation de la couverture médiatique concernant des affaires de cybercriminalité, des questions de cybersécurité et d´autres nouvelles liées à l´informatique ;
- les théories criminologiques et les approches socio-économiques offrent de possibles explications à la récente augmentation des activités de cybercriminalité ;
- dans de nombreux pays dans toutes les régions, l´explosion de la connectivité globale est survenue à un moment de transformations économiques et démographiques, avec une disparité croissante des revenus, une contraction des dépenses du secteur privé et une liquidité financière réduite.

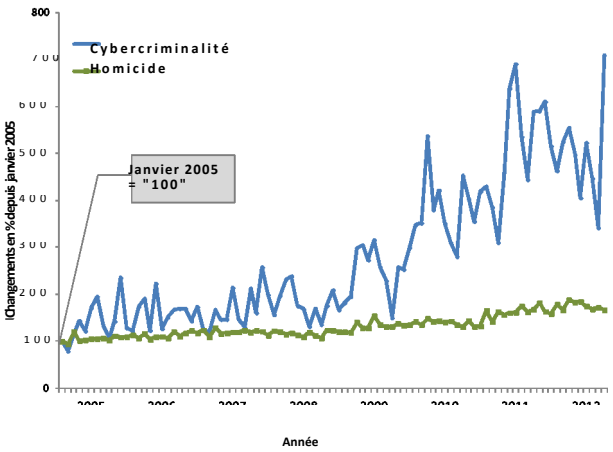
Avec l´omniprésence croissante de la connectivité globale les taux de cybercriminalité risquent d´augmenter. Bien qu´il soit difficile d´obtenir des statistiques fiables, plusieurs pays qui ont répondu à l´étude ont signalé que la cybercriminalité constitue un défi croissant – un point de vue plausible au regard des facteurs socio-économiques et criminologiques sous-jacents. Par exemple, un des pays répondants en Europe, a signalé que : « *en se basant sur la recherche et les statistiques principalement fournis par le secteur privé ou le milieu universitaire, il est communément admis que les actes de cybercriminalité sont en pleine recrudescence, avec des pouvoirs limités pour les contrôler* ».[30] La Déclaration de Salvador de 2010 sur des stratégies globales pour faire face aux défis mondiaux, annexée à la résolution de l´Assemblée générale 65/230, signalait que « *le développement des technologies de l´information et de la communication et l´utilisation croissante d´internet créent de nouvelles opportunités pour les délinquants et facilitent la croissance de la criminalité* ».[31]

28 Questionnaire de l´étude sur la cybercriminalité. Q83.
29 En 2016, le gigaoctet équivalant à tous les films réalisés traversera les réseaux mondiaux IP toutes les 3 minutes. Cisco, 2012. *Indice de réseautage visuel de Cisco, 2011-2016*.
30 Questionnaire de l´étude sur la cybercriminalité. Q84.

En raison d´importantes difficultés pour mesurer la cybercriminalité, les statistiques comparatives transnationales sur la cybercriminalité sont beaucoup plus rares que pour d´autres types de délits.[32] L´Annexe deux de la présente étude examine les approches méthodologiques actuelles utilisées pour mesurer la cybercriminalité et présente quelques-unes des rares statistiques disponibles.

Lors de ces cinq dernières années notamment, la question de la cybercriminalité a figuré à l´avant plan de la discussion publique, y compris dans les pays en développement. Une recherche au niveau mondial des agences de presse pour les termes « cybercriminalité » et « homicide », dans les six langues officielles des Nations Unies, révèle une importante croissance relative dans la fréquence des informations du monde entier qui concernent la cybercriminalité, en comparaison avec les références à l´homicide. Entre les années 2005 et 2012, les références à la cybercriminalité ont augmenté jusqu´à 600 % et d´environ 80 % dans le cas des références à l´homicide.[33] Ces mesures ne sont pas directement liées aux actes sous-jacents de cybercriminalité. Elles peuvent néanmoins refléter une activité globale relative à la cybercriminalité – y compris les reportages des média sur les initiatives et les mesures de lutte du gouvernement.

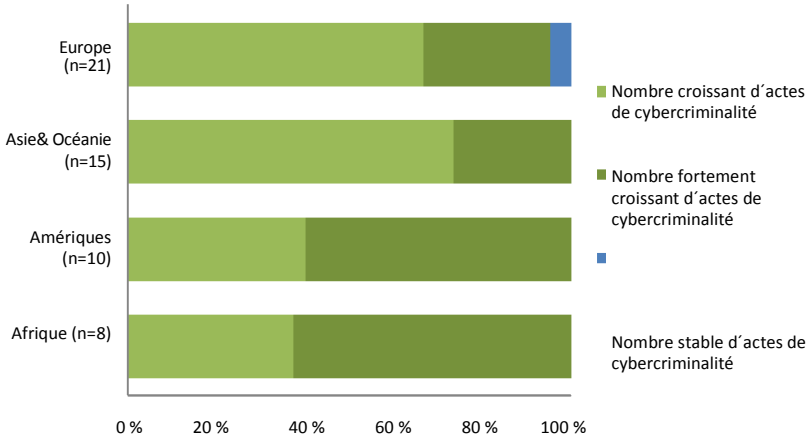
Figure 1.5 : fréquence relative des informations au niveau mondial 2005-2012



Source : ONUDC estimations de Dow Jones Factiva.

Le point de vue des agents des services répressifs reflète également un consensus sur l´augmentation des niveaux de cybercriminalité. Pour ce qui concerne les tendances en matière de cybercriminalité qu´ils ont observées dans leur propre pays lors des cinq dernières années, tous les agents des services répressifs de 18 pays d´Afrique et d´Amérique ont répondu que la cybercriminalité était en

Figure 1.6 : tendances de la cybercriminalité observées par les agents des services répressifs 2007-2011



Source : questionnaire de l´étude sur la cybercriminalité Q84 (n=54).

31 *Déclaration de Salvador sur les stratégies globales pour faire face aux défis mondiaux*, annexée à la résolution de l´Assemblée générale des Nations Unies A/Res/65/230 sur le *Douzième congrès des Nations Unies pour la prévention du crime et la justice pénale*, 1 avril 2011, para.39.

32 Commission de statistique des Nations Unies, 2012. *Statistiques de la criminalité de l´Institut national de statistique et de géographie de Mexico.* Note du Secrétaire Général E/CN.3/2012/3, 6 décembre 2011.

33 ONUDC estimations de Dow Jones Factiva.

34 Questionnaire de l´étude sur la cybercriminalité. Q84. En raison de la préparation et des délais de parution variables des statistiques officielles, ceci peut se référer au temps

augmentation ou en forte augmentation.[34] Les agents des services répressifs en Europe, en Asie et en Océanie tendent à signaler une croissance de la cybercriminalité plutôt qu´une forte croissance ; et un petit nombre de pays en Europe considérait que ce phénomène était stable.[35]

Les agents des services répressifs signalaient que tout un panel d´actes de cybercriminalité était en augmentation, et cela incluait les fraudes informatiques et le vol d´identité ; la production, la distribution ou la possession de pornographie infantile liée à l´informatique ; la tentative d´hameçonnage ; l´accès illégal à des systèmes informatiques ainsi que le piratage informatique. Les agents des services répressifs attribuent les niveaux croissants de cybercriminalité à une capacité croissante en matière de techniques d´anonymat lors de l´utilisation des TIC, ainsi qu´à la commercialisation croissante d´outils informatiques permettant une utilisation abusive. Le chapitre deux (la perspective d´ensemble) analyse de manière détaillée les informations fournies par les états et le secteur privé sur les tendances et les menaces d´actes spécifiques de cybercriminalité.

Facteurs sous-jacents : approches criminologiques et socio-économiques

Depuis une perspective criminologique, le fait de suggérer que les TIC et l´utilisation croissante d´internet créent de nouvelles opportunités pour les délinquants et facilitent la croissance de la criminalité, est hautement plausible. Même si de nombreuses théories criminologiques différentes sont applicables, le fait que la cybercriminalité représente *« une nouvelle forme de criminalité différente, »*[36] rend difficile la prévision et la prévention des évolutions en appliquant les théories générales sur la criminalité.[37]

Une des principales théories est que l´émergence du « cyberespace » crée un nouveau phénomène qui est nettement différent de la simple existence des systèmes informatiques, et des opportunités directes de criminalité que présentent les ordinateurs. Au sein du cyberespace, les personnes peuvent présenter des différences entre leur conduite en conformité (légale) et en non-conformité (illégale) en comparaison avec leur conduite dans le monde physique. Les personnes peuvent, par exemple, commettre des crimes dans le cyberespace qu´ils n´auraient pas commis dans le monde physique en raison de leur statut et de leur position. De plus, la flexibilité de l´identité, l´anonymat dissociatif et une absence de facteurs dissuasifs peuvent encourager une conduite criminelle dans le cyberespace.[38]

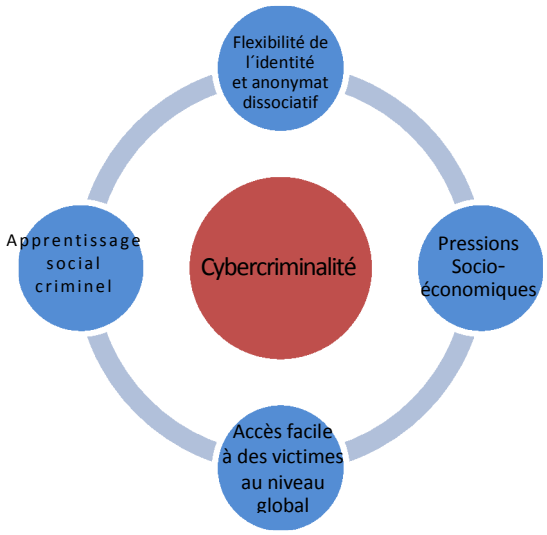


Figure 1.7 : possibles facteurs sous-jacents liés à l´augmentation de la cybercriminalité

36 Période de 2007 à 2011 ou de 2006 à 2010 (« les cinq dernières années »)
35 *Ibid.*
36 Yar, M., 2005. La nouveauté de la « cybercriminalité » : une évaluation à la lumière de la théorie des activités routinières. *Journal européen de criminologie,* 2(4) :407427.
37 Koops, B.J., 2010. L´iinternet et ses opportunités pour la criminalité. *In :* Herzog-Evans, M., (ed.) *Manuel transnational de criminologie.* Nijmegen, Netherlands : WLP, pp.735-754.
38 Jaishankar. K., 2011. Développer la cyber-criminologie avec une anthologie avant-garde. *In :* Jaishankar, K., (ed.) *Cyber-Criminologie : explorer les cimes commis sur l´iinternet et la conduite criminelle.* Boca Raton, FL : CRC Press, Taylor & Francis Group.
39 Kigerl, A., 2012. La théorie des activités routinières et les facteurs déterminant une cybercriminalité élevée des pays. *Revue informatique de sciences sociales,* 30(4) :470-486, 470.

La théorie des activités routinières (RAT)[39] peut également fournir un aperçu des causes sous-jacentes de la cybercriminalité. La théorie des activités routinières suggère que le risque de criminalité augmente avec la convergence de : (i) un délinquant motivé, (ii) une cible appropriée et (iii) l´absence d´un gardien compétent.[40] Dans le cas de la cybercriminalité, de nombreuses cibles appropriées peuvent apparaître en augmentant le temps passé en ligne, et avec l´utilisation de services en ligne tels que les services bancaires, les services d´achat et de partage des fichiers – qui exposent les utilisateurs à des attaques par hameçonnage ou à des fraudes.[41] L´émergence de réseaux sociaux en ligne, y compris Twitter et Facebook, fournit également des millions de victimes potentielles pour les fraudes et les escroqueries. Si les utilisateurs n´ont pas des paramètres de communication limités permettant une interaction seulement avec leur réseau privé « d´amis », ces réseaux peuvent permettre l´accès à un grand nombre de victimes potentielles à la fois. Les personnes tendent également à organiser leurs profils de réseaux sociaux en fonction de leurs intérêts et de leur localisation, ce qui permet aux criminels de cibler des victimes ayant des conduites ou des antécédents spécifiques. Les mesures existantes en matière de « gardiens », telles que les programmes anti-viruset un risque d´action de la part des services répressifs (comparativement faible), peuvent être insuffisantes pour dissuader un délinquant motivé par l´appât du gain.

La recherche met également en évidence que la théorie générale sur la criminalité relative à un contrôle de soi réduit et la disposition à assumer des risques pour des gains à court terme, peut s´appliquer aux actes facilités ou renforcés par les communications électroniques et l´internet. De plus, les individus exposés en ligne à des pairs et des modèles de cybercriminalité peuvent vraisemblablement s´impliquer eux-mêmes dans des actes de cybercriminalité.[42] Cette théorie de « l´apprentissage social » peut s´appliquer à la cybercriminalité, car les délinquant ont souvent besoin d´apprendre des procédures et des techniques informatiques spécifiques.[43] La théorie de l´apprentissage social et la théorie générale sur la criminalité interagissent, et les personnes qui ont un contrôle de soi réduit peuvent rechercher activement des pairs et s´unir dans un environnement virtuel comme ils le feraient dans le monde réel. Dans le cyberespace, ce processus peut avoir lieu dans un délai considérablement réduit et la portée géographique est beaucoup plus vaste.

La connectivité et l´apprentissage entre pairs en ligne sont essentielles pour que des groupes criminels organisés s´impliquent dans des activités de cybercriminalité. Les forums en ligne de piratage des cartes bancaires servant à échanger des données relatives aux cartes bancaires volées, en sont un exemple. Les forums de piratage des cartes bancaires commencent souvent avec une structure « en essaim », sans chaîne de commandement, car les auteurs d´actes de cybercriminalité se cherchent réciproquement et « se rencontrent » en ligne pour échanger leurs connaissances et pour fournir des services criminels. Les forums évoluent postérieurement vers des plates-formes plus contrôlées - dont les opérations ont des degrés plus élevés d´organisation criminelle.[44]

---

40 *Ibid.*

41 Pour une synthèse et des références supplémentaires, voir *ibid.* p.473 ; Hutchings, A., Hennessey, H., 2009. La théorie des activités routinières et la victimisation de l´hameçonnage : qui se fait prendre sur le « net » ? *Questions actuelles dans le domaine de la justice pénale,* 20(3) :433-451 ; Pratt, T.C., Holtfreter, K., Reisig, M.D., 2010. Les activités routinières en ligne et le ciblage des fraudes sur internet : étendre la généralité de la théorie des activités routinières. *Journal de recherches en matière de crime et de délinquance*, 47(3) :267-296.

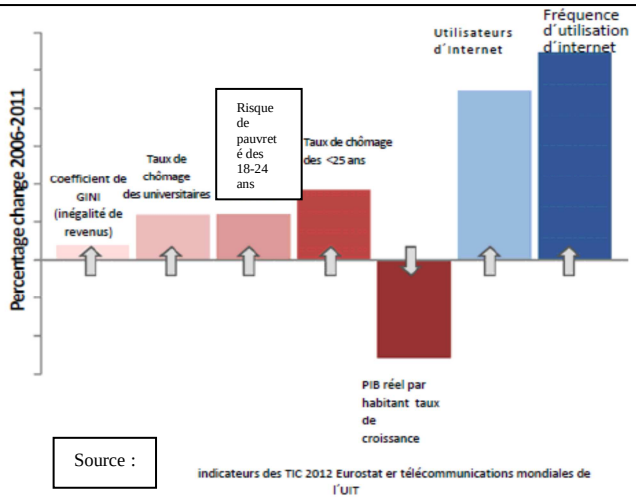
42 Holt, T.J., Burruss, G.W., Bossler, A.M., 2010. Apprentissage social et cyber-déviance : examiner l´importance d´un modèle d´apprentissage social complet dans le monde virtuel. *Journal du Crime et de la Justice*, 33(2) :31-61.

43 Skinner, W.F., Fream, A.M., 1997. Une analyse de la théorie de l´apprentissage social de la cybercriminalité parmi les étudiants universitaires. *Journal de recherches en matière de crime et de délinquance*, 34(4) :495-518.

44 BAE Systems Detica et le centre John Grieve de surveillance et de sécurité, Université métropolitaine de Londres, 2012. *La criminalité organisée à l'ère numérique.*

45 De nombreux fils Twitter, par exemple, censés représenter des individus associés à des groupes de piratage comme Anonymous ou Lulzsec, ou les organisations elles-mêmes.
46 Forum économique mondial *vision de l´agenda global 2011.*

Figure 1.8 : changements socio-économiques et fréquence de l'utilisation d'internet dans un pays d'Europe de l'est 2006-2011



Source : indicateurs des TIC 2012 Eurostat er télécommunications mondiales de l´UIT

L´utilisation de sites de réseautage social peut aussi donner lieu à des formes de « rayonnement » et de connectivité sociale entre les individus et les groupes criminels.[45] L´émergence de la connectivité globale dans un contexte de transformations démographiques et économiques globales est une autre des évolutions sous-jacentes qui peuvent déterminer les niveaux de cybercriminalité. D´ici à l´année 2050, le monde verra quasiment doubler sa population urbaine à 6,2 milliards – 70 % de la population mondiale qui est estimée à 8,9 milliards.[46] Le rapport mondial des risques du Forum économique mondial 2012 mentionne les graves disparités des revenus et les déséquilibres budgétaires chroniques comme étant deux des cinq plus grands risques à l´échelle globale pour l´année 2012.[47] Les données des sondages Gallup de 2011 révèlent que, globalement, les personnes considèrent que leur niveau de vie est en baisse – un mécontentement exacerbé par des disparités extrêmes de revenus.[48] Les recherches réalisées par l´ONUDC montrent que les facteurs économiques jouent un rôle important dans l´évolution des tendances criminelles. Sur un total de 15 pays examinés, la modélisation statistique suggère un lien global entre les changements économiques et trois types conventionnels de délits dans 12 pays. [49] Les facteurs socio-économiques peuvent également jouer un rôle important pour ce qui concerne l´augmentation de la cybercriminalité. Les pressions subies par le secteur privé visant à réduire le niveau des effectifs et des dépenses peut entraîner, par exemple, des réductions en matière de sécurité et des opportunités d´exploitation des faiblesses des TIC.[50] Étant donné que les entreprises doivent embaucher des intervenants extérieurs ou temporaires, et que les employés sont mécontents des baisses de salaires et ont peur de perdre leur emploi, les risques d´actions criminelles et d´influence exercée par des groupes criminels organisés sur des « initiés » de l´entreprise, peuvent augmenter.[51] Certaines entreprises de cybersécurité se disent inquiètes du fait que d´anciens employés qui ont été licenciés représentent une menace potentielle durant des périodes de ralentissement économique.[52] Un nombre croissant d´étudiants diplômés sans emploi ou sous employés, avec des compétences informatiques, ont également été signalés comme une source potentielle de nouvelles ressources pour la criminalité organisée.[53]

Le rôle des facteurs socio-économiques dans la cybercriminalité ne se limite pas aux pays développés, ils sont également applicables dans le contexte des pays en développement. Dans un pays d´Afrique de l´ouest, par exemple, des études sur les caractéristiques sociodémographiques des *yahooboys*[54] montrent que nombre d´entre eux sont des étudiants universitaires qui considèrent les fraudes en ligne comme un moyen de subsistance économique.[55] Le chômage, notamment, est identifié comme un facteur crucial qui entraîne les jeunes vers le *yahooboyism*.[56] De manière similaire, des études réalisées dans un autre pays d´Afrique souligne que les « *Sakawa* » impliqués dans des fraudes sur internet justifient fréquemment leurs activités en signalant que c´est leur unique moyen de survie en l´absence d´un emploi.[57]

47 Forum économique mondial, 2012. Rapport mondial des risques *2012.*
48 *Ibid*, citation de l´institut de recherche du Crédit Suisse, 2011. *Rapport global sur la richesse 2011.*
49 ONUDC, 2011. *Suivi de l´impact de la crise économique sur la criminalité.*
50 BAE Systems Detica et le centre John Grieve de surveillance et de sécurité, Université métropolitaine de Londres, 2012. *La criminalité organisée à l´ère numérique*
51 *Ibid.*
52 McAfee, 2009. *Économies sans garanties : Protection des informations vitales.*
53 BAE Systems Detica et le centre John Grieve de surveillance et de sécurité, Université métropolitaine de Londres, 2012. *La criminalité organisée à l´ère numérique.*
54 La sous-culture des « *yahooboys* » comprend des jeunes, en particulier ceux qui vivent dans des villes, qui utilisent l´internet pour commettre des actes d´escroquerie, d´hameçonnage et de fraude liés à l´informatique. Adeniran, A.I., 2011. Café Culture et hérésie du Yahooboyism. *In :* Jaishankar, K., (ed.) *Cybercriminologie : explorer les délits commis sur iinternet et la conduite criminelle.* Boca Raton, FL : CRC Press, Taylor & Francis Group.
55 Adeniran, A.I., 2008. L´internet et l´émergence de la sous-culture des Yahooboys. *Journal international de Cybercriminologie*, 2 (2) :368-381 ; etAransiola, J.O., Asindemade, S.O., 2011. Comprendre les auteurs de cyberdélits et les stratégies qu´ils emploient. *Cyberpsychologie, conduite et réseautage social* ,14(12) :759.
56 *Ibid.*

La croissance actuelle de la cybercriminalité est importante en raison de l´impact et des menaces qu´elle entraîne à de multiples niveaux. Interrogés sur les menaces de la cybercriminalité, les agents des services répressifs mentionnent une série d´impacts. Ceux-ci incluent le fait que certains actes de cybercriminalité, comme le vol d´identité et les fraudes en ligne, représentent une menace car ils sont extrêmement communs, et produisent un impact collectif à cause du volume des effets attentatoires et cumulatifs. Le chapitre deux de la présente étude (la perspective d´ensemble) examine la portée de l´impact financier de la cybercriminalité sur les individus et les entreprises. Ces actes peuvent également générer des ressources pour les groupes criminels organisés, qui peuvent les utiliser pour commettre d´autres délits. D´autres actes de cybercriminalité, comme la création d´outils illégaux permettant un abus informatique, sont plutôt rares mais représentent une menace importante car les incidents individuels peuvent causer des préjudices importants. Une troisième catégorie inclut les délits qui causent des préjudices aux individus, comme la création et la diffusion en ligne de pornographie infantile.[58]

1.4 Description de la cybercriminalité

Principaux résultats :

- les « définitions » de la cybercriminalité dépendent surtout des fins recherchées en utilisant un terme ;
- un nombre limité d´actes contre la confidentialité, l´intégrité et la disponibilité des données et des systèmes informatiques représentent l´essentiel de la cybercriminalité ;
- les actes liés à l´informatiques commis pour un profit personnel ou financier, ou pour porter préjudice, y compris des formes de crimes liés à l´identité et les actes liés au contenu informatique ne facilitent pas l´établissement des définitions légales du terme global ;
- certaines définitions sont requises pour les principaux actes de cybercriminalité. Cependant, une « définition » de la cybercriminalité n´est pas essentielle pour d´autres finalités, comme lorsqu´il s´agit de définir la portée des pouvoirs en matière de coopération internationale et d´enquêtes spécialisées, qui concernent surtout les preuves électroniques pour tout délit, au-delà d´un concept vaste et artificiel de la « cybercriminalité ».

Une étude complète sur la cybercriminalité doit définir clairement les actes qui sont inclus dans ce terme. Le terme même de « cybercriminalité » ne se prête pas à une définition simple, et est considéré comme une série d´actes ou de comportements plutôt que comme un unique acte. Néanmoins, la teneur essentielle du terme peut être décrite – au moins aux fins de la présente étude – avec une liste non-exhaustive d´actes qui constituent un cyberdélit. Ces actes peuvent à leur tour être classifiés en catégories, en se basant sur l´objet matériel du délit et le *modus operandi*.

Le terme « cybercriminalité »

De nombreux ouvrages académiques ont tenté de définir le terme de « cybercriminalité ».[59]Cependant, une stricte définition du terme ne parait pas être un objet de préoccupation pour les législations nationales.

57 Warner, J., 2011. Comprendre la cybercriminalité : une perspective d´en dessous. *Journal international de cybercriminologie* 5(1) :736-749.

58 Questionnaire de l´étude sur la cybercriminalité. Q81.

59 Parmi plusieurs autres, Union internationale des télécommunications, 2011.*Comprendre la cybercriminalité : un guide pour les pays en développement* .Rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe, ETS n°. 185 ; Pocar, F., 2004. De nouveaux défis pour les règles internationales en matière de lutte contre la cybercriminalité. *Journal européen sur la recherche et les politiques en matière pénale,* 10(1) :27-37 ; Wall, D.S., 2007. *Cybercriminalité : la transformation du crime à l´ère de l´information.* Cambridge : Polity Press.

Sur presque 200 articles des législations nationales cités par les pays en réponse au questionnaire de l´étude, moins de cinq % de ces articles utilisaient le terme « cybercriminalité » dans le titre ou le champ d´application des dispositions législatives.[60] De plus, la législation faisait généralement référence à des *« délits informatiques, »*[61] *« communications électroniques, »*[62] *« technologies de l´information, »*[63] ou *« criminalité utilisant les technologies avancées high-tech ».*[64] Dans la pratique, beaucoup de ces textes législatifs établissent des délits pénaux qui sont inclus dans le concept de la cybercriminalité, comme l´accès non autorisé à un système informatique ou l´interférence avec des données ou un système informatiques. Lorsque les législations nationales n´utilisent pas spécifiquement le terme cybercriminalité dans le titre d´une loi ou d´un article (comme « Loi sur la cybercriminalité »), les articles qui présentent les définitions de la législation incluent rarement une définition du mot »cybercriminalité ».[65] Lorsqu´une définition juridique du terme « cybercriminalité » était incluse, une approche commune consistait à le définir simplement comme *« les délits visés par la présente loi ».*[66]

De même, très peu d´instruments juridiques régionaux ou internationaux définissent la cybercriminalité. Par exemple, ni la Convention sur la cybercriminalité du Conseil de l´Europe, ni la Convention de la Ligue des états arabes, ni le Projet de Convention de l´Union Africaine ne contient une définition de la cybercriminalité aux fins de l´instrument. L´accord de la Communauté des états indépendants, sans utiliser le terme « cybercriminalité, »[67] définit un « délit concernant les informations de l´ordinateur » comme un « *un acte criminel qui vise les informations informatiques ».*[68]De même l´Accord de coopération de l´organisation de Shanghai définit les « délits relatifs à l´information » comme « *l´utilisation des ressources d´informations et (ou) leur impact dans la sphère informationnelle à des fins illicites ».*[69]

Les approches en matière de définitions des instruments régionaux, nationaux et internationaux façonnent la méthode adoptée par la présente étude. L´étude ne cherche pas à définir la cybercriminalité *per se*. Elle identifie une liste ou un « panier » d´actes qui pourraient constituer un cyberdélit. Ceci a l´avantage de mettre l´accent avant tout sur une description minutieuse du comportement précis à incriminer. Ainsi le terme même de « cybercriminalité » pourrait ne pas être considéré comme un terme juridique.[70] Il convient de noter que ceci équivaut à l´approche adoptée par des instruments internationaux tels que la Convention des Nations Unies contre la Corruption.[71] Cet instrument ne définit pas la « corruption », mais exige que les états parties incriminent des formes spécifiques de conduites qui peuvent être plus efficacement décrites.[72] La « Cybercriminalité » est donc considérée comme une série d´actes ou de conduites.

60 Questionnaire de l´étude sur la cybercriminalité. Q12.
61 Voir, par exemple, la Loi sur les délits informatiques de 1997, Malaisie ; la Loi sur les délits informatiques de 2007 ; Sri Lanka, la Loi sur les délits informatiques de 2007, Soudan
62 Voir, par exemple, La loi n°. 9918 2008 sur les communications électroniques dans la République d´Albanie ; le Code des postes et des communications électroniques (version consolidée) 2012 ; France, la loi sur les communications 2000 Tonga.
63 Voir, par exemple, la loi sur les technologies de l´information, 2000 ; Inde, la loi pénale sur les TIC de 2007 ; d´Arabie Saoudite, la loi spéciale contre les délits informatiques de 2001 de la République bolivarienne du Venezuela ; la loi sur les technologies de l´information de 2007 du Vietnam.
64 Voir, par exemple, la loi sur l´organisation et les compétences des autorités gouvernementales pour combattre la criminalité liée à la haute technologie de 2010 de la Serbie.
65 Voir, par exemple, Botswana, loi sur la cybercriminalité et les délits liés à l´informatique 2007 ; Bulgarie, chapitre 9, Code pénal SG n°. 92/2002 ; Cambodge, projet de loi sur la cybercriminalité 2012 ; Jamaïque, loi sur les cyberdélits 2010 ; Namibie, loi sur la cybercriminalité et l´abus informatique 2003 ; Sénégal, Loi n°. 2008-11 sur la cybercriminalité 2008.
66 Voir, par exemple, Oman, Décret Royal n° 12/2011 qui promulgue la loi sur la cybercriminalité ; Philippines, loi sur la prévention de la cybercriminalité 2012.
67 L´accord original est rédigé en russe et utilise le terme « преступление в сфере компьютерной информации », plutôt que l´équivalent contemporain du mot « cybercriminalité » : « киберпреступности ».
68 Accord de la communauté des états indépendants, Art. 1(a).
69 L´accord de coopération de l´organisation de Shanghai, Annexe 1.
70 Voir également l´Union internationale des télécommunications, 2011. *Comprendre la cybercriminalité : un guide pour les pays en développement.*
71 Nations Unies. 2004. *Convention contre la Corruption.*
72 *Ibid*., Arts. 15 et seq.

Descriptions des concepts connexes

Il est également intéressant d´examiner les descriptions des concepts connexes, tels que « ordinateur », « système informatique », « donnée » et « information ». Leur signification est inhérente à la compréhension de l´objet et/ou[13] des intérêts juridiques protégés, concernés par des actes

de cybercriminalité. Un examen des instruments régionaux et internationaux révèle deux approches principales : (i) une terminologie basée sur le système ou des données de « l´ordinateur » ; (ii) une terminologie basée sur le système ou des données « informatiques ».[73] Une analyse des éléments des définitions suggère toutefois que les termes peuvent être considérés comme interchangeables dans une grande mesure. La figure présente des éléments communs de ces définitions. Bien que la nomenclature varie, de nombreux concepts fondamentaux concordent.

Système informatique/information

- Dispositif [ou dispositifs interconnectés] qui [par le biais d´un programme d´ordinateur/informatique] réalise un traitement [[automatisé] des données de l´ordinateur/informatiques] [fonctions logiques/arithmétiques/de stockage] [y compris les données de l´ordinateur/informatiques stockées/traitées/extraites /transmises par le système d´ordinateur /informatique] [y compris le matériel ou les dispositifs de communications] [y compris l´ internet]

Programme d´ordinateur/informatique

- Les instructions [sous une forme lisible par machine] qui [permettent à un système d´ordinateur /informatique de [traiter des données de l´ordinateur/informatiques] [de réaliser une fonction /opération]] [qui peut être exécutée par un système d´ordinateur /informatique]

Données de l´ordinateur/informatiques

- Représentation de faits/informations/concepts [sous une forme lisible par machine] [pouvant être traités par un programme d´ordinateur/informatique][ou un système d´ordinateur /informatique] [y compris un programme d´ordinateur/informatique]

Les caractéristiques essentielles des descriptions juridiques des termes « ordinateur », « système de l´ordinateur » ou « système informatique », consistent, par exemple, dans le fait que le dispositif doit être *«* capable de traiter des informations ou des données de l´ordinateur ».[74] Certaines approches spécifient que le traitement doit être « automatisé » ou « à haute vitesse » ou « en exécution d´un programme ».[75] Certaines approches élargissent la définition pour englober des dispositifs qui stockent ou transmettent et reçoivent des informations ou des données informatiques[76] D´autres incluent dans la définition les données informatiques traitées par le système.[77] Si le terme « système de l´ordinateur » ou « système informatique » exclut les données stockées dans le système ou dans d´autres dispositifs de stockage, celles-ci sont souvent traitées séparément dans les dispositions juridiques de fond de l´instrument.[78] Si certains instruments définissent le terme « ordinateur » ainsi que le terme « système de l´ordinateur, » ce dernier inclut normalement le premier terme, et le contexte d´utilisation des deux termes dans l´instrument suggère qu´il n´existe aucune différence significative dans la pratique.[79] D´autres instruments définissent le terme « réseau informatique » et « système informatique ».[80] Une fois encore, ce dernier terme peut inclure le premier, et cela ne représente pas de différence perceptible dans l´utilisation de l´instrument.

73 La Convention sur la cybercriminalité du Conseil de l´Europe et la loi type du Commonwealth utilisent les termes « système informatique » et « données informatiques ». Le projet de convention de l´Union Africaine utilise les termes « système informatique » et « données informatisées ». La décision relative aux attaques visant les systèmes d´information de l´UE utilise les termes « système d´information » et « données informatiques ». La Convention de la Ligue des états arabes utilise les termes « systèmes d´information » et « données », et l´Accord de la Communauté des états indépendants utilise le terme « informations informatiques ».

74 Voir, par exemple, l´Art. 1. de la Convention sur la cybercriminalité du Conseil de l´Europe

75 Voir, par exemple, l´Art. 1. du projet de loi type du COMESA et l´Art. 3 des textes législatifs types de l´UIT/CARICOM/CTU

76 Projet de convention de l´Union Africaine, Partie III, Section 1, Art. III-1(6).

77 Décision relative aux attaques visant les systèmes d´information de l´UE, Art. 1(a).

78 Voir, par exemple, l´Art 19 de la Convention sur la cybercriminalité du Conseil de l´Europe, les pouvoirs procéduraux pour que autorités compétentes recherchent ou aient accès (a) à un système informatique ou à une partie de ce système et aux données qui y sont stockées ; et (b) un support de stockage informatique permettant de stocker des données informatiques

79 Le projet de loi type du COMESA, Partie 1, Art. 1(b) et (e).

80 Convention de la Ligue des états arabes, Art. 2(5) et (6).

Les textes des instruments juridiques régionaux et internationaux sur la cybercriminalité sont majoritairement neutres du point de vue technologique. Ils n´établissent pas une liste spécifique de dispositifs qui pourraient être considérés comme des systèmes informatiques ou des systèmes d´information. Dans la plupart des contextes, cette approche est considérée comme une bonne pratique, dans la mesure où elle atténue les risques pour les nouvelles technologies se trouvant hors des paramètres des dispositions juridiques et la nécessité de continuellement mettre à jour la législation.[81] Il est probable que les dispositions, basées sur les concepts essentiels du traitement des informations ou des données informatiques, soient applicables à des dispositifs tels que les unités centrales et les serveurs informatiques, les ordinateurs personnels de bureau, les ordinateurs portables, les smartphones, les tablettes, les ordinateurs embarqués destinés au transport et à la machinerie, ainsi qu´aux dispositifs multimédias tels que les imprimantes, les lecteur MP3, les caméras numériques et les machines de jeu.[82] Dans le cadre du concept du « traitement des informations ou des données informatiques, » on peut parfaitement soutenir que pourrait être inclus tout dispositif, tel qu´un routeur fixe ou sans fil, connecté à l´internet. Les dispositifs de stockage, comme les disques durs, les clés USB ou les cartes mémoire peuvent ou non faire partie du « système informatique » ou « du système d´information ». Même s´ils n´en font pas partie, ils restent, néanmoins, des objets pertinents avec des dispositions juridiques distinctes.

Un seul instrument régional ou un international mentionne une limite au « niveau inférieur de technologie » dans la description d´un système informatique – en déclarant que le terme n´inclut pas de *« machine à écrire ou de typographe automatique, de calculatrice de poche portative ou tout autre dispositif similaire ».*[83] Alors que le monde se dirige vers un « internet des objets » et la nano-informatique, des descriptions telles que le « système informatique » ou le « système d´information » devraient vraisemblablement être interprétées comme comprenant un plus large éventail de dispositifs.[84] En principe, le concept fondamental de « traitement automatisé d´informations » devrait être suffisamment flexible pour inclure, par exemple, une puce intelligente de surveillance et de contrôle avec une connectivité NFC et IP, logée dans un appareil ménager.

Les « données informatiques » ou les « informations informatiques » sont généralement décrites comme une *« représentation des faits, des informations ou des concepts pouvant être lus, traités ou stockés par un ordinateur ».* Certaines approches précisent que cela inclut un programme informatique.[85] D´autres ne font aucun commentaire sur ce point. La différence entre la formulation « pouvant être lus par une machine » et « pouvant être lus, traités ou stockés par un système informatique (ou un système d´information) » a seulement un caractère sémantique. Dans la pratique, les informations ou les données informatiques incluent des informations ou les données stockées sur un support de stockage physique (comme des disques durs, des clés USB ou des cartes), des informations ou les données stockées dans la mémoire d´un système informatique ou d´un système d´information, la transmission des informations ou des données (câblée, optique, ou radio fréquence), et l´affichage physique des informations ou des données, sous la forme d´une impression ou sur un écran de dispositif.

Tout en reconnaissant les différentes approches en matière d´utilisation de la terminologie, la présente étude utilise les termes « système informatique » et « données informatiques », qu´elle utilise comme des termes équivalant à « système d´information » et « informations informatiques »

Catégories de cybercriminalité

Si le terme « cybercriminalité » ne se prête pas à une définition simple, la question se pose de savoir si le *modus operandi*, les caractéristiques et les objectifs de la cybercriminalité peuvent être décrits dans des termes généraux, plutôt qu´en se référant (ou en complément de) à une liste d´actes individuels de cybercriminalité.

---

81 Voir, par exemple, le rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe, ETS n°. 185.

82 Une note d´orientation du comité de la Convention sur la cybercriminalité du Conseil de l´Europe(T-CY) conclut également que la définition du terme « système informatique » de l´Article 1(a) de la Convention sur la cybercriminalité du Conseil de l´Europe couvre des formes avancées de technologies qui vont au-delà des systèmes d´ordinateur central ou d´ordinateur de bureau traditionnels, comme les téléphones portables modernes, les smartphones, des assistants numériques personnels, des tablettes ou

des dispositifs similaires. Voir la note d´orientation 1 sur le concept de « système informatique ». T-CY (2012) 21 du Conseil de l´Europe. 2012, du 14 novembre 2012.

83 Projet de loi type du COMESA, Partie 1, Art. 1(b).

84 Pour une analyse des évolutions potentielles et des problèmes de règlementation associés à l´internet des objets, voir la communication de la Commission au parlement européen, au Conseil, au comité économique et social européen et au comité des régions. *L´internet des objets – un plan d´action pour l´Europe.* COM (2009) 278 Final,18 juin 2009.

85 Convention sur la cybercriminalité du Conseil de l´Europe, Art. 1(b).

Comme mentionné précédemment, il y a un exemple de cette approche dans l´Accord de la Communauté des états indépendants, qui décrit un *« délit relatif à l´information informatique »* comme *« un acte criminel qui vise les informations informatiques ».*[86] De même, l´Accord de coopération de l´organisation de Shanghai définit les « délits relatifs à l´information » comme « *l´utilisation des ressources d´informations et (ou) leur impact dans la sphère informationnelle à des fins illicites ».* La Convention sur la cybercriminalité du Conseil de l´Europe – bien que ce ne soit pas par le biais de la définition des termes – utilise de vastes catégories d´incrimination, et ceci inclut les *« les infractions contre la confidentialité, l´intégrité et la disponibilité des données et des systèmes informatiques » l*es *« délits liés à l´informatique »* et *« les délits liés au contenu ».*[87] De même le projet de convention de l´Union Africaine comprend des intitulés de chapitres qui établissent des différences entre les *« infractions spécifiques relatives aux technologies de l´information et de la communication »* et *« l´adaptation de certaines infractions relatives aux technologies de l´information et de la communication ».*[88]

Ces approches démontrent clairement que certaines caractéristiques générales peuvent être utilisées pour décrire des actes de cybercriminalité. Une des approches consiste à se concentrer sur l´objet de l´infraction – c´est à dire la personne, la chose ou la valeur à l´encontre de laquelle est commise l´infraction.[89] Cette approche figure dans l´Accord de la Communauté des états indépendants (ou l´objet de l´infraction est l´information informatique) et également dans le Titre premier du chapitre de droit pénal matériel de la Convention sur la cybercriminalité du Conseil de l´Europe (ou les objets de l´infraction sont les données informatiques ou les systèmes informatiques). Une autre approche tend à évaluer si les systèmes informatiques ou les systèmes d´information font partie intégrante du *modus operandi* de l´infraction.[90] Cette approche figure dans les Titres second, troisième et quatrième du chapitre de droit pénal matériel de la Convention sur la cybercriminalité du Conseil de l´Europe, ainsi que dans l´Accord de coopération de l´organisation de Shanghai et le projet de convention de l´Union Africaine. Identifier de potentiels objets d´infractions et le *modus operandi* en matière de cybercriminalité ne décrit pas les actes de cybercriminalité dans leur intégralité, mais peut fournir des catégories générales utiles pour classer ces actes.

Certains instruments régionaux ou internationaux abordent la cybercriminalité dans un concept étroit dans lequel l´objet de l´infraction est le système ou les données informatiques.[91] D´autres comprennent une gamme plus ample d´infractions et incluent des actes dans lesquels l´objet de l´infraction est une personne ou une valeur plutôt que le système ou les données informatiques – mais où le système informatique ou le système d´information reste, néanmoins, une partie intégrante du *modus operandi* de l´infraction.[92] Le chapitre quatre (incrimination) examine de manière détaillée les actes spécifiques incriminés par ces instruments. Alors que tous les instruments régionaux ou internationaux n´utilisent pas une conception plus vaste de la cybercriminalité, l´approche utilisée par la présente étude vise à être aussi exhaustive que possible. Elle utilise donc une vaste liste de descriptions d´actes de cybercriminalité, classifiés en trois catégories basées sur l´objet de l´infraction et le *modus operandi*. En raison de l´utilisation de deux méthodes de classification, il peut y avoir un chevauchement entre les catégories.

---

86 Accord de la Communauté des états indépendants, Art. 1(a).
87 Convention sur la cybercriminalité du Conseil de l´Europe, Titres 1, 2, et 3.
88 Projet de convention de l´Union Africaine, Partie III, chapitre V, Section II, chapitres 1 et 2.
89 elles incluent des infractions contre la confidentialité, l´intégrité et la disponibilité des systèmes et des données informatiques. Voir Calderoni, F.2010. Le cadre juridique européen sur la cybercriminalité : lutter pour une mise en œuvre efficace. *Crime, droit et changement social,* 54(5) :339-357.
90 Podgor, E.S., 2002. Fraudes informatiques internationales : un paradigme pour limiter la juridiction nationale. Revue juridique *U.C. Davis*, 35(2) :267- 317, 273 et seq.
91 EU Décision relative aux attaques visant les systèmes d´information et l´Accord de la Communauté des états indépendants.
92 Par exemple, le projet de directive de la CEDEAO, Art. 17 (Facilitation d´accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur). Voir également Pocar, F., 2004. De nouveaux défis pour

les règles internationales en matière de lutte contre la cybercriminalité. *Journal européen sur la recherche et les politiques en matière pénale*, 10(1) :27-37.

Actes constituant un cyberdélit

La figure ci-dessous propose 14 actes qui peuvent constituer un cyberdélit, classifiés en trois vastes catégories. La première Annexe de cette étude fournit une description plus détaillée de chaque acte. Cette liste d´actes a également été utilisée dans le questionnaire envoyé aux états, aux entités du secteur privé, et aux organisations universitaires et intergouvernementales, afin de recueillir des informations pour l´étude.[93] L´objectif de la liste est d´introduire un ensemble provisoire d´actes pouvant être inclus dans le terme « cybercriminalité, » afin d´établir une base d´analyse pour l´étude. La liste n´a pas la prétention d´être exhaustive et de plus, les termes utilisés – et les descriptions afférentes de la première Annexe – n´ont pas la prétention de représenter des définitions juridiques. Il s´agit donc d´amples « descriptions d´actes » qui peuvent être utilisées comme un point de départ pour l´analyse et la discussion. Bien que la présente étude ne « définisse » pas la cybercriminalité (avec une définition du terme en soi ou avec une liste « définitive » d´actes), les conduites énumérées peuvent toutefois être considérées comme le contenu de base pour ce qui concerne la signification du terme, du moins aux fins de la présente étude.[94]

Actes contre la confidentialité, l´intégrité et la disponibilité des systèmes ou des données informatiques

- Accès illégal à un système informatique
- Accès illégal, interception ou acquisition de données informatiques
- Interférence illégale avec un système ou des données informatiques
- Production, distribution ou possession d´outils informatiques permettant un abus informatique
- Violation de la vie privée ou des mesures de protection des données

Actes liés à l´informatique commis pour un profit personnel ou financier ou pour porter préjudice

- Falsification ou fraude informatique
- Délit lié à l´informatique concernant l´identité
- Délit lié à l´informatique relatif aux droits d´auteur et aux marques déposées
- Envoi ou contrôle de l´envoi de messages non sollicités (SPAM)
- Actes liés à l´informatique causant un préjudice personnel
- Sollicitation ou « prédation sexuelle » des enfants liée à l´informatique

Actes liés au contenu informatique

- Actes liés à l´informatique impliquant des discours de haine
- La production, la distribution ou la possession de pornographie infantile liée à l´informatique
- Actes d´appui au délit de terrorisme liés à l´informatique

Il faut signaler, à ce stade, que l´omniprésence de l´internet et des dispositifs informatiques personnels signifie que les données ou les systèmes informatiques peuvent être des auxiliaires – du moins dans les pays développés – pour presque tous les délits pénaux. Le domaine des preuves électroniques est étroitement lié à la cybercriminalité mais est conceptuellement distinct. La collecte et la présentation des preuves électronique font partie intégrante d´une enquête et de la poursuite contre un cyberdélit. C´est également de plus en plus le cas pour des délits classiques comme le vol, le vol aggravé ou le

93 ébauche du questionnaire pour collecter des informations a initialement été développée par le Secrétariat en se basant sur une liste de thèmes à inclure dans l´étude, approuvée par un groupe d´experts en cybercriminalité (incluse dans le *Rapport du groupe intergouvernemental d´experts à composition non limitée sur le problème de la cybercriminalité* (E/CN.15/2011/19)). L´ébauche du questionnaire, ainsi qu´une première ébauche des descriptions des actes de cybercriminalité, a été envoyée à tous les pays pour commentaires, en 2011. Après que le Secrétariat y ait incorporé les commentaires reçus, le questionnaire final, ainsi que la liste des actes présentés ici, a été approuvé par le Bureau du groupe d´experts en cybercriminalité lors de sa réunion le 19 janvier 2012.

94 En réponse aux commentaires des pays, la liste des actes présentée dans ce chapitre a fait l´objet de plusieurs modifications, en comparaison avec celle qui a été utilisée dans le questionnaire de l´étude. Dans le questionnaire de l´étude, la seconde catégorie était intitulée « actes liés à l´informatique commis pour un profit personnel ou financier ». Elle a été modifiée de la manière suivante : « actes liés à l´informatique commis pour un profit personnel ou financier ou pour porter préjudice ». Dans le questionnaire de l´étude, la troisième catégorie était intitulée « actes spécifiques liés à l´informatique ». Elle a été modifiée de la manière suivante : « actes liés au contenu informatique ». Les points « actes liés à l´informatique causant un préjudice personnel » et « sollicitation ou prédation sexuelle des enfants liées à l´informatique » sont passés de la troisième catégorie à la seconde catégorie. Le questionnaire contient également le point « actes liés à l´informatique impliquant du racisme ou de la xénophobie ». Ceci a été modifié avec une catégorie plus vaste « actes liés à l´informatique impliquant des discours de haine ».

cambriolage, ainsi que pour des formes de criminalité organisée. Les registres téléphoniques informatisés, les courriels, les emails, les journaux des connexions IP, les messages SMS, les carnets d´adresse des téléphones portables et les fichiers informatiques peuvent tous contenir des preuves relatives à la localisation, au motif, à la présence sur la scène du crime ou crime ou à l´implication d´un suspect dans des activités criminelles, pour pratiquement toutes sortes de délits.

Actes contre la confidentialité, l´intégrité et la disponibilité des systèmes ou des données informatiques

Les principaux actes de cybercriminalité de la liste visent les systèmes ou les données informatiques. Ces actes incluent l´accès non autorisé, l´interception, l´acquisition, ou l´interférence avec les systèmes ou les données informatiques. Le chapitre quatre (incrimination) examine cela de manière plus détaillée, avec des extraits des législations nationales et des instruments régionaux ou internationaux. Ces actes peuvent être commis en utilisant divers *modus operandi*. L´accès illégal à un système informatique, par exemple, peut consister en l´utilisation non autorisée d´un mot de passe qui a été découvert ou en l´accès à distance en utilisant un logiciel d´exploitation.[95] Ceci peut également représenter une interférence avec les données informatiques et /ou un système informatique. Les actes individuels peuvent donc représenter un degré de chevauchement avec le « panier » des infractions. La première catégorie inclut également des actes liés aux outils qui peuvent être utilisés pour commettre des actes contre les systèmes ou les données informatiques.[96] La catégorie inclut aussi des actes criminels liés au traitement (inapproprié) des données informatiques conformément aux exigences spécifiées.

« Opération Aurora »

En 2010, une série d´attaques en ligne a été signalée par plusieurs grandes sociétés de fabrication de logiciels, et dernièrement, des violations ont été signalées dans une grande entreprise de moteurs de recherche. En se servant d´une vulnérabilité jour zéro dans un navigateur web, les attaquants créèrent un tunnel dans le réseau interne via les employés, mirent en péril des stations de travail, et eurent accès aux comptes e-mail et aux dépôts des codes sources insuffisamment sécurisés.

La même année, les utilisateurs d´un réseau social reçurent des e-mails provenant d´un faux compte avec des liens vers un nouveau système de code d´accès fictif qui paraissait être de l´entreprise, avec le nom d´utilisateur de la victime déjà introduit dans le système de code d´accès. Les authentifiants des utilisateurs seraient alors compromis, et l´hôte infecté pourrait éventuellement devenir un membre de ZeuS botnet.

Source : Trustwave. 2011. SpiderLabs Global Security Report.

Actes liés à l´informatique commis pour un profit personnel ou financier ou pour porter préjudice

Le virus « *Goxi* »

Au début de 2013, trois hommes européens furent accusés par des procureurs américains d´avoir créé et distribué un virus informatique qui avait infecté plus d´un million d´ordinateurs dans le monde, en leur permettant l´accès à des informations bancaires personnelles et de voler au moins 50 millions de dollars de 2005 à 2011. Le virus avait été introduit en Europe et s´était dispersé en Amérique du nord où il avait également infecté des ordinateurs appartenant à des agences nationales. Les procédures d´extradition à l´encontre de deux des accusés sont en cours. Le cas est considéré comme *« l´un des plus destructif sur le plan financier jamais vu. »*

Source : http://www.fbi.gov/

La seconde catégorie incluent des actes pour lesquels l´utilisation d´un système informatique est inhérente au *modus operandi*. L´objet de ces actes varie. Dans le cas des fraudes informatiques, l´objet serait le bien économique visé. Dans le cas d´une infraction liée à l´informatique relative aux droits d´auteur ou aux marques déposées, l´objet de l´infraction serait le droit protégé de propriété intellectuelle. Dans le cas des actes liés à l´informatique qui causent un préjudice personnel, comme l´utilisation d´un système informatique pour harceler, malmener, menacer, traquer, effrayer ou intimider une personne, ou commettre un acte de prédation sexuelle à l´encontre d´un enfant, l´individu visé est considéré comme étant l´objet de l´infraction.

95Nations Unies, 1994. *Manuel des Nations Unies sur la prévention et le contrôle des délits liés à l´informatique.*

96 Les exemples incluent Low orbit ion cannon (canon à ion à faible orbite) (LOIC), sKyWIper et le maliciel bancaire ZeuS.

L´opinion selon laquelle divers actes avec des objets d´infraction différents peuvent, néanmoins, être considérés comme des « cyberdélits » est soutenue par des travaux préliminaires sur le développement d´un cadre pour la classification internationale des délits à des fins statistiques. Les travaux effectués par la Conférence des statisticiens européens signalent que actes de « cybercriminalité » pourraient être consignés, à des fins statistiques, en utilisant une « étiquette d´attribut » pour indiquer « la facilitation informatique » d´un acte spécifique dans un système de classification des délits. Cette « étiquette » pourrait s´appliquer, en principe, aux actes facilités par l´informatique qui relèvent d´un système plus ample de classification des délits – des actes commis contre des personnes, contre des biens ou contre les autorités ou l´ordre public.[97]

Une difficulté inhérente aux délits « liés à l´informatique » est que cette catégorie risque de s´étendre, afin d´y inclure une vaste gamme de délits commis « hors ligne », lorsqu´ils ont été commis avec l´utilisation ou l´assistance d´un système informatique. La question de savoir si ce type d´acte devrait être considéré comme un « cyberdélit » reste ouverte. Alors que certains instruments régionaux ou internationaux sont limités à un nombre relativement restreint d´infractions liées à l´informatique, d´autres sont exhaustifs. La Convention sur la cybercriminalité du Conseil de l´Europe, par exemple, couvre (de cette catégorie) isolément la falsification informatique et la fraude informatique.[98] En revanche, la loi type de la Ligue des états arabes contient des dispositions pénales relatives à l´utilisation d´un système informatique à des fins de falsification, de menaces, de chantage, d´appropriation d´un bien meuble ou d´un titre de propriété par le biais de l´utilisation frauduleuse d´un nom, d'obtention illicite des numéros ou des détails d´une carte de crédit, de jouissance illicite de services de communication, d'établissement d'un site (internet) avec l´intention de se livrer à la traite des êtres humains ou au trafic de stupéfiants ou de substances psychotropes, et de transférer illicitement des fonds ou d´en déguiser l´origine illicite.[99]

Un autre acte qui peut entrer dans cette catégorie – et qui contrairement aux actes mentionnés précédemment, est exclusivement lié à l´informatique – est l´envoi et le contrôle de l´envoi de SPAM[100] Bien que l´envoi massif de messages non sollicités soit interdit par tous les fournisseurs de services internet, il n´est pas incriminé par tous les pays. Le chapitre quatre (incrimination) examine cette question plus en détails.

Actes liés au contenu informatique

La dernière catégorie des actes de cybercriminalité concerne le contenu informatique – les mots, les images, les sons et les représentations transmis ou stockés par les systèmes informatiques, y compris l´internet. L´objet matériel des infractions liées au contenu est souvent une personne, un groupe identifiable de personnes, ou une valeur ou une croyance largement répandue. De même dans la seconde catégorie, ces actes pourraient en principe être commis « hors ligne », ou en utilisant un système informatique. Cependant, plusieurs instruments régionaux et internationaux sur la cybercriminalité incluent des dispositions spécifiques sur le contenu informatique.[101] Un argument pour l´inclusion des actes liés au contenu informatique dans le terme « cybercriminalité » est que les systèmes informatiques, y compris l´internet, ont fondamentalement modifié la portée de la diffusion de l´information.[102]

---

97 Voir la Commission économique des Nations Unies pour l´Europe, la Conférence des statisticiens européens. *Principes et cadre pour une classification internationale des délits à des fins statistiques.* ECE/CES/BUR/2011/NOV/8/Add.1. 11 octobre 2011.

98 Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 7 et 8.

99 Loi type de la Ligue des états arabes, Articles 4, 9-12, et17-19.

100 l´envoi ou le contrôle de l´envoi de SPAM concerne des actes qui impliquent l´utilisation d´un système informatique pour envoyer des messages à un grand nombre de destinataires sans autorisation ni demande. Voir la première Annexe (descriptions des actes).

101 Voir la Convention sur la cybercriminalité du Conseil de l´Europe, Art. 9 ; la Convention de la Ligue des états arabes, Art. 12 et seq. ; et les textes législatifs types de l´UIT/CARICOM/CTU, Section II, entre autre.

102 Marcus, R.L., 2008. L´impact des ordinateurs sur la profession juridique : évolution ou révolution ? *Revue de droit de l´université Northwestern,* 102(4) :1827-1868.

Les pays peuvent considérer comme une conduite criminelle la possession ou la divulgation de contenus par le biais de systèmes informatiques. À cet égard, il est important de signaler que, outre le principe de souveraineté de l´état, un point de départ fondamental entériné dans les traités internationaux sur les droits de l´homme, est le droit à la liberté d´opinion et d´expression.[103] À partir de ce point de départ, le droit international permet certaines restrictions nécessaires comme le prévoit la loi.[104] De plus, le droit international exige que les états interdissent certaines formes d´expression, comme la pornographie infantile, l´incitation directe et publique au génocide, toutes les formes de discours haineux et l´incitation au terrorisme.[105] Le chapitre quatre (incrimination) examine les approches régionales, nationales et internationales relatives à l´incrimination des contenus informatiques, y compris depuis la perspective des lois internationales sur les droits de l´homme, de manière détaillée.

Conspiration pour la préparation d´un acte terroriste

En mai 2012, un tribunal d´Europe occidentale a condamné l´un de ses ressortissants à cinq ans de prison pour avoir participé à une conspiration criminelle pour préparer un acte. Lors du procès, le parquet présenta des douzaines de communications de courriels décryptés avec un contenu djihadiste, qui avaient été envoyés, entre autre, au site web du président du pays, et qui permirent de remonter jusqu´à un membre d´un groupe extrémiste qui opère à l´échelle globale. Une ordonnance de conservation permit aux autorités d´identifier des communications entre les membres du groupe extrémiste et des sites web extrémistes, y compris un site web dont l´objectif déclaré était d´héberger et de diffuser les documents du groupe extrémiste, des enregistrements d´audio et de vidéo, des déclarations des guerriers et des attaquants suicidaires et le matériel d´autres groupes extrémistes. Ceci indiquait que le prévenu réalisait de manière active, entre autre, la traduction, l´encodage, la compression et la protection par mot de passe du matériel pro-jihadiste, qu´il téléchargeait et distribuait ensuite sur internet ; et prenait des mesures concrètes pour fournir un appui financier au groupe extrémiste, y compris en tentant d´utiliser PayPal et d´autres systèmes virtuels de paiement. Le tribunal estima que les preuves requises étaient suffisantes pour démontrer que le prévenu avait fourni non seulement un appui intellectuel mais également un appui logistique direct à un plan terroriste clairement identifié.

Source : UNODC. 2012. Utilisation de l´internet à des fins terroristes.

Les actes d´appui au délit de terrorisme liés à l´informatique sont inclus dans la catégorie des cyberdélits liés au contenu. La récente publication de l´ONUDC « l´utilisation de l´iinternet à des fins terroristes »[106] signale que les systèmes informatiques peuvent être utilisés pour une gamme d´actes qui promeuvent et appuient le terrorisme. Ceci inclut la propagande (le recrutement, la radicalisation et l´incitation au terrorisme) ; le financement ; la formation, la planification (y compris par le biais de communications secrètes et d´informations de source publique) ; l´exécution ; et les cyberattaques.[107] Le questionnaire utilisé pour recueillir des informations mentionnait directement les délits d´incitation au terrorisme, de planification et de financement du terrorisme liés à l´informatique.[108] À cet égard, la présente étude se concentre seulement sur le contenu informatique des délits de terrorisme et exclut de la portée de l´analyse les menaces de cyberattaques des organisations terroristes – une approche équivalente à celle de la publication de l´ONUDC sur l´utilisation de l´internet à des fins terroristes.

Autres actes de cybercriminalité

La liste de 14 actes de cybercriminalité n´est pas exhaustive. Lors du recueil des informations pour l´étude, les pays furent invités à signaler d´autres actes qu´ils considèrent comme étant des cyberdélits.[109] Les réponses incluaient *« les outils informatiques qui facilitent des actes illégaux liés*

103 UDHR, Art. 19 ; ICCPR Art. 19 ; ECHR, Art. 9 ; ACHR Art. 13 ; ACHPR Art. 9.
104 Cassese, A., 2005. *Droit international.* 2nd ed. Oxford : Oxford University Press. p. 53. et pp.59 et seq.
105 Assemblée générale des Nations Unies, 2011. *Promotion et protection du droit à la liberté d´opinion et d´expression. Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d´opinion et d´expression.* A/66/290. 10 août 2011.
106 ONUDC, 2012. *L´utilisation d´iinternet à des fins terroristes.* Disponible sur https ://www.unodc.org/documents/frontpage/Use_of_internet_for_Terrorist_Purposes.pdf
107 *Ibid.*
108 Questionnaire de l´étude sur la cybercriminalité .Section de descriptions des actes. Voir aussi la première Annexe (descriptions des actes).
109 Questionnaire de l´étude sur la cybercriminalité. Q39.

aux instruments financiers et aux moyens de paiement ; *« les paris en ligne* ; *« l´utilisation de dispositif de technologie de l´information à des fins de traite de personnes* ; *« le trafic de drogue lié à l´informatique »* ; *« l´extorsion lié à l´informatique* ; *« le trafic de mots de passe* ; et *« l´accès à des informations classifiées ».*[110] Dans tous ces cas, les répondants ont indiqué que l´acte était couvert par une cyberlégislation spécifique – et ont signalé le caractère essentiel de l´utilisation de systèmes ou de données informatiques pour ces actes.

Dans certains de ces cas, l´acte peut être considéré comme une forme spécialisée ou une variation de l´un des actes de cybercriminalité déjà mentionnés. L´utilisation ou la possession d´outils informatiques pour commettre des infractions financières, par exemple, peuvent être couvertes par l´acte plus général de falsification ou de fraude informatique.[111] L´accès à des informations classifiées peut être une sous-catégorie de l´accès illégal à des données informatiques. Le trafic de mots de passe est couvert par certaines dispositions relatives à l´usage abusif d´outils informatiques.[112]

L´internet et la vente de drogues illicites

Depuis le milieu des années 90, l´internet a de plus en plus été utilisé par des trafiquants de drogue pour vendre des drogues illicites ou les précurseurs chimiques nécessaires pour fabriquer ces drogues. En même temps, des pharmacies illégales sur internet proposent au public en général des ventes illicites de médicaments délivrés sur ordonnance, y compris de substances placées sous contrôle international. Ces substances sont contrôlées conformément aux trois traités internationaux relatifs au contrôle des drogues et incluent des analgésiques opioïdes, des stimulants du système nerveux central, des tranquillisants et d´autres substances psychoactive. Divers médicaments, offerts ainsi à la vente, sont détournés du marché licite, contrefaits ou frauduleux – et constituent un danger pour la santé des consommateurs. Le fait que des pharmacies illégales sur internet mènent leurs activités dans toutes les régions du monde et aient la capacité de facilement transférer leurs activités lorsqu´un site web est fermé, signifie qu´il est essentiel de prendre des mesures efficaces dans ce domaine.

En 2009, l´Organe international de contrôle des stupéfiants (OICS) publia le « principes directeurs à l´intention des gouvernements pour la prévention de la vente illégale par internet de substances soumises à un contrôle international. » Ces principes directeurs soulignent l´importance de : habiliter les autorités compétentes à enquêter et à prendre des mesures légales contre les pharmacies d´internet et d´autres sites web, utilisés pour la vente illégale de substances soumises à un contrôle international ; interdire l´envoi par courrier de ces substances soumises à un contrôle international et s´assurer que ces envois soient interceptés ; et établir des normes de bonne pratique professionnelle pour ce qui concerne les services pharmaceutiques par l´entremise d´ internet.

D´autres actes, comme l´extorsion liée à l´informatique,[113] soulève le problème de l´inclusion (ou de la non-inclusion) des délits commis hors ligne qui sont maintenant, à des degrés divers, commis en ligne – un point qui a été abordé brièvement dans le contexte des actes liés à l´informatique commis pour un profit personnel ou financier ou pour porter préjudice. Comme l´ont signalé de nombreux pays répondants, un principe général est que fréquemment *« les actes qui sont illégaux hors ligne, le sont également en ligne ».*[114] Dans plusieurs cas, les lois pénales qui règlementent la conduite hors ligne peuvent également être appliquées aux versions en ligne des mêmes conduites. Les pays ont donc interprété, par exemple, les lois conventionnelles existantes pour couvrir l´extorsion liée à l´informatique,[115]ou l´utilisation de systèmes informatiques pour faciliter la traite de personnes.[116]

---

110 *Ibid.*

111 Certains pays incluent, par exemple, l´acte de « possession d´articles pour les utiliser dans des fraudes » dans les délits pénaux de fraudes.

112 Les mots de passe informatiques, les codes d´accès ou des données similaires ne sont pas explicitement inclus dans la description de l´acte de la rubrique « Production, distribution ou possession d´outils permettant un abus informatique » utilisée dans le questionnaire de l´étude, ce qui amène certains pays à identifier cette conduite comme un acte additionnel.

113 Outre l´utilisation de systèmes informatiques pour communiquer des menaces d´extorsion, les extorsions informatiques peuvent être associées à une interférence non autorisée avec les données ou les systèmes informatiques, comme les demandes d´argent liées aux attaques DDoS.

114 Questionnaire de l´étude sur la cybercriminalité Q39.

115 Voir, par exemple, Landgericht Düsseldorf, Allemagne. 3 KLs 1/11, 22 mars 2011, où l´accusé a été condamné pour extorsion et sabotage informatiques contre des sites de paris en employant des services de botnet.

116 UN.GIFT, 2008. *Le Forum de Vienne sur la lutte contre la traite des êtres humains. Document de référence pour l´atelier 017 : Technologie et traite des êtres humains.* Disponible sur : http ://www.unodc.org/documents/humantrafficking/2008/BP017TechnologyandHumanTrafficking.pdf . La base de données de l´UNODC sur la traite des personnes inclut aussi des cas impliquant l´utilisation d´annonces en ligne, https ://www.unodc.org/cld/index.jspx. Pour plus d´informations voir également https ://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html?ref=menuside

117 Ceci peut être applicable, par exemple, à l´exploitation sexuelle des enfants, quand des images créées « hors ligne » par des délinquants

Les pratiques juridiques nationales à cet égard sont examinées de manière plus détaillée dans le chapitre quatre (incrimination). Une des approches pourrait être l´inclusion, dans la description de la « cybercriminalité, des actes pour lesquels l´utilisation d´un système informatique est requise pour modifier fondamentalement la portée ou la nature desdits actes s´ils avaient été commis « hors ligne ».[117] Il est extrêmement difficile de définir ici une limite. Il est approprié de soutenir, par exemple, que l´utilisation de systèmes informatiques change la donne pour ce qui concerne la nature et la portée des fraudes à la consommation, mais non dans le cas du trafic de stupéfiants ? Est-ce que l´utilisation des services financiers en ligne pour dissimuler l´origine des profits criminels [118] est significativement différente des transactions fiancières traditionnelles pour que soit nécessaire la définition d´un délit séparé de blanchiment de capitaux lié à l´informatique ? Dans une certain mesure, la liste des 14 actes présentée dans l´étude est une tentative de recueillir les pratiques contemporaines pour les actes considérés comme des « cyberdélits ».

D´autres actes mentionnés par les pays, en particulier les paris en ligne, ne sont pas incriminés systématiquement par tous les pays. Les paris sur internet sont permis dans plusieurs pays, mais sont interdits directement ou indirectement dans d´autres pays.[119] Indépendamment de leur statut légal, les sites de paris sur internet peuvent fréquemment causer ou être l´objet de fraude informatique ou d´interception ou d´interférence de données informatiques.[120] Sous le terme général « pari en ligne », on fait parfois une distinction entre l´internet comme un simple support de communication – analogue aux paris à distance sur un évènement du monde physique par le biais de dispositifs de télécommunications – et le cas d´un casino « virtuel » casino dans lequel le joueur n´a pas la possibilité de vérifier les résultats du jeu.[121] Ces derniers, en particulier, sont souvent différents des paris hors ligne, en raison de la possibilité d´engagement compulsif, de fraudes [122] et d´abus commis par les mineurs. Conformément au principe de la souveraineté nationale, au moins une des approches régionales reconnait le droit des pays d´établir les objectifs de leurs politiques en matière de jeux et de paris, en conformité avec leur propre échelle de valeurs, et de définir des mesures restrictives proportionnées.[123] L´inclusion des paris en ligne dans une description générale de la cybercriminalité peut donc présenter des difficultés concernant l´universalité de leur incrimination.

Discussion

Il faut signaler que, hormis les 14 actes de cybercriminalité énumérés dans le questionnaire de l´étude, les pays répondants n´ont pas mentionné un grand nombre de conduites. Un certain degré de consensus peut donc exister pour ce qui concerne les principales conduites incluses dans le terme « cybercriminalité ».

Néanmoins, comme l´indique la présente étude, déterminer s´il est nécessaire d'inclure des conduites spécifiques dans une description de la « cybercriminalité » dépend en grande partie des fins recherchées lors de l´utilisation du terme « cybercriminalité ».

Du point de vue juridique international, la teneur du terme est particulièrement importante dans le cadre des accords de coopération internationale. Une caractéristique des instruments régionaux et internationaux sur la cybercriminalité, par exemple, est l´inclusion de pouvoirs d´enquêtes spécialisés qui ne sont généralement pas inclus dans les instruments qui ne concernent pas spécifiquement la cybercriminalité.[124]

---

sont ensuite partagées « en ligne » sur des réseaux de personnes aux vues similaires – les actes additionnels de distribution, de réception et de collecte de matériel « en ligne » sont de nouveaux délits pénaux. Une vue d´ensemble de ce scénario et des exemples supplémentaires sont disponibles dans : UK Home Office, 2010. *Stratégie de cybercriminalité* p.45.

118 Comité d´experts chargés de l´évaluation des mesures contre le blanchiment de capitaux et le financement du terrorisme du Conseil de l´Europe (MONEYVAL), 2012. *Flux financiers criminels sur iinternet : méthodes, tendances et contremesures intentées par de nombreuses parties prenantes.*

119 Fidelie, L.W., 2008. Paris sur internet : activité innocente ou cybercriminalité ? *Journal international de cybercriminologie*, 3(1) :476-491 ; Yee Fen, H., 2011. Paris en ligne : l´état des jeux à Singapour. *Journal juridique de l´Académie de Singapour* 23 :74.

120 Voir, par exemple, McMullan, J.L., Rege, A., 2010. La criminalité en ligne et les paris sur iinternet. *Journal sur les problèmes en matinée de jeux*, 24 :54-85.

121 Pereira de Sena, P., 2008. Interdiction de parier sur iinternet à Hong Kong : lois et politiques. *Journal juridique de Hong Kong*, 38(2) :453-492.

122 Voir, par exemple, Cour de justice européenne, *Sporting Exchange Ltd v Minister van Justitie*, Cas C-203/08. para 34 : *« en raison de l´absence d´un contact direct entre le consommateur et l´opérateur, les jeux de hasard accessibles via l´internet impliquent des risques différents et plus importants de fraude commise par les opérateurs en comparaison avec les marchés traditionnels pour ce type de jeux »*

123 *Ibid.* para 28.

124 Ces pouvoirs incluent des ordonnances pour la collecte des données informatiques stockées et des données informatiques en temps réel, et la conservation rapide des données informatiques. Voir, par exemple, le projet de convention de l´Union Africaine, le projet de loi type du COMESA, la loi type du Commonwealth, la Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes

Les états parties aux instruments conviennent de mettre ces pouvoirs à la disposition d´autres états parties à la suite d´une demande d´entraide judiciaire. Si la portée de certains instruments est vaste et leur permet d´utiliser ces pouvoir pour recueillir des preuves électroniques pour tout délit pénal,[125] d´autres limitent la portée de la coopération internationale et des pouvoirs d´enquête à la « cybercriminalité », ou à des « infractions relatives à l´information informatique ».[126] Dans le contexte international, les conceptions de « cybercriminalité » peuvent donc avoir des implications pour ce qui concerne la disponibilité des pouvoirs d´enquête et l´accès à des preuves électroniques extraterritoriales. Le chapitre sept (coopération internationale) examine cette question de manière détaillée.

Étant donné que le monde se dirige vers un accès universel à l´internet, les conceptions de la cybercriminalité devront peut-être fonctionner à de nombreux niveaux : de manière spécifique et détaillée quand il s´agit de la définition de certains actes individuels de cybercriminalité, mais de manière suffisamment ample, afin de garantir que les mécanismes relatifs aux pouvoirs d´enquête et à la coopération internationale puissent être appliqués, avec des garanties efficaces, à la constante migration des délits commis hors ligne vers leurs variantes en ligne.

125 Voir, par exemple, la Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes.
126 Voir, par exemple, l´Accord de la Communauté des états indépendants et le projet de convention de l´Union Africaine.

CHAPITRE DEUX : LA PERSPECTIVE D´ENSEMBLE

Après un bref aperçu des mesures visant à mesurer la cybercriminalité, le chapitre présente une perspective d´ensemble de « qui » (et combien) est impliqué dans « quel » cyberdélit (et dans quelle mesure). Il conclut que les actes de cybercriminalité sont largement distribués dans diverses catégories de cybercriminalité avec des taux de victimisation souvent plus élevés que ceux des délits conventionnels. Les profils des auteurs de ces délits dépendent du type d´acte de cybercriminalité et on estime que plus de 80 % des actes de cybercriminalité sont issus d´activités organisées.

2.1 Mesurer la cybercriminalité

Principaux résultats :

- les sources d´informations permettant de mesurer la cybercriminalité incluent les statistiques de délits enregistrés par la police ; (des enquêtes en population générale et en entreprises ; des initiatives de déclarations des victimes ; et des informations sur la cybersécurité technologique ;
- il est peu probable que les statistiques qui prétendent mesurer la cybercriminalité comme un phénomène global soient comparables à l´échelle internationale. Les données ventilées selon les différents actes de cybercriminalité offrent un niveau élevé de cohérence et de comparabilité ;
- bien que les statistiques sur les cyberdélits enregistrés par la police soient utiles pour définir les politiques et la prévention de la criminalité au niveau national, elles ne représentent généralement pas une base de comparaison au niveau international en matière de cybercriminalité. Des sources d´informations basées sur la technologie et sur des enquêtes peuvent toutefois fournir des aperçus intéressants ;
- de différentes sources d´informations sont utilisées dans cette étude, afin de traiter les questions « *qui* », « *quoi* » et « *combien* » relatives à la cybercriminalité.

Pourquoi mesurer la cybercriminalité ?

L´Article 11 des Principes directeurs applicables à la prévention du crime des Nations Unies[1] déclare que les mesures, les programmes, les politiques et les stratégies de prévention de la criminalité devraient s´appuyer « *sur une large base multidisciplinaire de connaissances des problèmes de la criminalité* ». Cette « base de connaissances » devrait inclure l´établissement de « systèmes de donnée ».[2] Le recueil des données, afin de planifier des interventions pour prévenir et réduire la criminalité est aussi importante dans la cybercriminalité que pour d´autres types de délits. Mesurer la cybercriminalité peut aussi servir à élaborer des initiatives pour la réduction de la criminalité ; à renforcer les interventions locales, régionales, nationales et internationales ; à identifier les lacunes des interventions ; à fournir des services de renseignement et d´évaluation des risques ; et à sensibiliser et informer le public.[3]

1 *Principes directeurs pour la prévention du crime*, annexe à la résolution 2002/13 du Conseil économique et social des Nations Unies sur les *Actions pour promouvoir une prévention efficace de la criminalité,* 24 juillet 2002.
2 *Ibid.* Art. 21(f).
3 Fafinski, S., Dutton, W.H. et Margetts, H., 2010. *Répertorier et mesurer la cybercriminalité.* Discussion du forum de l´institut internet Oxford. Document n°. 18. juin 2010.

Plusieurs commentateurs ont souligné la difficulté pour recueillir des informations sur la nature et l´étendue de la cybercriminalité.[4] Parmi ces difficultés figure tout d´abord le problème qui consiste à déterminer ce qui constitue un « cyberdélit » ; l´insuffisance du signalement et de l´enregistrement, les questions de méthodologie et de sensibilisation relatives aux enquêtes ; et les potentiels conflits d´intérêt pour les données du secteur privé.[5]

Quels délits devraient être mesurés ?

Le chapitre antérieur examine la teneur possible du terme « cybercriminalité ». À des fins de mesure, il s´agirait des actes inclus dans la première catégorie des actes cybercriminalité (actes contre la confidentialité, l´intégrité et la disponibilité des systèmes ou des données informatiques) et la troisième catégorie (actes liés au contenu informatique) qui sont clairement définis. Toutefois, la seconde catégorie (actes liés à l´informatique commis pour un bénéfice personnel ou financier ou pour porter préjudice) pourrait devenir plus ample. Comme cela a été indiqué, est ce l´implication de données ou de systèmes informatiques qui pourrait garantir qu´un délit soit enregistré comme un cyberdélit dans cette catégorie ? À cet égard, les approches peuvent varier, notamment pour ce qui concerne les délits enregistrés par la police. La partie ci-après sur les statistiques de la police traite ce problème de manière détaillée.

En général, il est clair que les statistiques qui prétendent mesurer la « cybercriminalité » comme un *simple phénomène* ne sont pas comparables à l´échelle internationale, en raison des variations significatives de la teneur du terme parmi les systèmes d´enregistrement. L´approche privilégiée sera donc vraisemblablement celle qui fournit des données ventilées pour chaque *acte distinct de cybercriminalité* – comme celles mentionnées dans la liste des 14 actes présentée au premier chapitre (connectivité et cybercriminalité). Cette approche offre un niveau plus élevé de cohérence et de comparabilité, et est en conformité avec les bonnes pratiques en matière de statistiques de justice pénale et de criminalité en général.[6]

Que souhaitons-nous savoir ?

Une approche pour mesurer les nouvelles formes et dimensions de la criminalité, y compris de la cybercriminalité, vise à définir « *qui* » (et *combien de personnes*) est impliqué dans « *quoi* » (et *dans quelle mesure*).[7] Ceci requiert la *convergence* de sources de données, telles que : des informations relatives aux auteurs des délits y compris les groupes criminels organisés ; des informations relatives aux flux dans les marchés illicites ; ainsi que des informations relatives au nombre d´activités criminelles, de dommages et de pertes, et les flux financiers illicites résultants. Chacun de ces éléments a des implications pour les mesures contre la cybercriminalité. La compréhension, par exemple, des réseaux et des structures d´un groupe criminel organisé est fondamental pour établir des mesures en matière de justice pénale. La compréhension des marchés illicites – comme l´économie souterraine basée sur les informations de cartes de crédits volées – fournit des détails sur les incitatifs sous-jacents des activités criminelles (indépendamment des individus ou des groupes impliqués) et donc des points d´entrée en matière de programmation de la prévention. La compréhension de l´étendue des dommages, des pertes et des gains financiers illicites fournit une orientation quant aux mesures prioritaires.

---

4 Voir, par exemple, Brenner, S.W., 2004. Paramètres de la cybercriminalité : vieux vin, bouteilles neuves? *Journal de droit & Technologie de Virginie*, 9(13) :1-52.
La cybercriminalité est aussi incluse comme un exemple de « délit émergent difficile à mesurer » dans les documents de la 42 ième Session Commission de statistique des Nations Unies. Conseil social et économique des Nations Unies, Commission de statistique, 2012. *Rapport de l´institut national de statistique et géographie de Mexico sur les statistiques criminelles.* E/CN.3/2012/3, 6 décembre 2011.

5 Fafinski, S., Dutton, W.H. er Margetts, H., 2010. *Répertorier et mesurer la cybercriminalité.* Discussion du forum de l´institut internet Oxford. Document n°. 18. juin 2010

6 Voir, par exemple, ONUDC, 2010. *Élaboration des normes pour les statistiques relatives à la justice et aux affaires intérieures : acquis international et de l´UE ;* ET Nations Unies, 2003. *Manuel pour l´élaboration d´un système de statistiques de la justice pénale.*

7 Institut européen pour la prévention et le contrôle du crime, affilié aux Nations Unies (HEUNI), 2011. Collecte de données sur les [Nouvelles] Formes et manifestations de la criminalité. *dans :* Joutsen, M. (ed.) *Nouveaux types de criminalité, Procédures du séminaire international tenu à l´occasion du trentième anniversaire de l´HEUNI*, 20 octobre 2011, Helsinki : EICPC. Voir aussi UNODC, 2010. *La globalisation du crime : évaluation des menaces de la criminalité organisée transnationale*

Quelles informations peuvent être recueillies ?

Il existe quatre sources principales d´informations pour mesurer « *quels* » actes de cybercriminalité sont commis et « *combien* » : (i) les statistiques des délits enregistrés par la police ; (ii) des enquêtes en population générale et en entreprises ; (iii) des initiatives de déclarations des victimes ; et (iv) des informations sur la cybersécurité technologique. La liste n´est pas exhaustive mais elle couvre les principales sources d´informations ayant un certain degré de comparabilité à l´échelle transnationale. D´autres sources incluent les études individuelles sur des phénomènes spécifiques, comme les techniques d´indexation URL ou les prises de contrôle des botnets.[8] L´Annexe deux de l´étude examine les difficultés et les points forts de chaque source. Il s´avère qu´actuellement, bien que les statistiques sur les cyberdélits enregistrés par la police soient utiles pour définir les politiques et la prévention de la criminalité au niveau national, elles ne représentent généralement pas une base de comparaison au niveau international en matière de cybercriminalité. Par contre, les résultats des sondages effectués et les informations relatives à la cybersécurité se basant sur la technologie, commencent à fournir des aperçus sur la nature et l´étendue de ce phénomène. Ces sources d´informations ont été utilisées pour aborder les questions « *quoi* » et « *combien* » en matière de cybercriminalité. La question « *qui* » est examinée dans la section suivante du chapitre sur les auteurs des cyberdélits.

2.2 La situation globale de la cybercriminalité

Principaux résultats :

- les actes de cybercriminalité sont répartis entre des actes commis pour un profit financier, des actes liés au contenu informatique et des actes contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques ;
- les perceptions des entreprises et des gouvernements relatives aux menaces et aux risques sont variables ;
- la victimisation des cyberdélits individuels est significativement plus élevée que dans le cas des formes « conventionnelles » de la criminalité. Les taux de victimisation des fraudes en ligne de cartes de crédit, le vol d´identité, les réponses à des tentatives d´hameçonnage, et faire l´objet d´un accès non autorisé à un compte, touchent entre 1 et 17 % de la population en ligne ;
- les taux de victimisation des cyberdélits individuels sont plus élevés dans les pays à faible niveau de développement, mettant en évidence la nécessité de renforcer les efforts de prévention dans ces pays ;
- les entreprises du secteur privé en Europe signalent des taux de victimisation allant de 2 à 16 % pour des actes tels que la violation de données par intrusion ou hameçonnage ;
- les outils criminels choisis pour commettre ces délits, comme les botnets, ont une portée mondiale. Plus d´un million d´adresses IP uniques fonctionnaient au niveau global comme des serveurs de contrôle et des commandes de botnets en 2011 ;
- le contenu internet devant être supprimé comme la pornographie infantile et les discours de haine, mais également les contenus liés aux critiques et aux diffamations à l´égard du gouvernement, soulèvent des préoccupations relatives aux lois sur les droits de l´homme dans certains cas ;
- on estime qu´environ 24 % du trafic global d´internet enfreint le droit d´auteur.

Cette section dresse un tableau de l´étendue et du caractère global de la cybercriminalité en se basant sur les données fournies par les pays, le secteur privé et le milieu universitaire lors de la collecte d´informations pour l´étude, ainsi que sur la révision de plus de 500documents publics.[9]

8 Voir, par exemple, Kanich, C. *et al.*, 2011. *Aucun plan ne survit au contact : expérience d´évaluation de la cybercriminalité* .Disponible à : http ://static.usenix.org/events/cset11/tech/final_files/Kanich.pdf ; Voir également Kemmerer, R.A., 2011. *Comment voler un Botnet et que peut-il se passer lorsque vous le faites.* Disponible à : http ://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6080765

9 Dossiers du Secrétariat.

Répartition des actes de cybercriminalité

Les actes de cybercriminalité se répartissent dans une vaste gamme d´infractions. Selon les perceptions des services répressifs, les actes commis avec une motivation financière, comme la falsification ou la fraude liée à l´informatique, représentent environ un tiers des actes commis à l´échelle mondiale. De nombreux pays ont mentionné que « *la fraude dans le paiement et le commerce électroniques* », « *la fraude sur des sites de ventes aux enchères comme ebay,* » « *la fraude par paiement anticipé de frais* », « *la cybercriminalité visant les informations personnelles et financières,* » et « *le schéma de fraude par email et les réseaux sociaux* » étaient particulièrement répandues.[10] Comme cela a été signalé précédemment, ce délit a un impact financier important.

Figure 2.1 : les actes plus communs de cybercriminalité enregistrés par la police nationale

Source : questionnaire de l´étude sur la cybercriminalité Q80. (n=61, r=140)

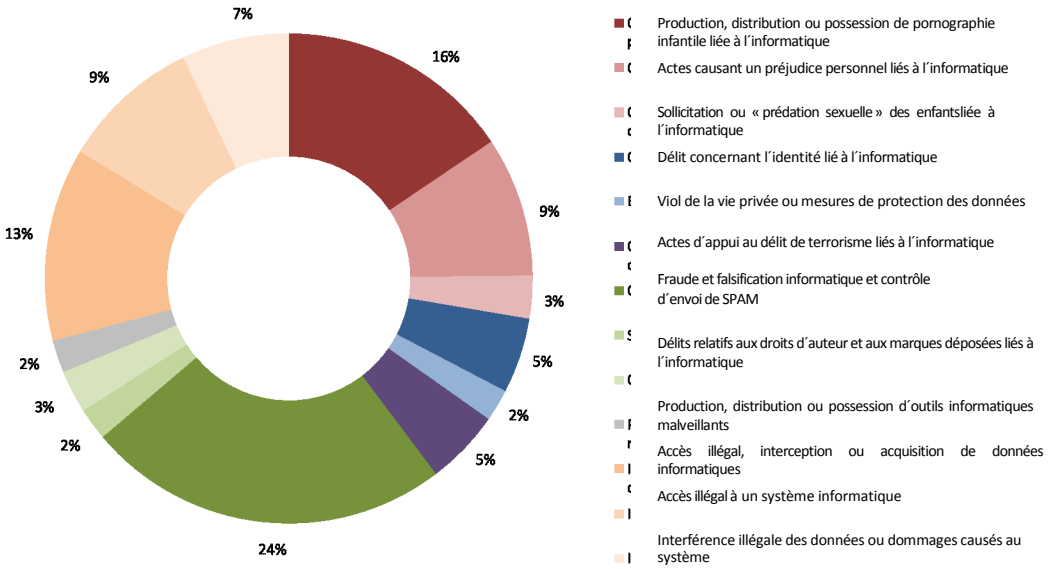
Un tiers des actes, et jusqu´à la moitié dans certaines régions, concernent le contenu informatique – y compris la pornographie infantile, le contenu relatif à des délits de terrorisme et les contenus enfreignant les droits de propriété intellectuelle. Les délits liés à la pornographie infantile étaient signalés plus fréquemment en Europe et en Amérique, qu´en Asie, en Océanie ou en Afrique – bien que ceci puisse être lié aux différences de priorité en matière d´application de la loi plutôt qu´à des différences sous-jacentes. D´autre part, les actes liés à l´informatique qui « causent un préjudice personnel, » étaient signalés plus fréquemment en Afrique, en Amérique, en Asie et en Océanie qu´en Europe. La discussion sur les actes liés au contenu examine ces tendances de manière plus détaillée.

Conformément aux perceptions des services répressifs, les actes contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques, comme « l´accès illégal à un système informatique », représentent entre un tiers et 10 % des actes, selon la région. Ces agissements font partie d´une gamme de cyberdélits et la capacité variable des pays pour identifier et poursuivre ces délits (plus techniques) peut affecter la perception de leur prévalence dans les régions.

10 Questionnaire de l´étude sur la cybercriminalité. Q80 et Q85.

D´autre part, comme il a été signalé précédemment, les enquêtes sur la victimisation suggèrent qu´il existe des différences, par exemple au niveau de l´accès informatique non autorisé. Ces différences ne sont pas toujours similaires à celles que perçoivent les services répressifs.

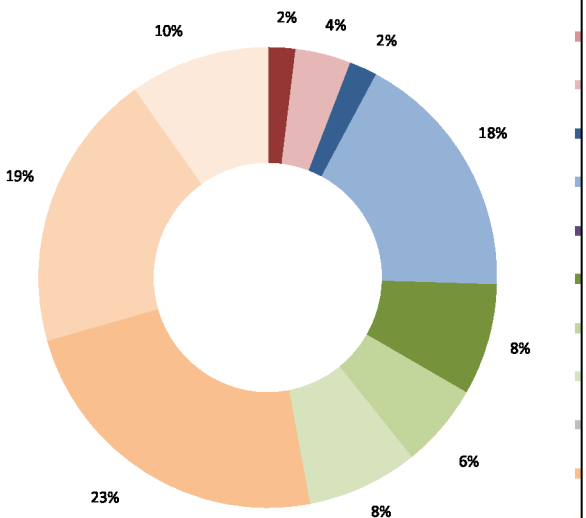
Figure 2.2 : les menaces les plus importantes en matière de cybercriminalité selon le point de vue des états membres



Source : questionnaire de l´étude sur la cybercriminalité Q81. (n=59, r=138)

La perception des menaces représentées par la cybercriminalité et sa prévalence varie en fonction de l´interlocuteur interrogé, et la comparaison des résultats fournis par les pays et le secteur privé en est un bon exemple. Interrogés sur les actes de criminalité qui représentent les menaces les plus significatives (en termes de gravité, de pertes ou de dommages), les réponses des services répressifs furent similaires à celles concernant les actes commis plus fréquemment – avec une répartition relativement égale entre les actes commis pour réaliser un gain financier, les actes liés au contenu, et les actes commis directement contre les données ou les systèmes informatiques.

Figure 2.3 : les menaces les plus importantes en matière de cybercriminalité selon le point de vue des organisations du secteur privé



Source : questionnaire de l´étude sur la cybercriminalité (secteur privé). Q56. (n=8, r=51

Contrairement à ce que l´on pourrait attendre, les organisations du secteur privé considèrent les *actes contre les systèmes informatiques* comme une menace plus significative que d´autres types de cyberdélits. L´accès illégal, l´interférence ou les dommages causés sont considérés par le secteur privé comme des menaces plus importantes que tous les autres types de cyberdélits. Ceci reflète une préoccupation majeure des organisations du secteur privé en matière de confidentialité, d´intégrité et de disponibilité de leurs données et systèmes informatiques. Lors de la collecte d´informations pour l´étude, les organisations du secteur privé ont mentionné les menaces et les risques principaux, en

y incluant « *l´accès non autorisé et l´exfiltration de la propriété intellectuelle* » ; « *l´intrusion sur notre site web de services bancaires* » ; « *les tentatives de piratage des systèmes de données des clients* » ; *« les attaques par intrusion* » ; « *les fuites d´information causées par les employés* » ; et « *des attaques par déni de services ».*[11] Comme cela a été signalé précédemment, toutes les organisations du secteur privé sont vulnérables à la cyber-victimisation et les coûts peuvent être considérables.

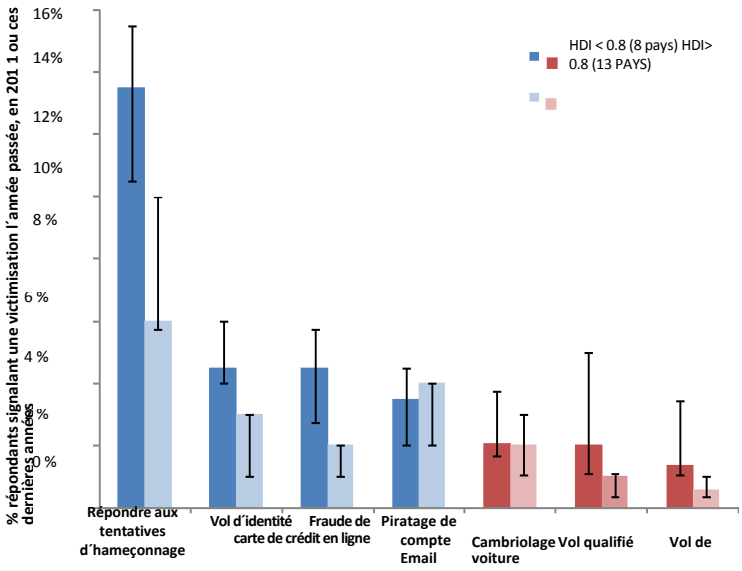
Prévalence et impact des actes de cybercriminalité

L´évaluation de la prévalence des actes de cybercriminalité peut être divisée entre la victimisation de la population générale (les consommateurs) et la victimisation des organisations – comme les entreprises, les institutions académiques et autres.[12]

La victimisation des consommateurs – pour la population générale, les niveaux de la victimisation de la cybercriminalité sont significativement plus élevés que pour les formes « classiques » de criminalité hors ligne – pour ce qui concerne les populations pertinentes à risque.[13] Par exemple, les taux de victimisation de la cybercriminalité pour 21 pays dans toutes les régions du monde, varient entre un et 17 % de la population en ligne pour quatre actes spécifiques :la fraude de cartes de crédit en ligne, le vol d´identité ; les réponses à des tentatives d´hameçonnage ; et l´accès non autorisé à un compte email.[14] Par contre, les sondages sur la victimisation révèlent que – dans le cas de ces 21 pays – les taux de victimisation de la criminalité « classique », pour des délits de cambriolage, de vol qualifié et de vol de voiture, varient entre 0,1 et 13 %, et la majorité des taux pour ces délits est inférieure à quatre %.[15] Un des facteurs responsable de ces différences est vraisemblablement le caractère « massif » de nombreux actes de cybercriminalité.

Pour des actes tels que l´hameçonnage ou « les attaques par force » des mots de passe d´un compte email pour obtenir un accès non autorisé, un seul individu peut cibler simultanément plusieurs victimes, comme il serait impossible de le faire avec des formes de délits classiques.

Figure 2.4 : victimisation de la cybercriminalité et de la criminalité classique



Source : ONUDC élaboration du rapport Norton sur la cybercriminalité et les sondages sur la victimisation de la criminalité.

11 Questionnaire de l´étude sur la cybercriminalité (secteur privé). Q50-52 et Q56.
12 La victimisation des institutions est exclu du champ de cette étude.
13 Tous les individus pour la criminalité « classique » et les utilisateurs d´internet pour la cybercriminalité.
14 Symantec, 2012. *Rapport Norton sur la cybercriminalité 2012*. Les recherches relatives au rapport Norton sur la cybercriminalité ont été effectuées de manière indépendante par StrategyOne (aujourd´hui EdelmanBerland) avec un sondage en ligne dans 24 pays en utilisant des questions identiques traduites dans la langue officielle de chaque pays. Les entretiens ont été réalisés entre le 16 juillet 2012 et le 30 juillet 2012. La marge d´erreur pour l´échantillon total des adultes (n=13,018) est de +0,9 % avec 95 % de niveau de fiabilité. Des données de 3 pays du rapport Norton sur la cybercriminalité sont exclues car les données sur la victimisation de la criminalité classique n´étaient pas disponibles. Les taux de victimisation se réfèrent à la prévalence de la victimisation sur 12 mois.
15 Les analyses des résultats de l´enquête internationale sur la victimisation criminelle (EIVC) et l´enquête nationale sur la victimisation criminelle de l´ONUDC.

Le second patron observé est que les taux de victimisation de la cybercriminalité (du moins pour l´échantillon des 21pays) sont généralement plus élevés dans les pays à faible développement. La division des pays en deux groupes - ceux dont l´indice de développement humain est inférieur à 0.8 (Groupe 1), et ceux dont l´indice est supérieur à 0.8 (Groupe 2)[16] – révèle des taux de victimisation plus élevés dans les pays moins développés (Groupe 1) pour ce qui concerne l´accès non autorisé à un compte email, le vol d´identité et les réponses à des tentatives d´hameçonnage. La victimisation en matière de cartes de crédit est légèrement plus élevée dans le groupe des pays plus développés. La figure montre le taux moyen de victimisation pour ces quatre type de cyberdélits, ainsi que le taux moyen de cambriolage, de vol qualifié et de vol de voiture, dans les deux groupes de pays.[17]

Le patron observé d´un taux plus élevé de victimisation de la cybercriminalité dans les pays moins développés concorde avec les taux plus élevés de criminalité classique dans les pays moins développés. En matière de criminalité classique, cette différence est due à de nombreux facteurs, y compris des disparités de revenu, des difficultés économiques, des populations jeunes, l´urbanisation, une histoire marquée par des conflits, une prolifération des armes à feu et des systèmes de justice pénale dénués de ressources.[18] Certains de ces facteurs ont moins d´importance en matière de cybercriminalité. D´autres, toutefois, tels que les pressions démographiques et économiques, font probablement partie de la problématique de la cybercriminalité. Dans les pays moins développés, les victimes de la cybercriminalité pourraient en principe être la cible de délinquants localisés n´importe où dans le monde. Cependant, en fonction des facteurs linguistes, locaux et culturels, les victimes potentielles pourraient être la cible de délinquants de leur propre pays – et le facteur de risque associé aux délinquants du même pays est important. De plus les utilisateurs d´internet des pays en développement font souvent face à des difficultés en raison d´une sensibilisation insuffisante en matière de cybersécurité – ce qui les rend souvent vulnérables à des délits tels que l´accès non autorisé, l´hameçonnage et le vol d´identité.[19] Ce patron concorde également avec le fait que – en dépit du patron suggéré par les enquêtes sur la victimisation – les services répressifs des pays moins développés ne perçoivent pas les actes de cybercriminalité tels que l´accès illégal comme étant particulièrement fréquents.[20]

Par contre, les fraudes de cartes de crédit en ligne montrent un patron opposé. Les taux de victimisation pour ce délit sont essentiellement équivalents et peut être légèrement plus élevés dans les pays plus développés. Il est vraisemblable que ce patron soit partiellement associé aux différences quant à la possession et l´utilisation en ligne de cartes de crédit, ainsi qu´aux différences relatives au ciblage de victimes dues aux perceptions de la valeur de celles-ci. EUROPOL, par exemple, signale que des niveaux élevés de fraudes de cartes de crédit sans présentation de la carte sont le résultat de transactions illégales et de violation de données et affectent les cartes de crédit de l´UE.[21]

La victimisation généralisée des consommateurs en matière de cybercriminalité entraîne des coûts financiers importants – directs et indirects. Les coûts financiers directs et indirects incluent le retrait d´argent des comptes de la victime, le temps et les efforts exigés pour réinitialiser les authentifiants des comptes ou réparer des systèmes informatiques, ainsi que des coûts secondaires comme les comptes mis à découvert. Les coûts indirects correspondent à l´équivalent monétaire des pertes imposées à la société par l´existence (en général) d´un phénomène déterminé de cybercriminalité. Les coûts indirects incluent la perte de confiance dans les services bancaires en ligne et une moindre utilisation des services électroniques. Le coût global de la cybercriminalité pour la société pourrait également inclure « les coûts de défense » des services et des produits de cybersécurité, ainsi que les efforts de détection et de répression.[22]

Les consommateurs victimes de la cybercriminalité dans 24 pays du monde signalent avoir souffert des pertes directes allant de 50 à 850 dollars US à la suite d´un incident de cybercriminalité au cours d´une année.[23]

16 Groupe 1 : HDI moyenne=0.69, médiane=0.7 ; Groupe 2 : HDI moyenne =0.89, médiane =0.90, l´indice de développement humain représente une mesure composite de développement économique et social. Voir http ://hdr.undp.org/en/statistics/hdi/

17 Les moyennes sont calculées comme des médianes des taux de victimisation pour chaque groupe de pays. Les barres représentent les quartiles supérieurs et inférieurs.

18 Voir, par exemple, ONUDC, 2005. *Criminalité et développement en Afrique* ; et ONUDC, 2007. *Criminalité et développement en Amérique centrale.*

19 Voir, par exemple, Tagert, A.C., 2010. *Difficultés en matière de cybersécurité dans les nations développées.* Dissertation. Document 22 ; et Grobler, M., et al.,
2010. évaluation de la sensibilisation en matière de cybersécurité en Afrique du sud *dans* : Ottis, R. (ed.) 2011. *Les procédures de la 10ème conférence européenne sur la guerre informatique et la sécurité* Talinn : Centre coopératif d´excellence pour la cyber défense.

20 Pour ce qui concerne, par exemple, montrées dans la Figure 2.4.voir ci-dessus

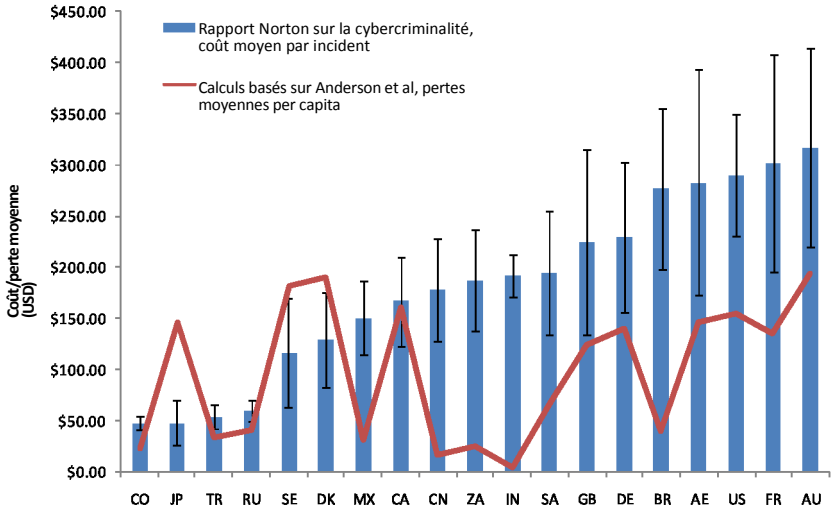
21 Europol, 2012. *Rapport de situation. Fraude par carte de paiement dans l´Union européenne. Point de vue des organismes d´application de la loi.*

22 Voir, par exemple, Anderson, R., et al., 2012. Mesurer les coûts de la cybercriminalité. *11ème atelier annuel sur l´économie de la sécurité de l´information*, WEIS 2012, Berlin, 25-26 juin 2012.

23 Symantec, 2012. *Rapport Norton sur la cybercriminalité 2012.* Les questions de l´enquête demandaient à toutes les personnes qui avaient déclaré être victimes d´un cyberdélit durant les 12 derniers mois, le montant des pertes financières subies à cause du fait de commettre ce cyberdélit durant ces 12 derniers mois. Les répondants étaient interrogés sur le montant total des pertes, y compris les montants volés et les coûts de réparation et de résolution. Les données relatives aux pertes totales annuelles étaient présentées en devises locales puis converties en USD à des fins de comparaisons transnationales.

Environ 40 % des coûts signalés consistaient en une perte financière causée par une fraude, presque 20 % était causé par un vol ou une perte, 25 % par des réparations, et le restant par la résolution du cyberdélit ou par un autre type de perte financière.[24]La figure 2.5 montre les pertes moyennes signalées par les pays de cette enquête.[25] Les différences entre les pertes moyennes signalées par les pays sont probablement dues à de nombreux facteurs, comme le type de victimisation concernant la cybercriminalité, l´efficacité des mesures de cybersécurité, et la mesure dans laquelle les victimes utilisaient l´internet pour des paiements ou des services bancaires en ligne. Les coûts estimés par les victimes elles-mêmes n´incluaient pas les coûts indirects et de défense. À des fins de comparaison, la figure montre également les coûts totaux estimés de la cybercriminalité (y compris les coûts directs, indirects et de défense) par personne, en se basant sur des calculs provenant de la documentation disponible.[26] Les niveaux absolus des deux figures ne sont pas comparables– l´un est le coût direct moyen par victime, l´autre représente les coûts totaux divisés par la totalité de la population. Néanmoins, les patrons relatifs montrent un certain degré de correspondance. Lorsque surgissent des différences importantes, un facteur qui y contribue peut être les différences relatives à la pénétration d´internet et à la répartition des coûts dans la société. Répartir les pertes causées par la cybercriminalité dans une vaste population où tous n´ont pas accès à l´internet – comme dans les pays les moins développés, par exemple – aura pour effet la réduction apparente des pertes moyennes *per capita*. Cet effet est clairement visible dans la figure dans le cas de nombreux pays en développement, où le patron des pertes totales estimées per capita ne concorde pas avec le patron des pertes directes signalées par les consommateurs. Dans ces cas, il est vraisemblable que le patron sous-jacent concorde davantage avec le patron suggéré par les enquêtes de victimisation. Par contre, dans le cas des pays hautement développés avec des coûts pour les consommateurs relativement bas, les pertes totales estimées per capita sont plus élevées que les pertes des consommateurs auxquelles on aurait pu s´attendre –ce qui suggère d´importants coûts indirects et de défense supplémentaires dans ces pays.

Figure 2.5 : coûts estimés de la cybercriminalité par les consommateurs, par pays



Source : rapport de Norton sur la cybercriminalité et élaboration d´ Anderson et al.de l´ONUDC

La victimisation du secteur privé– les techniques de cybercriminalité révolutionnent les délits classiques commis pour un gain financier et de fraude à l´encontre des organisations du secteur privé. Des possibilités criminelles croissantes de non seulement pouvoir frauder une entreprise mais également obtenir des données financières et personnelles stockées au travers d´une violation de données, a entraîné la perception d´une hausse significative du risque de cybercriminalité dans le secteur privé. [27]

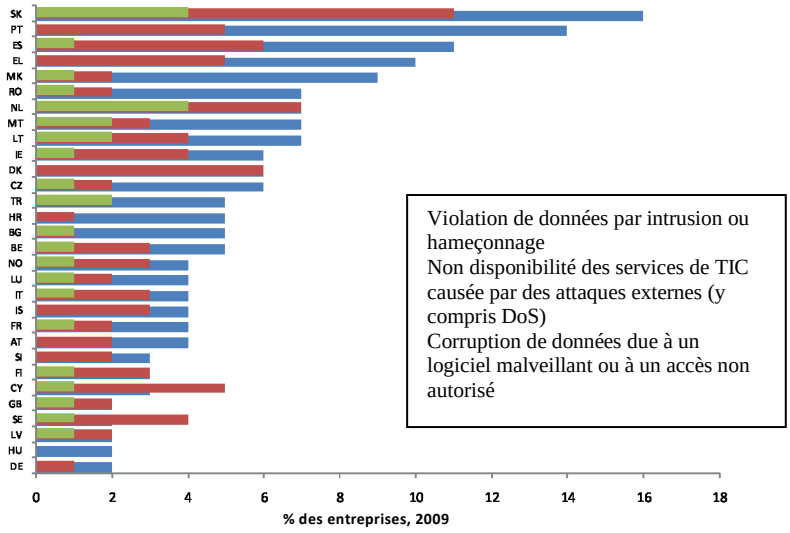
24 *Ibid.*

25 La figure exclut les pays où l´erreur type de l´estimation était supérieure à 0.5. Ceci était notamment le cas pour certaines des estimations de pertes signalées les plus élevées.

26 ONUDC calculs de Anderson, R., *et al.*, 2012. *Mesurer les coûts de la cybercriminalité.* Les estimations globales de cette source étaient attribuées aux pays sur la base de la part du PIB.

Par ailleurs, une utilisation accrue des innovations telles que l´informatique en nuage, présente un mélange de difficultés et de bénéfices en termes de cybersécurité.[28]

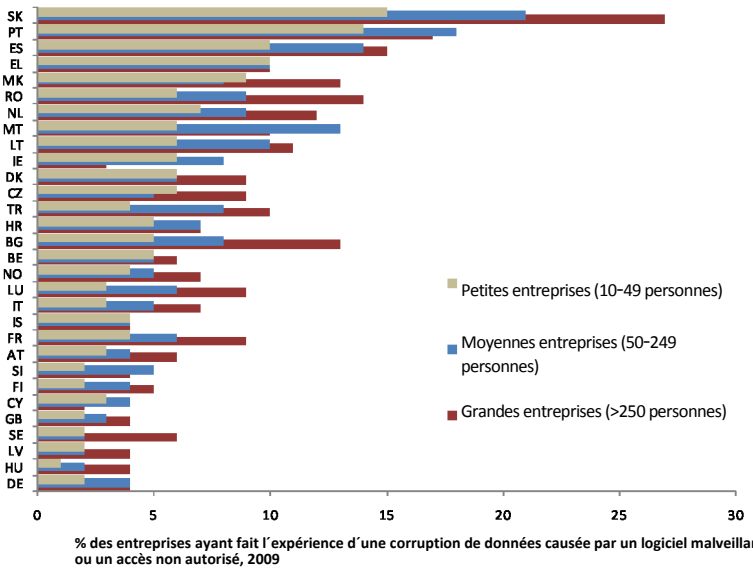
Figure 2.6 : cybercriminalité et victimisation des entreprises



Source : Eurostat enquête communautaire sur l´utilisation des TIC et du commerce électronique dans les entreprises

Il est difficile d´obtenir et d´interpréter les données sur la victimisation du secteur privé.[29] Les données relatives aux pays européens suggèrent que le taux de victimisation du secteur privé concernant la cybercriminalité pour des actes tels que « la violation des données par intrusion ou hameçonnage », « les interférences causées par des attaques externes », et « « les interférences avec les données causées par un accès illégal au système » sont généralement comparables aux problèmes d´accès non autorisé, d´hameçonnage et de crédit en ligne expérimentés par les consommateurs. Entre deux et 16 % des entreprises en Europe, par exemple, ont déclaré avoir connu un problème de corruption des données causé par un accès non autorisé ou un logiciel malveillant durant l´année 2010.[30] La corruption des données causée par un accès non autorisé est plus fréquente que la non disponibilité des services de TIC causée par des attaques externes (entre un et 11 %), qui sont elles mêmes plus fréquentes que la violation de données par intrusion ou par hameçonnage (entre zéro et quatre %).

Figure 2.7 : victimisation des entreprises par taille



Source : Eurostat enquête communautaire sur l´utilisation des TIC et du commerce électronique dans les entreprises.

27 Voir, par exemple, KPMG, 2011. *Rapport sur la cybercriminalité 2011.* Près de la moitié des décideurs en matière de sécurité des entreprises a signalé que le niveau global de risques de cybercriminalité auquel fait face leur entreprise a augmenté lors des 12 derniers mois. Seul 6 % ont signalé qu´il avait diminué. Europol signale que les principales sources de données illégales lors des enquêtes sur des fraudes sans présentation de cartes sont les violations de données des commerçants et des centres de traitement pour cartes de crédit, facilitées par la complicité interne et par l´utilisation de logiciels malveillants (Europol, 2012.*Rapport de situation. Fraude par carte de paiement dans l´Union européenne. Point de vue des organismes d´application de la loi.*).

28 PricewaterhouseCoopers, 2012.*l´œil du cyclone. Principales conclusions de l´étude mondiale sur la sécurité de l´information de 2012.*

29 Voir l´Annexe deux (Mesurer la cybercriminalité).

30 Eurostat, 2011. *Enquête communautaire sur l´usage des TIC et le commerce électronique dans les entreprises.* L´enquête couvrait 149 900 entreprises sur un total de 1,6 million de l´UE 27.

Cependant, ceci varie en fonction de la manière dont les questions sont posées et de la perception des répondants de ce qui constitue une « violation des données », une « intrusion », une « non disponibilité des services de TIC », ou d´un « logiciel malveillant ». Une enquête qui couvre les organisations du secteur privé dans cinq pays signale, par exemple, des taux de victimisation d´entreprises extrêmement élevés – entre 1.1 et 1.8 *« cyber-attaques réussies par organisation étudiée par semaine ».*[31] Ces résultats sont probablement fortement influencés non seulement par la perception de ce qui constitue une « cyber-attaque » dans une entreprise,[32] mais également par la taille de l´infrastructure informatique de l´entreprise qui peut faire l´objet d´une attaque. Ce sondage, par exemple, était axé sur des organisations de plus de 1000 « sièges d´entreprise » – définis comme des connexions directes au réseau et aux systèmes de l´entreprise.[33]

Un risque plus important pour les grandes entreprises en matière de cybercriminalité est corroboré par les données relatives au secteur privé européen. La proportion des entreprises en Europe qui ont été victimes d´une corruption de données causée par un logiciel malveillant ou un accès non autorisé est plus élevée dans le cas des grandes entreprises (plus de 250 personnes) (deux à 27 %) que dans celui des moyennes entreprises (50-249 personnes) (deux à 21 %), ou que dans celui des petites entreprises (10-49 personnes) (un à 15 %).

Outre « la surface d´attaque disponible », ces différences peuvent aussi être liées à la perception des délinquants que les entreprises plus grandes représentent des cibles de plus grande valeur. Cependant, il est également possible que les petites et moyennes entreprises aient une moindre capacité pour identifier les attaques. Environ 65 % des grandes entreprises ont mentionné avoir une politique formellement établie en matière de TIC, alors que c´est le cas pour 43 % des moyennes entreprises et pour seulement 22 % des petites entreprises.[34]

Outils criminels – les botnets

Une caractéristique distinctive du paysage actuel de la cybercriminalité est l´usage massif d´outils informatiques malveillants pour de nombreux cyber délits. Les « Botnets » (un terme provenant des mots « robot » et « réseau ») est un réseau d´ordinateurs interconnectés et contrôlés à distance, généralement infectés avec un logiciel malveillant qui transforme les systèmes infectés en « bots », « robots », ou « zombies ».[35] Les propriétaires légitimes de ces systèmes ignorent souvent l´infection. Les zombies dans le botnet connecté aux ordinateurs contrôlés par les délinquants (connus comme « serveurs de commande et de contrôle » ou C&Cs) ou à d´autres zombies, afin de recevoir des instructions, télécharge des logiciels supplémentaires et retransmet des informations recueillies dans le système infecté.

Étant donné que les botnets peuvent être utilisés à de nombreuses fins – y compris des attaques DDoS, des envois de spam, le vol d´informations personnelles, l´hébergement de sites malveillants et la distribution de charges d´autres logiciels malveillants [36] – ils représentent un outil privilégié pour la cybercriminalité. De nombreux pays répondants ont souligné l´augmentation de l´utilisation de botnets dans des cyberdélits lors des cinq dernières années.[37] Du point de vue du droit pénal, l´installation d´un logiciel malveillant dans un système informatique personnel ou d´une

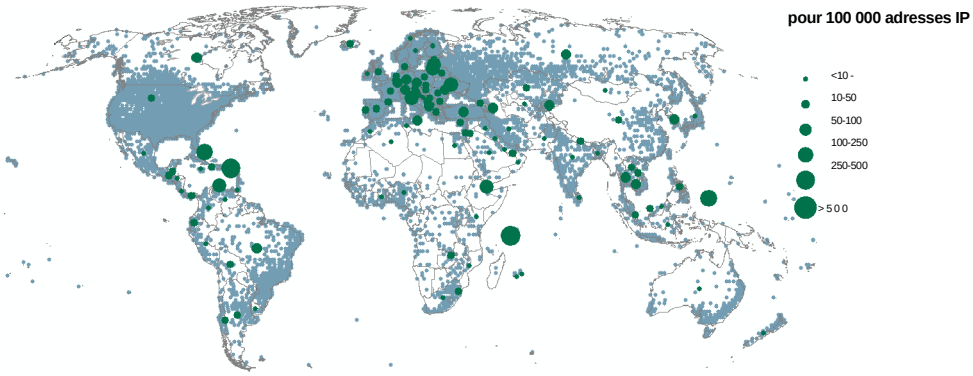
31 HP/Ponemon, 2012. *Étude sur le coût de la cybercriminalité AU, DE, JN, GB et US.*
32 Les résultats des sondages sont donc plus fiables lorsque la question est posée sur l´expérience d´un évènement défini. Voir UNODC/UNECE, 2010.*Manuel sur les enquêtes de victimisation.*
33 *Ibid.*
34 Eurostat, 2011. Statistiquesen bref 7/2011. ICT sécurité dans les entreprises, 2010.
35 OECD, 2008. *Logiciel malveillant (Maliciel). Une menace de sécurité pour l´économie d´iinternet.* DSTI/ICCP/REG(2007)5/FINAL. 28 avril 2008.
36 Hogben, G. (ed.) 2011. *Botnets : Détection, Mesure, Désinfection et Défense.* Agence européenne chargée de la sécurité des réseaux et de l´information (ENISA).
37 Questionnaire de l´étude sur la cybercriminalité .Q84.
38 Voir la première Annexe (descriptions des actes). Voir aussi NATO Centre coopératif d´excellence pour la cyber défense et ENISA, 2012. *Les implications juridiques de la lutte contre les Botnets.*

entreprise peut équivaloir à un accès illégal à un système informatique, et/ou à une interférence illégale avec des données ou des systèmes informatiques.[38]

Dans les pays où les outils informatiques malveillants sont pénalisés, le fait de créer, vendre, posséder ou distribuer des logiciels debotnet peut aussi être considéré comme un délit pénal. De plus, l´utilisation d´un botnet pour des profits criminels peut constituer une gamme d´infractions comme l´accès illégal, l´interception ou l´acquisition de données informatiques ; la fraude informatique ; les infractions liées à l´informatique concernant l´identité ; et l´envoi ou le contrôle de l´envoi de spam.[39]

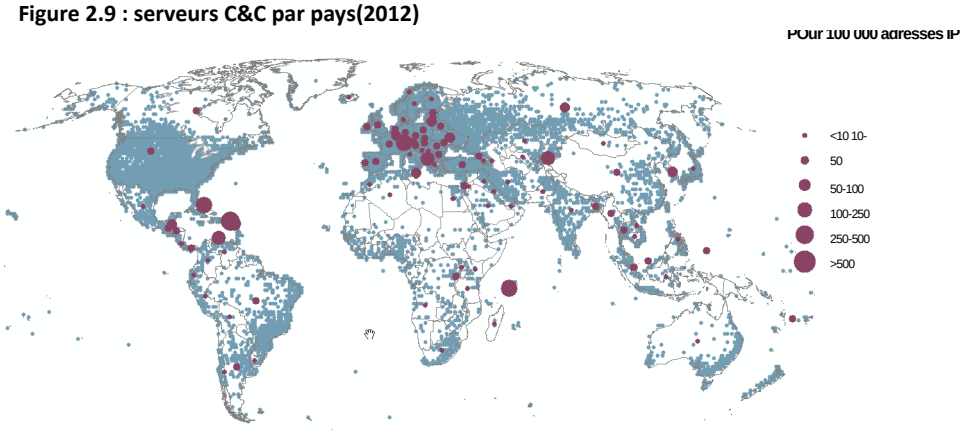
Répertorier les C&Cs et les zombies – étant donné que les botnets facilitent une vaste gamme d´actes de cybercriminalité, la connaissance de la localisation et de l´étendue des botnets de C&Cs et de zombies constitue une approche importante pour définir « la cybercriminalité globale ». Les estimations suggèrent que plus d´un million d´adresses IP uniques fonctionnaient au niveau global comme des C&C en 2011.[40] La répartition des C&Cs[41] identifiés est présentée dans les figures 2.8 et 2.9 pour les années 2011 et 2012, pour 100 000 adresses IP de pays.[42] Hormis un regroupement de C&C dans des pays de l'Europe de l´est, le nombre de C&C est élevé par rapport au nombre total d´adresses IP de pays en Asie centrale, de l´ouest et du sud-est ainsi qu´en Amérique centrale et dans les Caraïbes . Bien que le nombre absolu de C&C soit élevé dans les pays d´Amérique du nord, d'Europe occidentale et d´Asie de l´est, les taux relatifs de C&C de ces pays sont bas, en partie à cause du nombre élevé des connexions internet et des adresses IP résultantes.

Figure 2.8 : serveurs C&C, par pays (2011)



Source : UNODC élaboration des donnés de Team Cymru.

Figure 2.9 : serveurs C&C par pays(2012)



Source : UNODC élaboration des données de Team Cymru.

39 *Ibid.*

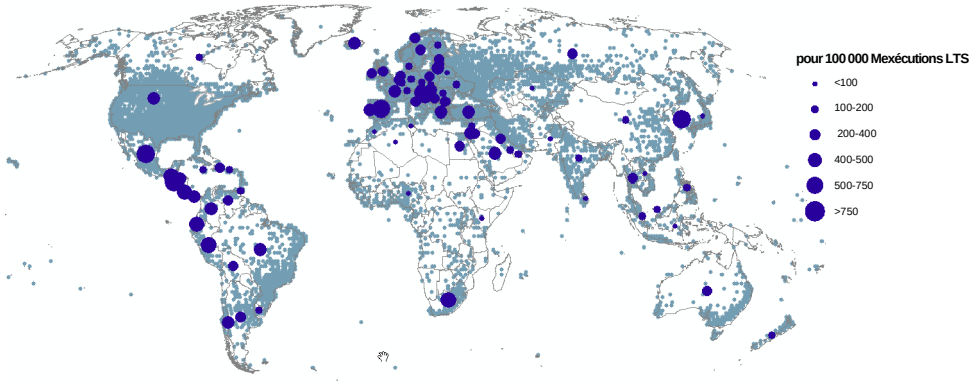
40 Estimations basées sur les données de Team Cymru.

41 Données correspondant aux adresses IP identifiées en 2011 ou 2012 opérant comme un IRC (discussion relayée par internet) ou un serveur C&C http (protocole de transfert hypertexte).

42 Données de Team Cymru. Les taux de C&C par pays sont en vert (2011) et en violet (2012), la géolocalisation de toutes les adresses IP globales est en bleu (données de MaxMind). Le traçage des C&C identifiés pour chaque 100 000 adresses IP de pays permet une meilleure comparabilité que le traçage des nombres absolus de C&C. La géolocalisation des adresses IP des C&C est assujettie à de nombreuses difficultés, entre autre l´utilisation de connexions proxy. Toutefois, la localisation au niveau national est généralement considérée comme acceptable.

À l´inverse, un faible nombre de C&C dans un pays ayant une connectivité limitée peut créer un taux élevé de C&C – de la même manière que quelques crimes commis sur une petite île peuvent créer un taux « élevé » de criminalité. La répartition globale des serveurs de C&C n´est pas nécessairement liée à la localisation des auteurs, ou des « éleveurs » de bot, qui contrôlent les C&C et leurs bots à des fins de profit. La localisation des serveurs de C&C peut être fréquemment déplacée pour éviter la détection, et peut inclure l´utilisation de systèmes « innocents » corrompus.[43] L´éleveur de bot n´a donc pas besoin d´être géographiquement proche de ses C&C. Toutefois, un lien local– notamment linguistique – peut exister entre les auteurs du délit et des fournisseurs d´hébergement, y compris les fournisseurs « pare balles ».[44] La section de ce chapitre sur les « auteurs des cyberdélits, » signale également l´existence de plates-formes d´auteurs de cyberdélits en Europe de l´est – ceci correspond au patron de taux élevés de C&C dans cette sous-région.

Figure 2.10 : infections de Botnet, par pays (2010)



Source : ONUDC élaboration du rapport sur les renseignements de sécurité de Microsoft

Les ordinateurs infectés (zombies) sont l´autre partie de la problématique des C&C. À l´échelle mondiale, au moins sept millions d´ordinateurs pourraient faire partie d´un botnet.[45] D´autres estimations considèrent que ce chiffre est plus élevé.[46] La figure 2.10 montre la répartition approximative de ces infections, par pays.[47]

Le patron de répartition de l´infection est différent de celui des C&C. Les zombies sont rassemblés plus massivement en Europe occidentale (contrairement à l´Europe de l´est pour les C&C), et il existe des taux importants d´infection en Amérique centrale et en Amérique du sud, ainsi que dans certains pays d´Asie de l´est. Cette répartition tend à représenter des pays ayant un nombre élevé d´utilisateurs actifs d´ordinateurs.

L´estimation du nombre total des zombies et des botnets comporte d´importantes limitations. Deux importantes distinctions méthodologiques qui affectent les estimations incluent le « *l´empreinte* » du botnet versus « *la population vivante* »,[48] et la quantification des « *adresses IP* » des zombies versus « *les dispositifs uniques* »[49] À cet égard, il faut signaler que (en raison des facteurs méthodologiques) l´estimation des C&C concerne les adresses IP uniques, alors que l´estimation des zombies concerne les ordinateurs. Les deux chiffres globaux ne sont donc pas aisément comparables.

43 De plus, dans des botnets P2P plus récents, un ordinateur zombie peut être un client ou un serveur, ce qui exclut la nécessité d´un serveur particulier pour que les bots téléchargent des programmes ou reçoivent des instructions.

44 Pour ce qui concerne les fournisseurs d´hébergement voir, par exemple, HostExploit et Group IB, 2012. Rapport sur le *Top 50 des mauvais hébergeurs et des mauvais réseaux.*

45 Calculs de l´UNODC basés sur le *rapport sur les renseignements de sécurité* de Microsoft, 2010. Volume 9. Figure du premier trimestre de 2010. Cette estimation est du même ordre de grandeur que celle de Symantec, 2011. *Rapport sur les menaces à la sécurité sur internet. 2011*. Volume 17 (estimation de 4,5 millions pour 2010).

46 Voir, par exemple, Acohido, B., 2010. Y a-t´il 6,8 millions – ou 24 millions – d´ordinateurs en bot sur iinternet ? *Le dernier surveillant.* Disponible sur : http ://lastwatchdog.com/6-8-million-24-million-botted-pcs-internet/

47 Les zombies sont tracés comme des infections de bot identifiées par 100 000 exécutions par l´outil de suppression des logiciels malveillants de Microsoft. Données de Microsoft, 2010. *Rapport sur les renseignements de sécurité* de Microsoft. Volume 9. La méthodologie couvre seulement les machines exécutant une mise à jour Windows update (environ 600 millions de machines dans le monde) et identifie seulement les infections de bot les plus répandues. Néanmoins, des méthodologies indépendantes ont trouvé des niveaux similaires d´infections calculés sur une base individuelle de pays. Voir, par exemple, van Eeten, M.J.G. *et al.*,

2011. *Fournisseurs de services internet et mitigation de botnets. Une étude documentaire sur le marché hollandais.* Faculté de gestion et de politique technologique, Université de technologie de Delft.

48 Les zombies abandonnent et s´unissent continuellement aux botnets car de nouvelles machines sont infectées et les zombies existantes sont nettoyées. De plus, les machines infectées peuvent souffrir de multiples infections ou migrer temporairement d´un botnet à l´autre (Abu Rajab, M., et al., 2007. Mon Botnet est plus grand que les tiens (et peut être, meilleur que les tiens) : pourquoi l´estimation des tailles reste difficile). *Procédures de la première conférence sur le premier atelier relatif aux thèmes sensibles de la compréhension des botnets.* Berkeley, CA : Usenet Association. L´empreinte du botnet fait référence au nombre total de machines infectées avec le temps. La population vivante du botnet indique le nombre de machines infectées simultanément connectées à un serveur C&C.

49 Un nombre spécifique d´adresses IP identifiées ne correspond généralement pas au nombre de dispositifs en raison de deux effets de réseau : (i) l´attribution de différentes adresses IP à court terme au même dispositif (DHCP dynamique), et (ii) le partage d´une seule adresse IP entre plusieurs dispositifs (NAT). Selon la taille du DHCP et les effets NAT, le nombre d´uniques adresses IP peut être supérieur ou inférieur au nombre correspondants de dispositifs. En raison du taux élevés d´IP dynamiques de DHCP des FSI commerciaux, le nombre d´adresses IP observé est généralement beaucoup plus élevé que le nombre de dispositifs.

En effet, pour estimer la taille d´un botnet individuel, il est probable que la technique généralement utilisée qui trace les adresses IP uniques des zombies pendant de longues périodes de temps, surestime beaucoup le nombre de dispositifs infectés.[50] Bien que l´estimation de la taille des botnets reste discutable, les preuves suggèrent que les éleveurs de bots réussissent à contrôler des groupes de dizaines ou de centaines de milliers d´ordinateurs infectés – plutôt que le chiffre souvent signalé de « millions » de dispositifs.[51] Sur cette base, il est vraisemblable que le nombre total de grands botnets criminels « commerciaux » dans le monde soit comparativement faible. De plus, il peut exister un nombre beaucoup plus élevé de petits botnets « amateurs » , avec de faibles populations de zombies.[52]

Exemple d´informations obtenues par des botnets : « Torpig »

- Des domaines C&C ont été contrôlés par des chercheurs universitaires durant une période de 10 jours
- 183 000 machines zombies ont été identifiées durant ces 10 jours. La moyenne de la population zombie vivante était de 49 000. La plupart des zombies se situaient probablement en Europe du nord et en Amérique du nord
- Les renseignements relatifs à 8300 comptes de 400 différentes institutions financières furent envoyés sur les serveurs C&C
- Les renseignements relatifs à 1700 cartes de crédit furent envoyés sur les serveurs C&C
- Les mots de passe et les noms d´utilisateurs des sites de réseaux sociaux et de messagerie web de 298 000 victimes furent envoyés sur les serveurs C&C
- La bande passante globale de zombies était suffisante pour lancer une attaque DDoS massive

Source : Stone-Gross *et al.*

Les dommages – ces réseaux malveillants peuvent causer des dommages importants. Il s´est avéré que durant une seule période de 10 jours, un botnet d´environ 183 000 machines zombies s´est approprié des renseignements et des authentifiants des comptes bancaires, des cartes de crédit, des réseaux sociaux et des messagerie web de près de 310 000 victimes.[53] Comme le mentionne la section de ce chapitre sur les « auteurs des cyberdélits », le potentiel des botnets pour récolter ces renseignements a entraîné le développement de « marchés » de cybercriminalité basés sur la vente et la location de botnets.[54] Comme le signale l´évaluation des menaces de la criminalité organisée transnationale de 2010 de l´ONUDC, le marché des informations personnelles obtenues au travers de botnets est largement divisé – avec différents individus qui s´emploient à collecter et identifier des informations financières, les vendre et les encaisser ».[55]

Infractions liées au contenu

Vue d´ensemble – entre un tiers et la moitié des actes les plus courants de cybercriminalité concernent les infractions liées au contenu.[56] Le contenu peut être réglementé par le droit pénal pour de nombreuses raisons, y compris quand il est contraire à la sécurité nationale, l´ordre public, la santé ou la morale, ou les droits et les libertés d´autrui.

Les 4600 demandes présentées par les autorités nationales de retrait de contenu des services Google démontrent que les gouvernements considèrent qu´une grande partie du contenu affecte ces domaines.[57] Cependant, ce n´est pas la totalité du contenu qui relève du droit pénal.

50 Il est probable que les estimations basées sur les adresses IP concordent seulement avec le nombre de dispositifs infectés lorsqu´ils sont signalés à court terme, par exemple, dans un laps d´une heure. Les adresses uniques IP identifiées sur de longues périodes surestiment beaucoup le nombre de dispositifs en raison des IP dynamiques. Dans une étude sur les botnets, 1,25 million d´adresses uniques IP de zombies identifiées sur une période de 10 jours correspondent à seulement 183 000 bots selon l´ID unique des bots (Stone-Gross, B., et al. 2009. votre Botnet est mon Botnet : analyse d´une prise de contrôle d´un Botnet. Dans : *16 ème conférence annuelle de l´ACM sur la sécurité de l´informatique et des communications (CCS)*, 9-13 novembre 2009). De plus, les comptes des machines zombies sont affectés par le laps de « non visibilité » avant qu´un dispositif ou une adresse IP ne soient plus considérés comme un membre du botnet (voir http ://www.shadowserver.org/wiki/pmwiki.php/Stats/BotCounts).

51 Voir, par exemple, http ://www.secureworks.com/cyber-threat-intelligence/threats/waledac_kelihos_botnet_takeover/ ; http ://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/ ; Stone-Gross, B., et al. 2009. Votre Botnet est mon Botnet : analyse d´une prise de contrôle d´un Botnet. CCS '09.

52 Voir, par exemple, http ://www.symantec.com/connect/blogs/botnets-masses

53 Stone-Gross, B., *et al.*, 2009. Votre Botnet est mon Botnet : analyse d´une prise de contrôle d´un Botnet. CCS « 09.

54 Voir, par exemple, Panda Security, 2010. Le marché noir de la cybercriminalité *: découvert.*

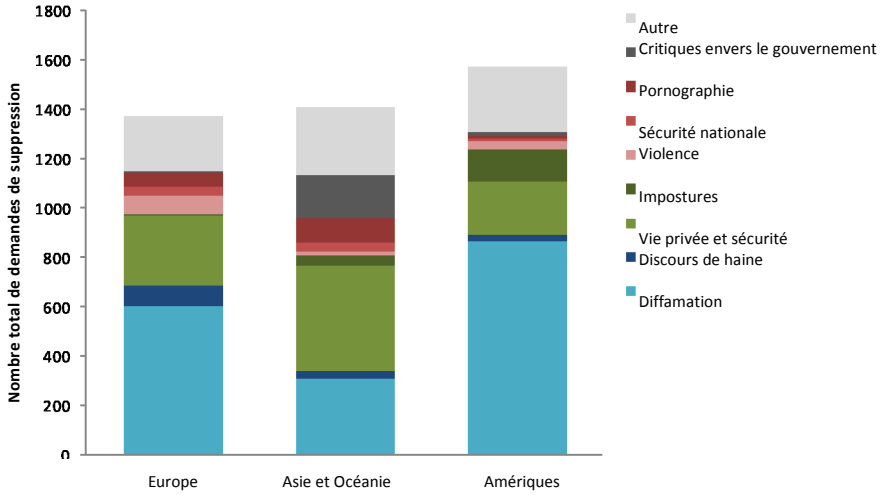
55 ONUDC, 2010. *La globalisation du crime : évaluation des menaces de la criminalité organisée transnationale.*

56 Voir ci-dessus la Section 2.2 la situation globale de la cybercriminalité, répartition des actes de cybercriminalité.

57 Données dewww.google.com/transparencyreport

La figure 2.11 démontre que la suppression d´un contenu d´internet vise les contenus impliquant de la violence ; des atteintes à la vie privée et à la sécurité ; des impostures ; des discours de haine ; de la diffamation ; et des critiques à l´encontre du gouvernement. Le nombre total de demandes de suppression est comparable d´une région à l´autre. Dans toutes les régions, les demandes de suppression concernent généralement le matériel lié à la diffamation, la vie privée et la sécurité. En relation avec ce patron, lors de la collecte des informations pour l´étude, de nombreux pays d´Afrique du nord et d´Asie du sud-est signalèrent des tendances en matière de cybercriminalité montrant *« une utilisation de plus en plus fréquente des réseaux sociaux pour la diffamation et la propagande,* » ainsi que « *de plus en plus d´actes liés à la réputation et à la vie privée* » et « *des messages diffamatoires postés en ligne* ».[58]

Figure 2.11 : demandes de suppression de contenus transmises à Google par les gouvernements 2010-2012



Source : ONUDC élaboration du rapport de transparence de Google.

Comme le mentionne le chapitre quatre de cette étude (incrimination), même si le contenu global en ligne ne peut être jugé en termes de simple moralité, un seuil élevé est requis lorsque les outils du droit pénal sont utilisés pour limiter la liberté d´expression.[59]

Pornographie infantile

Un type de contenu qui pourrait – ou plutôt doit – faire l´objet de mesures pénale, est la pornographie infantile. Lors de la collecte des informations pour l´étude, les actes relatifs à la pornographie infantile représentaient un tiers des cyberdélits les plus fréquents dans les pays d´Europe et d´Amérique. La proportion était plus faible – environ 15 % – dans les pays d´Asie et d´Océanie.[60] Depuis 2009, presque 1000 sites web commerciaux de pornographie infantile ont été identifiés, avec leur propre nom et « marque » distinctifs. Environ 440 d´entre eux étaient actifs en 2011.[61] Chaque site web est une passerelle pour des centaines ou des milliers d´images ou de vidéos d´abus sexuels sur des enfants. Ils sont souvent financés par des mécanismes de paiement, des magasins de contenu, des systèmes d´inscription et des publicités. Les évolutions récentes incluent l´utilisation de sites qui, lors de leur chargement direct, affichent un contenu légal, mais qui permettent l´accès à des images de pornographie infantile lorsqu´ils sont chargés par l´intermédiaire d´une passerelle référente spécifique. En outre, les opérations des services répressifs contre le partage de fichiers P2P de pornographie infantile ont identifié des millions d´adresses IP offrant de la pornographie infantile.[62]

58 Questionnaire de l´étude sur la cybercriminalité Q81 et Q85.
59 Voir le chapitre quatre (incrimination), Section 4.3 Loi internationale sur les droits de l´homme et l´incrimination, Limitations de la liberté d´expression et droit international.
60 Questionnaire de l´étude sur la cybercriminalité Q81.

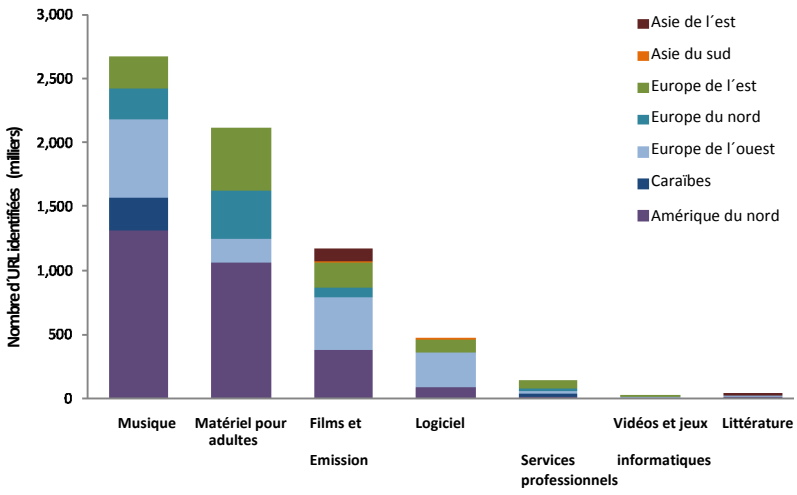
61 Fondation pour la surveillance d´internet, 2011. *Rapport annuel 2011.*
62 Voirhttp ://www.justice.gov/psc/docs/natstrategyreport.pdf

Violation de la propriété intellectuelle – les droits de propriété intellectuelle sont des droits donnés aux personnes sur les œuvres de l´esprit. Ils confèrent généralement au créateur un droit exclusif sur l´utilisation de sa création durant une période déterminée. Presque tout le matériel sur lequel portent ces droits peut vraisemblablement être disponible en ligne – qu´il s´agissent d´œuvres littéraires ou artistiques, d´enregistrements sonores, des signes distinctifs comme les marques, les détails des inventions protégées par des brevets, des dessins industriels ou des secrets commerciaux. Lorsque ces droits sont violés – comme dans le cas d´une utilisation ou d´une reproduction illicite – les moyens d´application reposent généralement sur des procédures civiles entre individus avec, dans certains cas, le droit d´engager des poursuites pénales privées. De plus, dans certaines circonstances l´état peut avoir le droit d´engager des procédures pénales. En général, les accords internationaux tels que l´ADPIC spécifient que les pays devront prévoir des peines et des procédures pénales au moins dans les cas qui sont « *commis délibérément et à une échelle commerciale* ».[63]

Identifier la nature et la portée des violations *criminelles* liées à l´informatique, ou en ligne, des droits de propriété intellectuelle est donc loin d´être simple. Le mieux que l´on puisse faire à l´échelle globale est d´identifier la quantité et le type de matériel qui viole les droits de propriété. Selon le contexte et les circonstances – y compris l´échelle, la tentative, les objectifs, la loi applicable et la juridiction – une certaine proportion d´individus impliqués dans ces violations pourrait faire l´objet de sanctions pénales.

Droits d´auteurs – les droits qui protègent les livres, les écrits, la musique, les films et les programmes informatiques – ont une importance particulière pour le contenu en ligne. À l´échelle globale, les estimations suggèrent que presque *24 %* du trafic total d´internet viole les droits d´auteurs.[64]

Figure 2.12 : demandes de suppression relatives aux droits d´auteurs des 60 principaux titulaires des droits d´auteurs reçues par Google, par type de contenu et emplacement du site web identifié2011-2012



Source : ONUDC élaboration du rapport de transparence de Google

Le niveau de trafic les enfreignant varie en fonction de la localisation et est plus élevé dans des zones de services P2P ou des sites de téléchargement qui hébergent des fichiers, généralement utilisés pour distribuer des films, des épisodes de télévision, de la musique, des jeux informatiques et des logiciels.[65] L´analyse des demandes de suppression de contenus des services Google qui enfreignent les droits d´auteurs, présentées par les titulaires des droits d´auteurs et concernant plus de 6,5 millions d´URL, donne un aperçu de la distribution et du type de matériel ainsi que de la localisation des sites d´hébergement.[66]

Les titulaires des droits d´auteurs demandent prioritairement la suppression de musique, suivie par le contenu destiné aux adultes, les films et les émissions ainsi que les logiciels informatiques qui enfreignent ces droits.

63 ADPIC, Art. 61.

64 Envisional, 2011. *Rapport technique : une estimation de l´utilisation contrefaisante d´iinternet. Janvier 2011.* Cette estimation exclut la pornographie car il peut être difficile d´établir son statut contrefaisant.

65 *Ibid.*

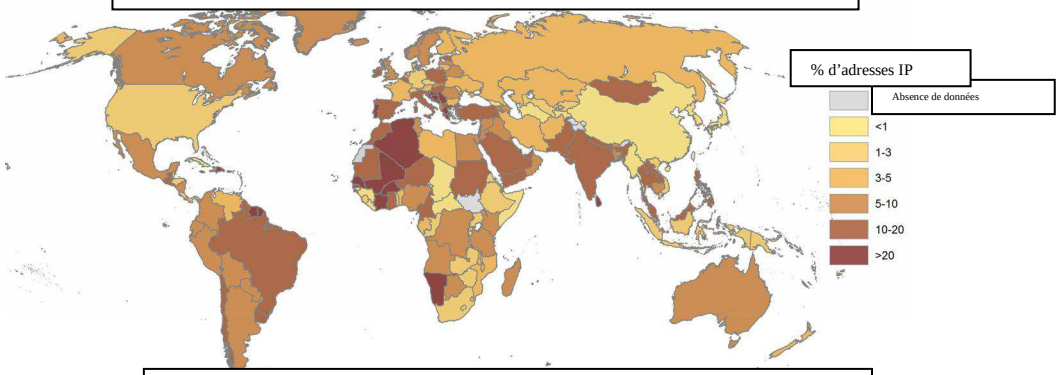
66 L´analyse se limite aux demandes de suppression des 60 plus importants titulaires de droits d´auteurs et au nombre d´URLS pour lesquelles a été requise la suppression. Les résultats des demandes de suppression reçues par Google sont influencés par la nature et la portée du matériel contrefaisant et la propension des titulaires de droits d´auteurs à présenter la demande de suppression et à rechercher activement le retrait de ce matériel .

D´autres types de contenus font l´objet d´un nombre considérablement inférieur de demandes de suppression. La majorité des sites qui hébergent ce matériel se trouvent en Amérique du nord et en Europe, bien qu´il y ait également des sites qui hébergent de la musique enfreignant les droits d´auteurs dans les Caraïbes.

% d'adresses IP

Bien que ces informations ne puissent être utilisées pour établir une violation criminelle de la propriété intellectuelle, il est à noter que certaines demandes de suppression concernent de multiples URL, parfois des dizaines de milliers, identifiées dans un unique domaine.[67] Des mesures pénales ont été prises à l´encontre des personnes responsables des sites web qui hébergent de grandes quantités de contenu contrefait similaire à celui qui est inclus dans les données relatives aux demandes de suppression de Google.[68] Des informations globales détaillées sur les téléchargements de services de partages de fichiers P2P, BitTorrent, montrent la répartition de l´utilisation des services d´internet qui peuvent être utilisés pour partager des contenus contrefaits. Le trafic total de BitTorrent représente 18 % de tout le trafic d´internet. On estime que près des deux tiers de ce trafic concernent un contenu non pornographique protégé par le droit d´auteur comme des films, des épisodes de télévision, de la musique et des logiciels informatiques.[69] La carte montre le pourcentage des adresses IP des pays identifiées uniquement par le biais du téléchargement de musique de l´un des 750 000 artistes référencés par BitTorrent au cours du premier trimestre de 2012.[70] En ce qui concerne ces artistes, durant cette période, 405 millions d´enregistrements de musique furent téléchargés par le biais de BitTorrent – presque 80 % en albums et près de 20 % en singles.[71] Le patron de téléchargement montre qu´en ce qui concerne le nombre d´adresses IP par pays, les téléchargements sont particulièrement élevés dans les pays d´Afrique, d´Amérique du sud et d´Asie du sud. Ces activités peuvent ne pas atteindre les seuils typiques de violations des droits de propriété intellectuelle. Néanmoins, lors de la collecte des informations pour l´étude, certains pays d´Amérique et d´Afrique ont indiqué que les délits liés à l´informatique concernant les droits d´auteurs et les marques déposées étaient communs en matière de cybercriminalité. Un pays d´Afrique australe a, par exemple, signalé que « *un des actes les plus fréquents de cybercriminalité et qui représente une menace significative est la production illicite d´œuvres artistiques qui entraîne une augmentation des marchandises contrefaites sur le marché* ».[72] Cependant, les réponses du questionnaire de l´étude montrent en général que les organisations du secteur privé tendent à considérer les cyberdélits relatifs aux droits d´auteurs comme une menace plus importante que ne le considèrent les pays.[73] Toutefois, les cyberdélits relatifs aux droits d´auteurs et aux marques déposées jouent un rôle beaucoup moins important pour le secteur privé que toute une gamme de potentiels cyberdélits comme la violation de la vie privée ou des mesures de protection des données, des données illégales ou une interférence avec le système.[74]

Figure 2.13 : téléchargement unique de musique de Bit Torrent, par pays (1H 2012)



Source : ONUDC élaboration des données de MusicMetric. Indice de musique numérique.

67 Voirhttp ://www.google.com/transparencyreport/removals/copyright/
68 Voir http ://www.justice.gov/opa/pr/2012/January/12-crm-074.html
69 Envisional, 2011. *Rapport technique : une estimation de l´utilisation contrefaisante d´internet. Janvier 2011.*
70 ONUDC élaboration des données de MusicMetric. Indice de musique numérique. Voir www.musicmetric.com/dmi
71 *Ibid.*
72 Questionnaire de l´étude sur la cybercriminalité Q81.
73 Voir la Section 2.2 La situation globale de la cybercriminalité, répartition des actes de cybercriminalité
74 *Ibid.*

2.3 Auteurs de cyberdélits

Principaux résultats :

- les habilités ou les techniques complexes ne sont plus nécessaires pour les auteurs des cyberdélits en raison de l´émergence et de la grande disponibilité des logiciels malveillants ;
- on estime que plus de 80 % des actes de cybercriminalité proviennent d´activités organisées, et il existe des marchés noirs de cybercriminalité établis dans des cycles de création des logiciels malveillants, des infections informatiques, des gestions de botnets, la récupération des données financières ou personnelles, la vente de données et leur encaissement ;
- la cybercriminalité exige souvent un haut niveau d´organisation pour sa mise en œuvre, et peut émerger dans de petits groupes criminels, des réseaux informels *ad hoc*, ou la criminalité organisée à grande échelle. La typologie des délinquants et des groupes criminels actifs reflète généralement les patrons du monde « classique » ;
- notamment dans le contexte des pays en développement, ont émergé des sous-cultures de jeunes qui commettent des fraudes financières liées à l´informatique, et l´implication de certains d´entre eux dans la cybercriminalité débute vers la fin de leur adolescence ;
- au niveau démographique, le patron des délinquants reflète la criminalité classique avec une majorité de jeunes hommes, bien que le profil d'âge s´élève avec des individus plus âgés (de sexe masculin), en particulier pour ce qui concerne les délits de pornographie infantile ;
- bien que certains délinquants aient effectué des études supérieures, notamment dans le domaine de l´informatique, beaucoup de délinquants identifiés n´ont pas de formation spécialisée ;
- il manque une recherche systématique sur la nature des organisations criminelles actives dans le cyberespace ; et il est nécessaire d´effectuer des recherches supplémentaires relatives aux liens entre les délinquants en ligne en matière de pornographie infantile et

Comme l´établit la section « Mesurer la cybercriminalité » de ce chapitre, qualifier un délit requiert généralement des informations relatives à « *qui* » et (*combien de personnes*) est impliqué dans « *quoi* » (et *dans quelle mesure*).[75] Cette section examine l´élément « *qui* » concernant les auteurs de délits, en mettant l´accent sur les délinquants typiques et les niveaux de l´organisation criminelle, notamment dans le cas de délits de fraude informatique, et de production, distribution ou possession de pornographie infantile.

La description complète d´un « auteur de cyberdélits » peut contenir plusieurs éléments. L'âge, le sexe, les antécédents socio-économiques, la nationalité et la motivation se trouvent parmi les principales caractéristiques.[76] De plus, le niveau de l´organisation criminelle – ou la mesure dans laquelle ces individus agissent en concert avec d´autres – représente une caractéristique distinctive de l´élément de l´association humaine derrière le comportement criminel.[77] La compréhension de la cybercriminalité comme un phénomène « socio-technologique », basée sur les caractéristiques des personnes qui commettent ces délits, représente une approche plus ample en matière de prévention que le fait de se baser uniquement sur des concepts techniques de cybersécurité.[78]

75 Institut européen pour la prévention et le contrôle du crime, affilié aux Nations Unies (HEUNI), 2011. Collecte de données sur les [Nouvelles] Formes et manifestations de la criminalité. *dans* : Joutsen, M. (ed.) *Nouveaux types de criminalité, Procédures du séminaire international tenu à l´occasion du trentième anniversaire de l´HEUNI*, 20 Ooctobre 2011, Helsinki : EICPC. Voir aussi UNODC, 2010. *La globalisation du crime : évaluation des menaces de la criminalité organisée transnationale.*

76 Département des affaires économiques et sociales des Nations Unies, Division de statistique, 2003. *Manuel pour l´élaboration d´un système de statistiques de la justice pénale* ST/ESA/STATSER.F/89.

77 Levi, M., 1998. Perspectives sur la « Criminalité organisée » : un aperçu. *Journal Howard*, 37(4) :335-345.

78 Yip, M., Shadbolt, N., Tiropanis, T. et Webber, C., 2012. *L´économie numérique souterraine : un réseau social. Approche pour comprendre la cybercriminalité.* Document présenté à la conférence *Futur numérique*, 23-25 octobre 2012, Aberdeen.

Bien que les caractéristiques individuelles soient comparativement simples à définir, il est bien connu que l´analyse de la criminalité organisée présente fréquemment des difficultés pour la mesurer et la définir. Cette étude adopte la définition élargie sur un groupe criminel organisé établie par la Convention des Nations Unies contre la criminalité organisée.[79] Dans cette définition, il existe plusieurs approches de la typologie,[80]ainsi que pour classifier un délit pénal spécifique comme un « crime organisé ».[81] Il n´y a aucune raison de penser que le développement de ces approches et ces typologies ne pourrait pas s´appliquer à l´implication des groupes criminels organisés dans la cybercriminalité – en faisant face à de nouveaux défis et au cas par cas.[82] En effet, l´une des principales propositions de l´évaluation de la menace représentée par la criminalité organisée facilitée par l´internet (iOCTA) d´EUROPOL est que « *la structure des groupes de cybercriminalité montre la plus claire rupture qu´il y ait jusqu´à présent avec le concept traditionnel de groupes de la criminalité organisée hiérarchisés* »[83] Cette section conclut que cela peut être vrai dans de nombreux cas, mais qu´il est nécessaire de considérer une vaste gamme de typologies, en tenant compte de la dynamique en ligne/hors ligne des activités criminelles.

Profils des « délinquants typiques »

Les informations sur les profils des délinquants proviennent généralementdes études rétroactives de cohorte de cas de poursuite des cyberdélits. Des opérations d´infiltration des services répressifs sur des forums clandestins en ligne, ainsi que des travaux d´observation des auteurs de cyberdélits menés par des chercheurs universitaires sur des forums de discussion représentent aussi des sources précieuses d´informations. D´autres approches incluent l´utilisation de questionnaires anonymes d´autoévaluation, des observations des évènements clandestins de sécurité informatique, et le déploiement de « pots de miel » interconnectés[84]

Suspects de cyberdélit identifiés par la police (un pays d´Asie du sud)

Dans un pays d´Asie du sud, les statistiques publiées par la police nationale contenaient des informations sur les délits de cybercriminalité enregistrés et les suspects. Les suspects étaient classifiés dans plusieurs catégories dans les statistiques enregistrées, en fonction des relations avec la victime et d´autres caractéristiques. Alors qu´une proportion élevée de suspects n´est pas classifiée, les statistiques de la police nationale montraient que :

- plus de 10 % des suspects de cyberdélits enregistrés sont connus des victimes et sont des voisins, des amis ou des membres de la famille ;
- « les employés mécontents » et les « pirates » représentent chacun près de 5 % des auteurs des cyberdélits enregistrés ;
- un nombre significatif de suspects de cyberdélits sont inscrits dans l´enseignement supérieur et d´autres programmes d´apprentissage.

Source : http ://ncrb.gov.in/

79 Conformément à l´Article 2 de la Convention sur la criminalité organisée ; « *un » groupe criminel organisé » désigne un groupe structuré de trois personnes, ou plus, existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves conformément à la présente Convention pour en tirer, directement ou indirectement, un avantage financier ou un autre avantage matériel ».* L´Article 2(c) précise que « *un « groupe structuré » désigne un groupe qui ne s´est pas constitué par hasard pour commettre immédiatement une infraction et qui n´a pas de rôles formellement définis pour ses membres, de continuité dans sa composition ou sa structure ».*

80 Une des typologies de l´UNODC des groupes criminels organisés inclut : (i) « hiérarchie standard » (un seul groupe hiérarchique avec de solides systèmes de discipline interne) ; (ii) « hiérarchie régionale » (des groupes dotés d´une structure hiérarchique, avec de solides systèmes de discipline et de contrôle interne mas une relative autonomie au plan régional) ; (iii) « hiérarchie groupée » (un une série de groupes criminels qui ont établi un système de coordination/contrôle allant de faible à important, sur toutes leurs activités) ; (iv) « groupe central » (un groupe solidement organisé mais non structuré, entouré dans certains cas d´un réseau d´individus impliqués dans des activités criminelles) ; et (v) « réseau criminel » (un réseau lâche et fluide, réunissant souvent des individus aux compétences particulières, qui sont eux-mêmes impliqués dans une série de projets criminels). UNODC, 2002. *Résultats d´une enquête pilote sur quarante groupes criminels organisés sélectionnés dans seize pays. Septembre 2002.*

81 Europol, par exemple, a spécifié qu´au moins six des caractéristiques suivantes doivent exister pour qu´un délit ou un groupe criminel soit classifié dans la "criminalité organisée", quatre desquels doivent être ceux qui sont mentionnés aux numéros (1), (3), (5) et (11) : (1) collaboration de plus de deux personnes ; (2) chacun doit avoir une tâche attribuée ; (3) pour une période prolongée ou indéfinie ; (4) utiliser une forme de discipline et de contrôle ; (5) être soupçonné du fait de commettre des délits pénaux graves ; (6) opérer au niveau international ; (7) utiliser la violence ou d´autres moyens d´intimidation ; (8) utiliser des structures de type commercial ; (9) implication dans le blanchiment de capitaux ; (10) exercer une influence sur les politiques, les médias, l´administration publique, les autorités judiciaire ou l´économie et (11) motivé par la recherche de profit et/ou de pouvoir. Europol Doc. 6204/2/97. ENFOPOL 35 Rev 2.

82 Même si, par exemple, les détenteurs individuels ou institutionnels d´ordinateurs compromis dans un botnet peuvent participer involontairement à une entreprise criminelle, certains commentateurs soutiennent que les botnets devraient être considérés comme une forme de criminalité organisée. (Chang, L. Y. C., 2012. *Cybercriminalité dans la région de la grande Chine.* Cheltenham : Edward Elgar).

83 Europol, 2011. *Evaluation de la menace représentée par la criminalité organisée facilitée par l´internet.* iOCTA. Dossier n°. 2530-264.

84 Voir, par exemple, Chiesa, R., Ducci, S. et Ciappi, S., 2009. *Profilage des pirates informatiques. La science du profilage criminel appliqué au monde du piratage informatique.* Boca Raton, FL : Taylor & Francis Group.

Il est compliqué de comparer les études à cause des différences de méthodologie ; y compris en ce qui concerne les actes de cybercriminalité, la sélection des échantillons, la couverture géographique ; et des approches concernant l´analyse et la présentation des caractéristiques des auteurs de cyberdélits – comme l´utilisation de différentes tranches d´âges des auteurs des cyberdélits. Cette section présente des données sur des études qui établissent les profils des auteurs d´une grande variété de délits, et des données relatives à des actes spécifiques – comme l´accès illégal à des systèmes ou des données informatiques, la production, la distribution ou la possession de pornographie infantile liée à l´informatique.

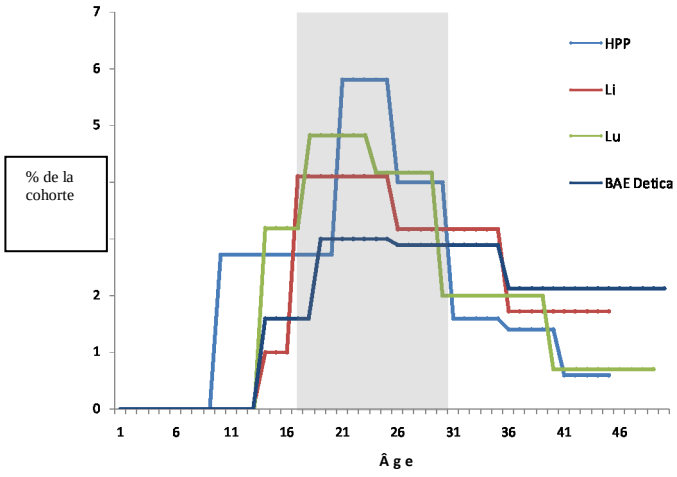
Utilisation d´une affaire licite comme façade pour la cybercriminalité

Les deux principaux organisateurs d´un groupe d´environ 30 personnes basé en Europe de l´est fournissaient des services légaux d'hébergement et de serveurs informatiques. Par le biais de cette activité licite, ils dissimulaient des centaines de « smswarez » (commerce illégal de contenus protégés par des droits d´auteurs en échange d´un paiement par SMS), de « smswebs » (pages web où des contenus protégés par des droits d´auteurs peuvent être téléchargés en échange d´un paiement par SMS) et des « torrents»... Les organisateurs utilisaient le spam pour annoncer ces services illicites, et cela entraîna la saisie de 48 serveurs illégaux avec une capacité de 200-250 téraoctets. Après que ce groupe ait été arrêté, le roulement de données nationales sur internet fut réduit d´environ 10 pour cent.

ONUDC : recueil de cas de la criminalité organisée

L´analyse ci-dessous provient de trois études clés[85] qui couvrent tout un panel d´actes de cybercriminalité, ainsi que d´un questionnaire d´autoévaluation centré sur les pirates informatiques.[86] La cohorte « Li » correspond à 151 auteurs de cyberdélits « typiques » poursuivis par un pays d´Amérique du nord entre 1998 et 2006.[87] La cohorte « Lu » correspond à près de 18 000 suspects de cyberdélits enregistrés sur la base de données de la police d´un territoire d´Asie de l´est entre 1999 et 2004.[88] L´étude « BAE Detica » examinait deux échantillons de 250 activités numériques distinctes de groupes de la criminalité organisée à partir de l´étude de publications à l´échelle mondiale. Par contre, l´étude sur le piratage « HPP » repose sur les données d´environ 1400 questionnaires d´autoévaluation renseignés par des pirates informatique – qui peuvent ou non avoir été impliqués dans un délit.[89]

Figure 2.14 : tranches d´âge des auteurs de cyberdélits



Source : ONUDC élaboration de HPP, Li, Lu et BAE Detica

Âge – la Figure 2.14 montre les tranches d´âges des auteurs des délits, tirées des quatre études.[90] Toutes les études suggèrent que les auteurs de cyberdélits sont généralement âgés de 18 à 30 ans. Selon l´étude Li, par exemple, 37 % des auteurs ont entre 17 et 25 ans. Selon l´étude Lu, 53 % des auteurs ont entre 18 et 29 ans.

85 Li, X., 2008. Le phénomène criminel sur iinternet : révision des principales caractéristiques des criminels et des victimes à travers des cas classiques faisant l´objet de poursuites. *Revue de droit et technologie de l´Université d´Ottawa,* 5(1-2) :125-140, (« Li ») ; Lu, C.C., Jen, W.Y., Chang, W. et Chou, S., 2006. Cybercriminalité& Cyber-délinquants. *Journal d´informatique*, 1(6) :1-10, (« Lu ») ; et BAE Systems Detica et Université métropolitaine de Londres, 2012. *Criminalité organisée à l´ère numérique* (« BAE Detica »).

86 UNICRI et Chiesa, R., 2009. *Profilage des pirates informatiques*. Disponible à : http ://www.unicri.it/emerging_crimes/cybercrime/cyber_crimes/docs/profiling-hackers_add-info.pdf (« HPP »).

87 La cohorte Li inclut le piratage/l´accès illégal, les attaques, le sabotage, les virus, le vol/espionnage de données, le vol d´identité lié à l´informatique, la fraude, le détournement et la corruption.

88 La cohorte Lu inclut les fraudes sur internet, le piratage informatique, l´abus informatique, le blanchiment de capitaux lié à l´informatique, la pornographie, le commerce du sexe, les paris, et le vol.

89 Les commentateurs signalent que les conceptions de la culture populaire relatives aux pirates informatiques, qui ne sont ni bien définies ni bien établies, ont été utilisées pour remplir les lacunes des informations relatives aux auteurs de cyberdélits. Voir Wall, D. 2012. La construction sociale des pirates informatiques comme des cyber-délinquants. *dans :* Gregoriou, C. (ed), *Construction de la criminalité : Discours et représentations culturelles de la criminalité et de la « déviance ».* Houndsmills, UK : Palgrave Macmillan, p.4-18.

90 Étant donné que les études signalent les âges des auteurs des délits en utilisant des tranches d´âges différentes, les résultats sont indiqués en utilisant une répartition égale entre les tranches d´âges signalées. Les données sous-jacentes de chaque étude montrent probablement des variations pour chaque tranche d´âges

La plus récente étude de BAE Detica diffère quelque peu car elle indique de possibles niveaux élevés d´infractions persistantes commises par des personnes d´une trentaine ou d´une quarantaine d´années – 32 % des auteurs de délits ont entre 36 et 50 ans. Contrairement aux études qui incluent un panel d´actes de cybercriminalité, l´étude HPP sur le piratage montre une diminution prononcée dans les tranches d´âges des auteurs de cyberdélits les plus âgés – seulement 21 % du total des auteurs de cyberdélits a plus de 30 ans. Ceci concorde avec l´identification de sous profils de pirates informatiques qui commencent leurs activités à un jeune âge – comme les « script kiddies (pirates débutants) ». Selon l´étude HPP, par exemple, 61 % des pirates signalent avoir commencé leurs activités entre l'âge de 10 et 15 ans. Les auteurs de cyberdélits peuvent donc être dans l´ensemble plus jeunes que les auteurs d´infractions criminelles en général. Sur le territoire d´Asie de l´est examiné par Lu, la tranche d'âge la plus représentée pour le total des auteurs de délits, se situe entre 30 et 39 ans, alors qu´elle se situe entre 18 et 23 ans pour les auteurs de cyberdélits.

Genre – les auteurs de cyberdélits sont majoritairement de sexe masculin – les études HPP, Li et Lu signalent 94, 98 and 81 % d´auteurs de sexe masculin, respectivement. Des résultats de plus de 90 % correspondent à une proportion masculine plus élevée en matière de cybercriminalité que pour la criminalité en général. Globalement, la proportion des hommes poursuivis pour un délit se situe typiquement entre 85 et 90 %, avec une médiane de 89 %.[91] Ce patron concorde avec les données fournies par les pays lors de la collecte des informations pour l´étude. Un pays d´Europe du nord a, par exemple, commenté que « *les auteurs sont des hommes jeunes ».*[92]

Quelques études qui ont été réalisées dans des pays en développement fournissent une vision claire qui couvre tous les âges. Néanmoins, les sous profils d´auteurs de cyberdélits comme les « yahooboys »[93] confirment l´implication dans des activités de cybercriminalité d´hommes jeunes. Une de ces études révèle que 50 % des auteurs de cyberdélits dans un pays d´Afrique de l´ouest sont âgés de 22 à 25 ans – et dont la moitié mentionne avoir commencé à commettre des cyberdélits depuis cinq à sept ans.[94]

Compétences techniques – pour ce qui concerne le niveau de connaissances et de compétences techniques des auteurs de cyberdélits, la majorité des cas analysés par Li n´implique pas des techniques ou des compétences complexes hors de la portée des utilisateurs communs d´ordinateurs. En général, 65 % de tous les actes sont relativement simples à accomplir, 13 % requièrent un niveau moyen de compétences et 22 % sont compliqués.

Profil des étudiants « yahooboys » dans un pays d´Afrique de l´ouest

Âge

<22 ans	5 pour cent
22-25 ans	50 pour cent
26-29 ans	40 pour cent
>29 ans	5 pour cent

Sexe

Masculin	95 pour cent
Féminin	5 pour cent

Nombre d´années impliqué en cybercriminalité

<2 ans	2,5 pour cent
2-4 ans	35 pour cent
5-7 ans	55 pour cent
>7 ans	7,5 pour cent

Niveau d´éducation des parents

Aucune	2,5 pour cent
Primaire	5 pour cent
Secondaire	12,5 pour cent
Supérieur	80 pour cent

Aransiola, J.O. et Asindemade, S.O. 2011. Comprendre les auteurs des cyberdélits et les stratégies qu´ils emploient. *Cyber psychologie, comportement et réseautage social* 14(12), 759-763.

91 HEUNI et UNODC, 2010. *Statistiques internationales sur lacriminalité et la justice.* Helsinki : HEUNI.

92 Suestionnaire de l´étude sur la cybercriminalité. Q85.

93 La sous-culture des « *yahooboys* » comprend des jeunes, en particulier ceux qui vivent dans des villes, qui utilisent l´internet pour commettre des actes d´escroquerie, d´hameçonnage et de fraude liés à l´informatique. Adeniran, A.I., 2011. Café Culture et hérésie du Yahooboyism. *dans :* Jaishankar, K., (ed.) *Cybercriminologie : explorer les délits commis sur iinternet et la conduite criminelle.*Boca Raton, FL : CRC Press, Taylor & Francis Group.

94 Aransiola, J.O., et Asindemade, S.O., 2011. Comprendre les auteurs des cyberdélits et les stratégies qu´ils emploient. *Cyber psychologie, comportement et réseautage social*, 14(12) :759

Les attaques les plus complexes sont celles qui impliquent des virus, des vers et des logiciels espions – dont 73 % sont considérés compliqués. Comme les organisations de cyber sécurité le soulignent généralement, il est probable que la possibilité d´acquérir des outils informatiques permettant d´exploiter les vulnérabilités informatiques et de pirater un grand nombre d´ordinateurs signifie que les auteurs de cyberdélits n´ont plus besoin de posséder de hauts niveaux de compétences techniques.[95] Les niveaux de compétences sont donc hautement variables[96] et – comme mentionné précédemment – ceci peut jouer un rôle dans la structure des groupes de cybercriminalité. Toutefois, les niveaux d´éducation sont généralement plus élevés parmi les auteurs de cyberdélits que dans le cas de la criminalité classique. D´après l´étude Lu, 28 % des suspects de cyberdélits dans le territoire ont suivi un enseignement supérieur contre huit % dans le cas de tous les autres délits. De même, suivant l´étude HPP, plus de la moitié des pirates informatiques ont suivi un enseignement supérieur. Cependant, comme le mentionne l´étude BAE Detica, il est probable que l´acquisition « artificielle » de compétences techniques (par le biais de logiciels malveillants comme ZeuS ou Butterfly Bot) a entraîné un changement, allant du profil traditionnel du cyber délinquant doté de grandes compétences, vers un groupe beaucoup plus vaste d´individus.

Auteurs du délit de pornographie infantile

Le profil des personnes impliquées dans la production, la distribution ou la possession de pornographie infantile liée à l´informatique peut être différent de celui des auteurs de cyberdélits en général. Des informations récentes sur ce groupe de délinquants ont été recueillies par le « groupe de travail virtuel international » (VGT)[97] sous la forme d´un petit échantillon non aléatoire de 103 personnes arrêtées pour avoir téléchargé et échangé de la pornographie infantile au travers des services P2P en ligne.[98]

Âge et statut social – tous les suspects de la cohorte de VGT étaient des hommes âgés de 15 à 73 ans, avec une moyenne d'âge de 41 ans. Un suspect sur cinq ne travaillait pas et était à la retraite, au chômage ou recevait des prestations sociales ou d´assurance maladie. Les autres travaillaient ou étudiaient. 42 % vivaient avec un(e) compagne(on) ou un enfant et/ou un enfant. Ces délinquants étaient significativement plus âgés (âge moyen de 50 ans) que les délinquants célibataires (âge moyen de 35 ans). Tous les suspects se souciaient de dissimuler leurs activités aux autres, mais 60 % y réussissaient en séparant totalement cela de leur vie quotidienne. Pour le reste du groupe, leurs activités délictueuses tendaient à devenir obsessives, étaient plus ou moins imbriquées dans leur vie quotidienne et probablement mal dissimulées. Ce dernier groupe tendait à avoir un faible statut socio-économique, à être versé en informatique et près de 4 % des délinquants signalèrent un problème de santé mentale.

Patrons de délits – les suspects tendent à avoir été impliqués dans des délits de pornographie infantile durant une période relativement longue – une moyenne de cinq ans, allant de six mois à trente ans. Plus de 60 % des suspects collectionnait, non seulement, de la pornographie infantile mais aussi la vendait/distribuait par le biais d´un réseau P2P, et 35 % était impliqué dans des réseaux que le P2P. La moitié de ceux-ci avait participé à des réseaux hors ligne – et cela suggère que les individus qui accèdent à la pornographie infantile pour en faire commerce, le font non seulement en ligne mais également hors ligne.

---

95 Voir, par exemple, Symantec, 2011. *Rapport sur les kits d´attaque et les sites web malveillants* ; Fortinet, 2013. *Fortinet 2013 rapport sur la cybercriminalité– les Cybercriminels d´aujourd´hui reflètent les processus commerciaux légitimes* ; et Trend Micro, 2012. L´évolution du logiciel criminel.

96 Selon l´étude HPP, par exemple, les compétences techniques des pirates étaient réparties comme suit : basses (21 %) ; moyennes (32 %) ; hautes (22 %) ; expert (24 %).

97 Le groupe de travail virtuel international pour lutter contre les abus sexuels d´enfants en ligne est un partenariat international de neuf organismes d´application de la loi établi en 2003. Voirwww.virtualglobaltaskforce.com

98 En raison de la petite taille de l´échantillon et de son processus de sélection non aléatoire, les résultats ne peuvent s´appliquer á toute la population des délinquants en ligne. Néanmoins, on peut en tirer des connaissances sur leurs caractéristiques et leur comportement. Voir Bouhours, B. et Broadhurst, R., 2011. *Rapport statistique : échantillon des délinquants P2P en ligne du groupe de travail virtuel international -Juillet 2010 –Juin2011*. Canberra : Université nationale australienne. Disponible sur : SSRN : http ://ssrn.com/abstract=2174815 or http ://dx.doi.org/10.2139/ssrn.2174815

99 Babchishin, K., Hanson, R. et Herrmann, C., 2011. Les caractéristiques des délinquants sexuels en ligne : une méta-analyse. *Abus sexuel : un journal sur la recherche et le traitement*, 23(1) :92-123.

100 non seulement oir, par exemple, Broadhurst, R. et Jayawardena, K., 2007. Pédophilie et réseaux sociaux en ligne : une recherche expérimentale

« arnaque ». *dans :* Jaishankar, K., ed. *Cybercriminologie : explorer les délits commis sur ünternet et la conduite criminelle.* Boca Raton, FL : CRC Press, 79-102 ;

Liens avec les délinquants hors ligne – il est probable que les délinquants en ligne soient caucasiens, au chômage et légèrement plus jeunes que les délinquants hors ligne.[99] Il peut cependant exister des liens.[100] Une méta-étude récente signalait que dans un échantillon de plus de 500 délinquants en matière de pédopornographie en ligne, un sur six était également impliqué dans des abus sexuels infantiles hors ligne.[101] Dans l´étude VGT, six % avait déjà été accusé d´infractions sexuelles commises en ligne contre les enfants, 18 % avait déjà été accusé d´une infraction avec contact contre des mineurs de moins de 16 ans et 15 % avait déjà été accusé d´une infraction non sexuelle. Il y avait un léger chevauchement entre les infractions antérieures sexuelles et non sexuelles qui suggérait que les suspects avaient eu tendance à se spécialiser en infractions sexuelles contre les enfants. Les suspects les plus fortement impliqués dans des activités de pornographie infantile en ligne étaient également ceux qui avaient été impliqués ou étaient actuellement impliqués dans des abus sexuels infantiles.[102]

Globalement, les délinquants de l´échantillon de VGT avaient un taux relativement élevé d´abus sexuels infantiles, antérieurs et actuels, hors ligne. Pour plus de la moitié des suspects accusés d´avoir déjà commis des abus sexuels infantiles, il y avait également des preuves d´une implication actuelle dans des abus sexuels infantiles. Toutefois, en raison du faible volume de l´échantillon VGT et d´un potentiel parti pris quant à la sélection, il était impossible de savoir si les hommes qui étaient impliqués dans des infractions de pornographie infantile en ligne risquaient davantage d´être également impliqués dans des délits sexuels contre des enfants dans la « vie réelle"». Ceci représente une orientation importante pour de futures recherches.

Rôle des groupes de la criminalité organisée

Divers actes de cybercriminalité requièrent un haut niveau d´organisation et de spécialisation et il est vraisemblable que le niveau d´implication dans la cybercriminalité des groupes conventionnels de criminalité organisée soit élevé – au moins pour ce qui concerne les actes de cybercriminalité motivés par un gain financier tels que les délits concernant l´identité, de fraude et de falsification informatiques.

Jeux d´argent en ligne par une famille de la mafia traditionnelle

En 2008, 26 individus – y compris des membres d´une famille réputée de la mafia – furent inculpés pour avoir opéré une entreprise sophistiquée de jeu d´argent illégaux, qui incluait quatre sites web de jeux d´argent dans un pays d´Amérique centrale. Le procureur de district commenta que « la répression que les services répressifs exerçaient depuis des années contre la mafia traditionnelle avec des salles d´écoute avait entraîné les cercles de jeux illégaux à utiliser de plus en plus des sites web de jeux délocalisés accessibles 24 heures sur 24»... Alors que les jeux d´argent étaient illégaux dans la juridiction de poursuite, les sites web bénéficiaient d´une différente législation dans d´autres juridictions. Les paris étaient placés dans le pays mais étaient gérés à l´étranger, et les données « rebondissaient » dans une série de nœuds de serveurs pour éviter les méthodes de détection traditionnelles des services répressifs.

Veuillez voirhttp://www.fbi.gov/newyork/press-releases/2012/four-gambino-

Elliot, A., Beech, A.R., Mandeville-Norden, R. et Hayes, E., 2009. Profils psychologiques des délinquants sexuels sur iinternet : Comparaisons avec les auteurs d´infractions de contact sexuel. *Abus sexuelun journal de recherches et de traitement* 21(1) :76-92 ; Endrass, J., Urbaniok, F., Hammermeister, L.C., Benz, C., Elbert, T., Laubacher, A. et Rossegger, A., 2009. La consommation de pornographie infantile sur iinternet et les délits sexuels violents. *BMC Psychiatry*, 9 :43-49 ; Webb, L., Craissati, J., Keen, S., 2007. Caractéristiques des auteurs d´infractions de pornographie infantile sur iinternet : une comparaison avec les agresseurs sexuels d´enfants. *Abus sexuel un journal de recherches et de traitement*, 19 :449- 465.

101 Wolak, J., Finkelhor, D., Mitchell, K., 2011. Les possesseurs de pornographie infantile : tendances et caractéristiques des. *Abus sexuel un journal de recherches et de traitement* 23(1) :22-42. Une autre étude sur les auteurs d´infractions de pornographie infantile, l´étude « Butner », comparait des groupes d´auteurs d´infractions qui participaient à un traitement volontaire, en se basant sur la l´éventuelle existence d´antécédents documentés d´infractions sexuelles avec contact commises contre au moins un enfant. Les résultats de l´étude *« mirent en évidence qu´il existe une interaction complexe entre le fait de voir de la pornographie infantile et les infractions sexuelles avec contact ».* Il s´avérait que les délinquants en ligne *« étaient beaucoup plus susceptibles de ne pas avoir commis d´infraction sexuelle avec contact contre un enfant, »* et que *« plusieurs d´entre eux pouvaient être des agresseurs d´enfants non détectés, et leur usage de pornographie infantile indiquait leur orientation paraphilique ».* Sans leurs activités criminelles en ligne, *« ces délinquants n´auraient pas attiré l´attention des services répressifs ».* Voir : Bourke, M.L., Hernandez, A.E., 2008. L´étude « Butner » Redux : un rapport sur l´incidence sur la victimisation des infractions sexuelles de contact commises contre les enfants par auteurs d´infractions de pornographie infantile. *Journal sur la violence familiale,* 24 :183-191.

102 Bouhours, B., Broadhurst, R., 2011. *Rapport statistique : échantillon des délinquants P2P en ligne du groupe de travail virtuel international -jJuillet 2010 –juin2011.* Canberra : Université nationale australienne.

Il faut toutefois rappeler que les estimations de la « *proportion des cas de cybercriminalité liés à la criminalité organisée* » sont notamment influencées par les définitions de la « cybercriminalité » et la « criminalité organisée » appliquées, et – en particulier – par la répartition des différents actes de cybercriminalité dans les cohortes examinées. Les actes qui impliquent, par exemple, la pornographie infantile, peuvent avoir une faible participation dans la « criminalité organisée » si on considère que les individus qui effectuent un téléchargement n´agissent pas dans un « groupe structuré » pour « commettre un délit ». De plus, l´application des modèles actuels de criminalité organisée aux activités « en ligne » comporte sa part de difficultés. Il est difficile d´appliquer les caractéristiques traditionnelles de la criminalité organisée, telles que l´utilisation de la violence et le contrôle du territoire, aux activités de cybercriminalité. En outre, il peut être difficile de régler les questions de « gouvernance » traditionnelle des groupes de la criminalité organisée, y compris la confiance et la mise en application, dans un environnement de salles de discussion ou de forums en ligne. Néanmoins, les organisations peuvent faire – et souvent mieux - ce que les individus peuvent faire. L´internet et les technologies associées se prêtent bien à une coordination accrue entre des individus dispersés dans une zone – et rendent possibles des associations criminelles de courte durée en « essaims », et la divergence avec des modèles traditionnels comme les groupes basés sur une hiérarchie standard et régionale.[103] Comme cela a été mentionné précédemment, dans une période de temps relativement courte, la cybercriminalité a cessé d´être un délit peu fréquent commis par un délinquant spécialisé pour devenir un délit massif, « *organisé et industrialisé* ».[104]

Une étude récente qui a examiné un échantillon de 500 délits enregistrés de cybercriminalité, estimait que plus de 80 % des cyber délits peuvent actuellement impliquer des activités organisées.[105] Une estimation supérieure relative à l´implication de la criminalité organisée dans la cybercriminalité pourrait être de 90 %.[106] LeiOCTA d´EUROPOL déclare que si ce n´est déjà le cas, dans un futur proche, la « *grande majorité* » des enquêtes sur la criminalité organisée transnationale nécessitera une certaine forme d´enquête sur internet. Bien qu´étant délibérément partial en matière de criminalité organisée, le recueil des affaires de criminalité organisée de l´ONUDC conclut que la présence d´un groupe criminel organisé qui était un facteur constant dans tous les cas de cybercriminalité examinés « *réduit considérablement le rôle des pirates isolés en tant qu´intervenants principaux de la cybercriminalité* ».[107] Le recueil signale également que la nature des délits de cybercriminalité « *requiert nécessairement l´organisation de nombreux moyens et de ressources humaines* ».

De nombreux pays répondants ont également mentionné une implication croissante des groupes de criminalité organisée dans la cybercriminalité durant les cinq dernières années. Par exemple, un pays d´Afrique de l´ouest signalait le « *développement de groupes de cybercriminalité qui sont de plus en plus organisés et possèdent une dimension transnationale* ». Un pays d´Amérique du sud déclarait « *la cybercriminalité a cessé d´être un délit commis par un individu isolé et est devenu un délit commis par des organisations criminelles,* » et un pays de l´Asie du sud-est concluait « *la cybercriminalité est devenue syndiquée avec des individus chargés de différents rôles spécialisés* »[108]

Les groupes de criminalité organisée peuvent donc au moins être considérés comme des *intervenants importants de la cybercriminalité*. Néanmoins, les preuves empiriques limitées exigent une certaine prudence – en ce qui concerne les conclusions relatives à la proportion de la criminalité organisée et, à sa forme et sa structure. La technologie informatique a donné un pouvoir sans précédent aux individus. Une étude sur des étudiants suspects de cyber délits suggérait, par exemple, que 77 % agissaient seuls plutôt qu´en groupe.[109] Un pays répondant d´Asie de l´ouest signalait également que la plupart des actes de cybercriminalité avait « *un caractère individuel et étaient réalisés par des individus à des fins personnelles et non par des organisations ou des groupes* ».

Comme cela a été mentionné précédemment, ces conclusions peuvent dépendre des conceptions de la « cybercriminalité » appliquées, et de la nature des cas dont prennent connaissance les autorités nationales.

---

103 BAE Systems Detica et Université métropolitaine de Londres, 2012. *Criminalité organisée à l´ère numérique*

104 Moore, T., Clayton, R., Anderson, R., 2009. L´économie de la criminalité en ligne. *Journal sur les perspectives économiques* 32(3) :3-4.

105 BAE Systems Detica etUniversité métropolitaine de Londres, 2012. *Criminalité organisée à l´ère numérique*

106 *Rapport Norton sur la cybercriminalité. 2011.* Disponible sur : http ://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

107 UNODC, 2012. *Recueil d´affaires de criminalité organisée : une compilation d´affaires avec les commentaires et les enseignements tirés.*

108 Questionnaire de l´étude sur la cybercriminalité. Q85.

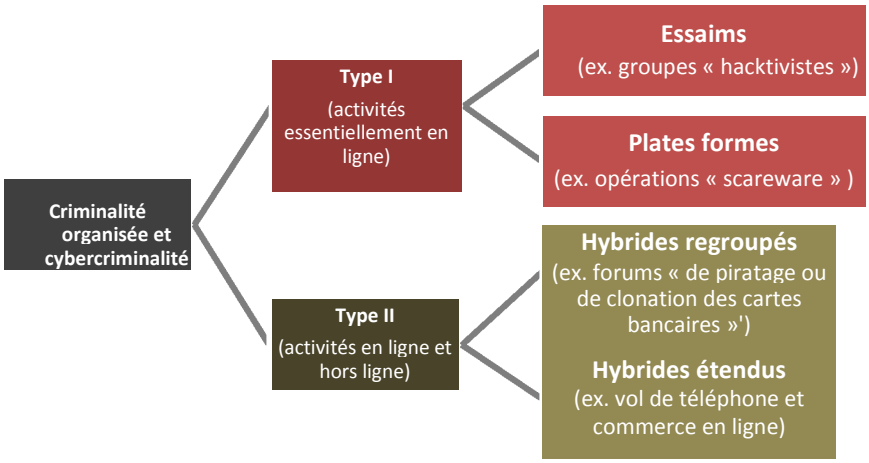
109 Lu, C.C., Jen, W.Y., Chang, W. et Chou, S., 2006. Cybercriminalité & Cybercriminels. *Journal informatique*, 1(6) :11-18. L´étude déclare également que 63 % de tous les suspects de cyberdélits ont agi de manière indépendante. Elle signale toutefois qu´il est difficile de détecter les complicités, et qu´il est vraisemblable que certains actes de cybercriminalités censés avoir été commis de manière indépendant peuvent en réalité avoir été commis par des groupes.

En général, bien que les groupes criminels prédominent dans certaines formes de cybercriminalité, il est clair que toutes les typologies – y compris les auteurs isolés– doivent être prises en compte. Les exemples inclus dans les encadrés de ce chapitre, par exemple, présentent en partie la gamme des auteurs d´infractions et les caractéristiques des groupes.

Structure des groupes – une analyse récente de la cybercriminalité et de la criminalité organisée propose une typologie basée sur le degré d´ implication des groupes dans des activités en ligne (opposées aux activités hors ligne) et la structure des associations dans le groupe.[110] Les groupes de type I sont censés avoir des activités largement dirigées ou axées sur des environnements numériques. Les groupes de type II sont censés avoir des activités qui oscillent entre des actes en ligne et des actes hors ligne. Le Type I est de plus divisé en « essaims » (structures dissociées, axées sur les activités en ligne) et en « plates-formes » (structures associées, axées sur les activités en ligne).

Du point de vue des services répressifs, la nature décentrée et en cellules des « essaims, » sans chaîne hiérarchique apparente, peut présenter des difficultés pour la police. Par contre, le fait que les essaims soient souvent des amateurs, qui vérifient moins les « affiliations, » peut représenter une opportunité pour la police. Il est, en revanche, plus difficile de pénétrer dans les « plateformes », mais elles possèdent une structure hiérarchique claire et des opératifs clés sur lesquels peuvent se concentrer les efforts des services répressifs. Les hybrides regroupés du Type II peuvent avoir des structures déroutantes basés sur des liens multiples pouvant être ciblés seulement par des opérations individuelles des services répressifs. Toutefois, le fait que ces groupes peuvent être coordonnés dans une certaine mesure, offre des opportunités de lancer des actions séquentielles contre les opérations criminelles individuelles.[111] De plus, les activités essentiellement réalisées hors ligne du groupe de Type III se croisent ou sont de plus en plus gérées dans des environnements numériques.[112] Les preuves suggèrent que – alors que les structures organisationnelles se recoupent souvent de manière très fluide – toutes les structures de ces groupes jouent un rôle dans les délits de cybercriminalité. Les plates-formes et les hybrides étendus regroupés représentent plus de 60 % des structures.[113]

Figure 2.15 : structures des groupes de criminalité organisée impliqués dans la cybercriminalité



Source : BAE Detica/LMU

Marchés de la cybercriminalité et de la criminalité organisée – les structures organisationnelles pour les cyberdélits motivés par des gains financiers, comme le vol des données bancaires et des numéros de cartes de crédit, ont fait l´objet d´une analyse spécifique. Un marché noir de la cybercriminalité a été identifié et comprend des groupes et des individus avec différents rôles ou exercent, parfois, de multiples rôles (cela inclut des « programmateurs », des « distributeurs », des « experts techniques », des

110 BAE Systems Detica et Université métropolitaine de Londres, 2012. *Criminalité organisée à l´ère numérique.*
111 *Ibid.* p.51.
112 *Ibid.* p.52.
113 *Ibid.* p.60.
114 Voir http ://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

« pirates », des « fraudeurs », des « hébergeurs », des « blanchisseurs », des « transporteurs d´argent », des « caissiers » et des « leaders »)[114] et qui interagissent dans le processus de création de logiciels malveillants, d´infection des ordinateurs (avec des courriels d´hameçonnage), de gestion des botnets, de collecte des données financières et personnelles, de vente de données, et de « l´encaissement » des informations financières.[115]

Un des types d´associations de ce marché est à travers l´utilisation de forums clandestins (souvent facilitée par des services d´anonymat ou des « routages en oignon » comme Tor) pour échanger des informations et négocier la vente des services de conseils, des services de dispersion d´infection, de location de botnet, des services de spam, d´hébergement, de listes d´e-mail et des données financières.[116] Même si ces marchés peuvent inclure un grand nombre d´individus, les associations peuvent être transitoires – en particulier dans le cas des transporteurs d´argent et des transactions « commerciales » criminelles, comme la location de botnet d´un individu ou un groupe à un autre. Les botnets sont utilisés pour commettre des attaques contre les systèmes d´information et pour voler des données, et sont offerts à un prix relativement bas, compensé par la rotation de nombreux clients. Par exemple, un serveur qui héberge un logiciel malveillant, exploite des kits ou des composants de botnet coûte entre 80$ et 200$ par mois. Un paquet d´administration de botnet appelé « Eleonore Exploit Pack » a une valeur au détail 1000$. Louer un botnet de 10 à 20 ordinateurs, administré avec ce paquet, coûte en moyenne 40$ par jour. Un kit Zeus v1.3 coûte de 3000$ à 4000$.[117] Ces coûts sont relativement bas par rapport au gain financier potentiel, qui peut s´élever de dizaines de milliers jusqu´à des dizaines de millions de dollars.

Interactions des auteurs d´infractions

Les plaintes présentées par des autorités d´application de la loi d´un pays d´Amérique du nord lors de procédures pénales engagées contre un groupe d´auteurs allégués d´actes de cybercriminalité transnationale révèlent la nature des interactions au sein des marchés de la cybercriminalité. L´extrait ci-après, obtenu par le biais de mandats de perquisition, provient des messages instantanés ou des salles de discussion :

11:55:42:68 PM CC-4 combien me coûtera votre Trojan ?
11:56:33:00 PM Alias-1 2000 par mois en incluant l´hébergement et le support
…
11:56:55:38 PM Alias-1 vous pouvez le donner [l´accès au botnet] à plusieurs personnes, le vérificateur et des collègues
…
12:28:22:32 AM Alias-1 …j´ai e .exe qui donne au moins 200 300 dollars pour 1k de téléchargement pour [différents pays] [c´est à dire vous obtiendrez avec [le botnet] 200USD-300USD pour chaque 1000 séries de données volées à des victimes de [différents pays]]

Source : http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin,%20Nikita%20Complaint.pdf

Le marché, dans son ensemble, n´est pas une entreprise d´un seul groupe criminel. Il s´agit plutôt d´un « réseau social d´individus impliqués dans des activités de criminalité organisée ».[118] Certains individus et des petits groupes – comme les programmateurs originaux des logiciels malveillants, et les propriétaires des botnets C&C – peuvent représenter des éléments clés du marché, autour desquels gravitent d´autres individus, essaims et plates-formes.

115 Voir, par exemple, Fortinet, 2013. *Fortinet 2013 rapport sur la cybercriminalité* ; Panda Security, 2010. Le marché noir de la cybercriminalité *: découvert,* et Groupe IB, 2011. *état et tendances du marché russe de la criminalité numérique*

116 Voir, par exemple, Motoyama, M. *et al.*, 2011. *Une analyse des forums clandestins.* IMC 2011, 2-4 novembre 2011, Berlin ; et Stone-Gross, B. *et al.*, 2011. *L´économie souterraine du Spam : le point de vue d´un botmaster sur la coordination des campagnes de spam à grande échelle.*

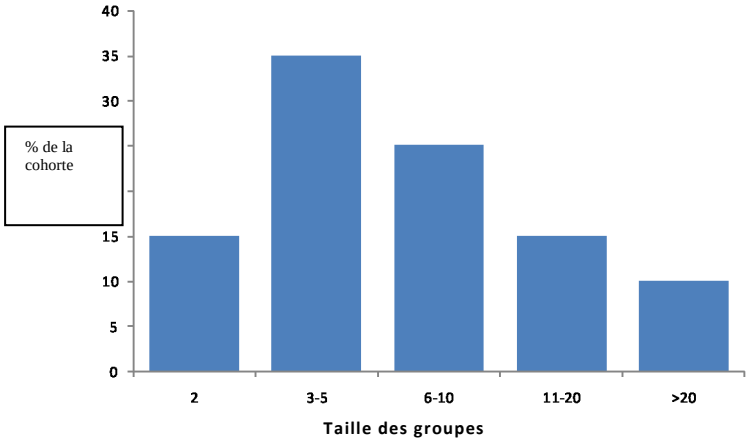
117 Laboratoire ESET d´amérique latine, 2010. *ESET, Tendances pour 2011 : les botnets et les logiciels malveillants dynamiques.* Disponible sur : http ://go.eset.com/us/resources/white-papers/Trends-for-2011.pdf

118 Voir, par exemple, Spapens, T., 2010. Macro-réseaux, processus coopératifs et commerciaux : une approche intégrée de la criminalité organisée. *Journal européen sur la criminalité, le droit pénal et la justice*, 18 :285-215.

119 Voir, par exemple, créateur de botnet Bredolab (http ://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/) ;créateur de botnet Kelihos (http ://nakedsecurity.sophos.com/2012/01/24/microsoft-kelihos-botnet-suspect/) ; créateur de botnet Mariposa (http ://nakedsecurity.sophos.com/2012/08/07/mariposa-botnet-trial/) ; et SpyEye convictions (http ://nakedsecurity.sophos.com/2012/07/01/uk-cops-announce-sentencing-of-baltic-malware-trio/)

D´après les enquêtes et les arrestations effectuées par les services répressifs jusqu´à ce jour, il semble que les personnes qui créent et gèrent des éléments clés du marché, comme les botnets, agissent isolément ou au sein de groupes relativement restreints.[119] Sur une cohorte de groupes[120] identifiés et examinés par l´étude BAE Detica/LMU, par exemple, il s´avère que les associations de 3 à 5 individus qui avaient opéré ensemble pendant environ une année étaient le patron organisationnel le plus commun.[121] La moitié des groupes comprenait 6 individus ou plus, et un quart incluait 11 individus ou plus. Un quart des groupes actifs opérait depuis moins de six mois. Toutefois, la taille des groupes ou la durée de l´association ne correspond pas nécessairement à l´impact du délit – des groupes restreints peuvent infliger des dommages importants en peu de temps.

Figure 2.16 : taille typique des groupes de criminalité organisée impliqués dans la cybercriminalité



Source : BAE Detica/LMU

Lorsque les individus et les associations au sein du marché ne correspondent pas à la définition formelle de la criminalité organisée, il est possible qu´ils relèvent des dispositions relatives au complot ou aux associations de l´Article 5 de la Convention sur la criminalité organisée qui couvrent les délits de complot/et ou d´association criminelle, ainsi que le fait d´organiser, de diriger, d´aider, de soutenir, de faciliter ou de conseiller le fait de commettre un délit grave impliquant un groupe de criminalité organisée.[122]

Répartition géographique

Bien que l´on suppose souvent que les cybercriminels opèrent fréquemment de manière globale et décentralisée, les preuves suggèrent que les groupes peuvent être géographiquement proches même si leurs activités sont internationales. Les réseaux locaux et régionaux par exemple, ainsi que les réseaux d´amis et de proches restent des facteurs importants. En effet, même si les groupes entrent en contact en ligne, il est prouvé

« Logiciel malveillant ZeuS »

Les ingénieurs en logiciel d´Europe de l´est ont utilisé un logiciel malveillant appelé le virus « ZeuS ». Les ordinateurs ciblés sont infectés lorsque la victime ouvre un courriel apparemment bénin. Avec l´accès aux numéros de comptes bancaires de la victime et aux mots de passe, les délinquants peuvent accéder aux comptes bancaires de la victime. Des complices des délinquants publièrent des annonces sur des sites web en langue russe qui invitaient des étudiants résidant en Amérique du nord à les aider à transférer des fonds hors du pays. De faux passeports étaient fournis à ces transporteurs appelés « mules » et on leur ordonnait d´ouvrir des comptes sous de faux noms dans plusieurs institutions financières d´Amérique du nord. Les auteurs des délits transféraient des fonds des titulaires légitimes des comptes vers les comptes des mules qui recevaient alors l´instruction de transférer ces fonds sur des comptes offshore, ou dans certains cas de passer les fonds en contrebande hors d´Amérique du nord. Cinq individus furent arrêtés en Europe de l´est, 11 en Europe du nord et 37 furent accusés en Amérique du nord. La motivation des participants semblait être essentiellement financière. La nature répétitive et le volume des infractions individuelles attirèrent l´attention des autorités et contribuèrent à mettre fin à la collusion.

120 Il faut noter que l´étude de BAE Systems et de l´Université métropolitaine de Londres inclut des groupes de 2 personnes. Ces associations relèvent de la définition contenue à l´Article 2(a) de la Convention sur la criminalité organisée, qui mentionne un groupe de 3 personnes ou plus

121 BAE Systems Detica et l´Université métropolitaine de Londres, 2012. *La criminalité organisée à l´ère numérique.*

122 Voir la Convention sur la criminalité organisée, Arts. 5(1)(a) et (b).

qu´ils utilisent des méthodes d´association et des formes de connaissances qui ont des caractéristiques locales. Ceci donne lieu à un effet de « glocalisation » où les facteurs linguistiques et culturels sont utilisés par des groupes criminels organisés pour promouvoir leurs activités. Les forums clandestins en ligne, par exemple, ont des langages, des surnoms et des repères culturels locaux. Ceci a pour effet d´en rendre l´accès difficile pour les services répressifs, et de permettre aux associations de malfaiteurs reconnues de s´identifier entre elles. Les localisations qui montrent des niveaux élevés d´activités de cybercriminalité avec des liens potentiels pour organiser des délits se trouvent, entre autre, dans des pays d´Europe de l´est et d´Asie de l´est. Le logiciel malveillant ZeuS, par exemple, est apparu en Europe de l´est en 2007, et des plateformes notables de cybercriminalité ont également été signalées en Europe de l´est.[123] Il est intéressant de noter que ce patron concorde avec les données indiquant la localisation des serveurs de commande et de contrôle des botnets présentées dans ce chapitre.[124] Il existe également une inquiétude croissante relative à l´envergure de la cyber-victimisation en Asie de l´est, et à un rôle potentiellement significatif des groupes criminels locaux.[125]

124 Voir ci-dessus la Section 2.2 La situation globale de la cybercriminalité, outils criminels– le botnet.

125 Kshetri, N., 2013. *Cybercriminalité et cybersécurité dans les pays du sud mondialisé*. Houndmills, UK : Palgrave Macmillan, chapitre 3 ; Broadhurst, R.,
Chang, Y.C., 2013. Cybercriminalité en Asie : tendances et défis. *dans :* Hebenton, B., Shou, S.Y. and Liu, J. (eds.) *manuel asiatique sur la criminologie*. Springer.

123 Bhattacharjee, Y., 2011. Pourquoi y a-t´il autant de cybercriminels dans une ville isolée de Roumanie ? *Wired*, 19(2) :82.

Page intentionnellement laissée vierge

CHAPITRE TROIS : CADRES ET LÉGISLATION

Ce chapitre examine le rôle des législations et des cadres régionaux, nationaux et internationaux dans la prévention et la lutte contre la cybercriminalité. Il s´avère que la législation est requise dans tous les domaines, et cela inclut l´incrimination, les pouvoirs procéduraux, la juridiction et la coopération internationale. Au cours de la dernière décenneie,l y a eu, des avancées importantes concernant la promulgation d´instruments multilatéraux visant à lutter contre la cybercriminalité. Le chapitre souligne une fragmentation juridique croissante au niveau national et international.

3.1 Introduction – le rôle des lois

Principaux résultats :

- les développements techniques associés à la cybercriminalité impliquent que – même si les lois traditionnelles peuvent être appliquées dans une certaine mesure – la législation doit se confronter à de nouveaux concepts et objets, aussi intangibles que des « données informatiques, » qui ne sont pas traditionnellement traités par la loi ;
- les mesures juridiques sont cruciales pour la prévention et la lutte contre la cybercriminalité, et sont requises dans tous les domaines, et ceci inclut l´incrimination, les pouvoirs procéduraux, la juridiction, la coopération internationale et la responsabilité des fournisseurs des services d´internet ;
- au niveau national, les lois en matière de cybercriminalité concernent le plus souvent l´incrimination – en établissant des délits spécialisés pour ce qui concerne les principaux actes de cybercriminalité. Toutefois, les pays mentionnent de plus en plus la nécessité de législation dans d´autres domaines ;
- en comparaison avec les lois existantes, les lois, nouvelles ou envisagées, relatives à la cybercriminalité traitent plus fréquemment les questions relatives aux mesures d´enquêtes, à la juridiction, aux preuves électroniques et à la coopération internationale.

Spécificité informatique

Les mesures juridiques jouent un rôle clé dans la prévention et la lutte contre la cybercriminalité. Le droit est un outil dynamique qui permet à l´état de riposter face aux nouveaux défis sociétaux et en matière de sécurité, tels que le juste équilibre entre la vie privée et le contrôle de la criminalité, ou l´étendue de la responsabilité des entreprises qui fournissent des services. Outre les lois nationales, au niveau international, le *droit des nations* – le droit international – couvre les relations entre les états et leurs multiples facettes. Les dispositions des lois nationales et internationales sont pertinentes pour ce qui concerne la cybercriminalité.

Les développements techniques associés à la cybercriminalité impliquent que – même si les lois traditionnelles peuvent être appliquées dans une certaine mesure – la législation doit se confronter à de nouveaux concepts et objets, qui ne sont pas traditionnellement traités par la loi. Dans plusieurs états, les lois relatives aux développements techniques datent du 19ème siècle. Ces lois étaient, et sont encore dans une grande mesure, axées sur des objets physiques – autour desquels gravitait la vie quotidienne de la société industrielle. Pour cette raison, de nombreuses lois générales traditionnelles ne tiennent pas compte des spécificités de l´information et de la technologie de l´information associées à la cybercriminalité et aux délits qui génèrent des preuves électroniques.

Ces actes sont amplement caractérisés par de nouveaux objets *intangibles* tels que des données ou des informations. Alors que les *objets physiques* peuvent généralement être exclusivement attribués à des propriétaires déterminés, il peut être beaucoup plus difficile d´attribuer la propriété de l´*information*. Cette différence est importante, par exemple, pour le concept juridique de « vol », appliqué par les lois traditionnelles de nombreux pays. Les éléments qui constituent un vol traditionnel peuvent ne pas s´appliquer à un « vol » de données informatiques, par exemple – pourinclure les données ou les informations bien que les concepts relatifs aux objets soient larges. Les données resteraient en possession du détenteur original, (selon les approches des lois nationales) en l'absence de conformité avec les éléments juridiques requis, tels qu´une « expropriation » ou la « prise » de l´objet. De même, les références juridiques à un « lieu » privé ou public dans les lois relatives au harcèlement peuvent ou non (à nouveau selon les approches des lois nationales) s´étendre à des « lieux » en ligne. Ces exemples illustrent un besoin potentiel – dans certains domaines – d´adaptation des doctrines juridiques aux nouvelles technologies de l´information.[1]

Fonctions de la législation sur la cybercriminalité

- Établir des normes claires de conduite pour l´utilisation des dispositifs informatiques.
- Dissuader les auteurs d´infractions et protéger les citoyens.
- Permettre les enquêtes des services répressifs tout en protégeant la vie privée.
- Établir des procédures de justice pénale efficaces et équitables.
- Requérir des normes minimales de protection standards dans des domaines tels que la conservation et le traitement des données.
- Permettre la coopération entre les pays dans des affaires pénales impliquant la cybercriminalité et les preuves électroniques.

Cela soulève la question de savoir si la cybercriminalité devrait être couverte par les dispositions générales des lois pénales existantes, ou si de nouvelles infractions spécifique relatives à l´informatique sont requises. On ne peut répondre à la question de manière générale, car cela dépend de la nature des actes individuels et de la portée et de l´interprétation des lois nationales. Le chapitre quatre de cette étude (incrimination) examine l´utilisation de lois générales et de lois spécialisées dans le cadre de l´incrimination des actes de cybercriminalité. Les réponses présentées par les pays montrent que certaines des « principales » infractions de la cybercriminalité sont couvertes par des infractions spécifique relatives à l´informatique, alors que d´autres sont couvertes par des infractions générales.[2] Les chapitres cinq (application des lois et enquêtes) et huit (prévention) considèrent que l´utilisation de lois spécifiques relatives à l´informatique ou à l´information peut être requise dans les domaines des pouvoirs d´enquêtes des services répressifs [3] et de la responsabilité des fournisseurs des services d´internet.[4]

Catégories pertinentes du droit

Bien que les lois pénales soient souvent perçues comme étant les plus pertinentes lorsqu´il s´agit de la cybercriminalité, les ripostes juridiques possibles incluent également l´utilisation du droit civil (qui traite les relations juridiques entre les personnes), et le droit administratif (qui traite les relations juridiques entre les personnes et l´état). D´autres divisions dans ces régimes juridiques incluent le droit procédural et le droit positif, ainsi que des lois régulatrices et constitutionnelles, ou basées sur des droits. Dans de nombreux systèmes juridiques, ces régimes sont caractérisés par des garanties, des institutions et des objectifs spécifiques. Les lois sur la cybercriminalité se trouvent généralement dans les domaines du droit pénal procédural et du droit positif.

1 Sieber, U., 2012. Straftaten und Strafverfolgung im internet. *In* : *Gutachten des Deutschen Juristentags*, Munich : C.H. Beck, pp.C 14-15.

2 Voir le chapitre quatre (incrimination), Section 4.1 Aperçu de l´incrimination, cyberdélits et infractions générales.

3 Les études existantes signalent que des dispositions spécifiques relatives à l´informatique sont requises pour ce qui concerne les pouvoirs d´enquêtes, afin de permettre de prendre des mesures de conservation immédiate des données et d´utilisation d´outils criminologiques à distance ; voir Sieber, U., 2012. Straftaten und Strafverfolgung im internet, *In : Gutachten des Deutschen Juristentags*. Munich : C.H. Beck, pp.C 62-72, 103-128.

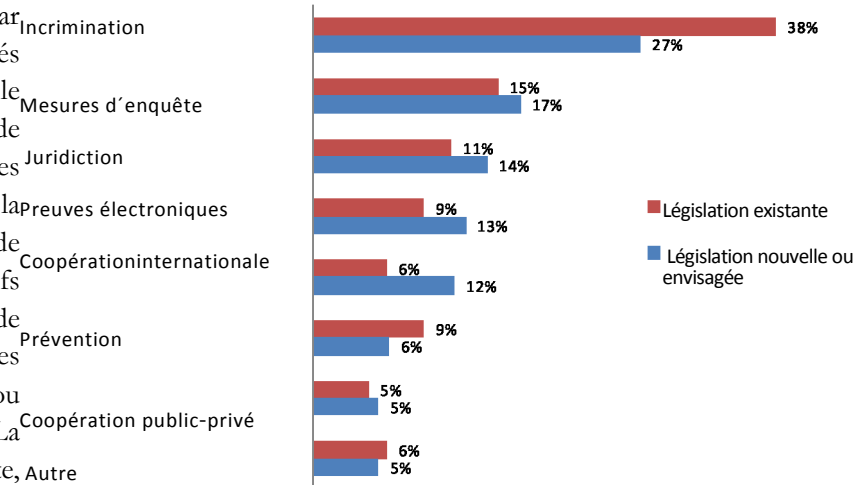
4 Par exemple, la transmission ou l´hébergement de grands volumes de contenus de tiers des fournisseurs de servicesd´internet rendent impraticable l´application des règles traditionnelles relatives à la responsabilité, qui sont applicables à la presse et aux médias–qui sont souvent tenus de contrôler le contenu avant la publication. La responsabilité générale est remplacée par des conditions spécifiques, y compris des procédures de notification. Voir le chapitre huit (prévention), la Section 8.3 prévention de la cybercriminalité dans le secteur privé et universitaire, prévention de la cybercriminalité des fournisseurs d´hébergement et de services internet.

Toutefois, de nombreux domaines du droit sont également importants. Le panel d´actes liés à l´informatique que l´état souhaiterait réglementer ne requiert pas toujours l´utilisation de mesures intrusives de droit pénal. Par exemple, les actes liés à l´informatique et considérés comme étant des infractions mineures, peuvent être traités conformément aux règlementations civiles et administratives plutôt qu´au droit pénal. De plus, les lois pénales font souvent référence à des normes sous-jacentes du droit administratif et civil, ou la protection des données. Des dispositions combinées peuvent également prévoir, simultanément, la responsabilité pénale, civile et administrative. La législation pertinente en matière de cybercriminalité peut donc traiter un vaste panel de questions, et cela inclut : l´incrimination de comportements spécifiques ; les pouvoirs d´enquêtes de la police ; des questions de juridiction pénale ; la recevabilité des preuves électroniques ; la protection des données, la responsabilité des fournisseurs de services électroniques ; et les mécanismes de coopération internationale dans des affaires pénales liées à la cybercriminalité.

L´étendue de ces domaines est illustrée par les pays répondants qui, lorsqu´on leur demandait d´indiquer la législation pertinente en matière de cybercriminalité, mentionnaient de nombreuses lois incluant : des codes pénaux ; des lois sur la criminalité utilisant les technologies avancées ; des codes de procédures pénales ; des lois sur les écoutes téléphoniques ; des lois sur la preuve ; des lois sur les communications électroniques ; des lois sur la sécurité des technologies de l´information ; des lois sur la protection des informations et des données personnelles ; des lois sur les transactions électroniques ; des lois sur la cybersécurité et des lois sur la coopération internationale.[5]

La figure 3.1 montre les domaines couverts par la législation, signalés par les pays dans le questionnaire de l´étude. Les données représentent la répartition de plus de 250 textes législatifs signalés existants et de plus de 100 textes nouveaux ou envisagés.[6] La législation existante, ainsi que les lois nouvelles ou prévues, se concentrent surtout sur l´incrimination.[7] Comme le mentionne le chapitre quatre (incrimination), ceci inclut des dispositions générales du droit pénal et des dispositions spécifiques relatives à l´informatique. Le fait que l´incrimination représente le domaine le plus fréquent des lois nouvelles ou prévues, indique que la priorité permanente des pays est le développement de nouveaux cyberdélits spécifiques, et/ou l´adaptation ou la modification d´infractions générales existantes.

Figure 3.1 : domaines de législation en matière de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalit Q12 et Q14. (n=55,36; r=262,111)

5 Questionnaire de l´étude sur la cybercriminalité Q12.
6 Législation mentionnée dans les réponses questionnaire de l´étude sur la cybercriminalité. Q12 et 14.
7 Alors que dans les pays de Common Law, les compétences juridictionnelles pour développer et étendre le droit pénal ont traditionnellement été majeures, les approches modernes de l´incrimination requièrent le droit statutaire même dans les principaux systèmes de Common Law. Voir *U.S. v. Hudson et Goodwin*,

Il existe cependant une nette tendance à la réduction de la proportion relative des législations nouvelles ou prévues (comparées aux législations existantes) concernant l´incrimination, et une augmentation de l´attention portée à d´autres domaines, tels que les mesures d´enquêtes, la juridiction, les preuves électroniques et notamment la coopération internationale. Ceci peut indiquer une tendance – du moins dans les pays répondants – vers une reconnaissance croissante du besoin d´une législation en matière de cybercriminalité parmi une multitude de domaines législatifs. Avec l´introduction de ces domaines législatifs, cette section présente brièvement les considérations juridiques pertinentes pour chacun d´eux.

Incrimination –le principe de *nullum crimen sine lege* (il n´y a pas de délit sans loi) exige que la conduite qui constitue un délit pénal soit clairement décrite par la loi.[7] Comme cela a été mentionné précédemment, afin de décrire sans ambiguïté la conduite constituant un cyberdélit, les lois pénales peuvent requérir l´introduction de nouveaux objets juridiques relatifs à l´information, ainsi que l´application de la protection des intérêts juridiques traditionnels pour ce qui concerne les nouvelles formes d´actes liés à l´informatique. Les nouveaux objets juridiques requis peuvent inclure des définitions comme les « données informatiques » ou « l´information informatique », et des intérêts juridiques tels que « l´intégrité » des systèmes informatiques.

Par le biais de ces concepts, le droit pénal a des outils de protection contre la violation des « cyber » intérêts des personnes – par exemple, en contrôlant l´accès aux systèmes informatiques qu´ils possèdent. Les différents systèmes juridiques ont différents critères de base pour identifier les conduites pouvant être incriminées par le droit pénal.[8] L´application systématique de ces critères à des conduites liées à l´informatique peut être difficile. Néanmoins, dans de nombreux systèmes nationaux, et dans certaines initiatives régionales ou internationales, il y a des travaux théoriques visant à renforcer l´incrimination des conduites constituant des cyberdélits. Le rapport explicatifpour la Convention sur la cybercriminalité du Conseil de l´Europe, par exemple, se réfère exhaustivement aux « intérêts juridiques » et aux « dommages » en jeu.[9] S´il n´existe aucune justification solide pour l´incrimination d´une conduite spécifique, il surgit alors le risque de sur incrimination. À cet égard, les lois internationales sur les droits de l´homme représentent un outil important pour évaluer les lois pénales conformément aux normes internationales externes. Le chapitre quatre de cette étude (incrimination) examine en détail de nombreux cyberdélits communs et leur conception dans les lois nationales et internationales.

Outre la conduite spécifique incriminée, les études sur les cyberdélits doivent tenir compte de la partie générale du droit pénal. C´est la partie qui aborde les questions applicables à tous les délits, comme la complicité, la tentative, l´omission, l´état d´esprit (tentative), la défense, et la responsabilité pénale des personnes morales. Les cyberdélits relèvent en général de la partie générale du droit pénal, comme c´est le cas pour d´autres délits spécifiques. De nombreux pays répondants ont signalé que « généralement » les délits pénaux sont limités à des actes intentionnels.[10] Cependant, ces positions générales peuvent être modifiées pour des actes spécifiques – comme lorsqu´une « intention particulière » est requise. Le chapitre quatre (incrimination) examine cette question de manière plus approfondie.

Pouvoirs procéduraux – il est impossible de mener une enquête efficace sur un délit sans les pouvoirs d´enquête adéquats. En raison de leur nature souvent intrusive, ces mesures doivent être règlementées par la loi et accompagnées de garanties adéquates. Alors que certaines mesures d´enquête peuvent être mises en œuvre avec les pouvoirs traditionnels, de nombreuses dispositions procédurales ne se transposent pas aisément d´une approche spatiale, orientée sur l'objet, à une approche impliquant le stockage de données électroniques et le flux de données en temps réel. Des pouvoirs spécialisés sont donc nécessaires pour recueillir le contenu informatique communiqué ou stocké sous forme électronique, pour identifier et localiser les communications et les dispositifs informatiques, pour « geler » rapidement les données informatiques volatiles et pour mener des enquêtes d´infiltration en ligne.[11] Ces pouvoirs sont requis non seulement pour les enquêtes sur la

cybercriminalité mais également pour enquêter sur les délits qui génèrent des preuves électroniques. Le chapitre cinq (application des lois et enquêtes) examine un certain nombre de pouvoirs d´enquêtes spéciaux prévus par les lois nationales et internationales.

---

11 U.S. 32 (1812) ; Dubber, M., 1999. Réforme du droit pénal américain. *Journal sur la criminologie et le droit pénal américain* 90(1)49-114 ; et Simester, A.P., Spencer, J.R., Sullivan, G.R., Virgo, G.J., 2010. Droit pénal. 4ieme ed. Oxford/Portland : Hart Publishing, p.46.

8 Y compris des concepts tels que les dommages, l´outrage, l´illicéité, la moralité, le paternalisme, les biens légaux et la dissuasion. Voir Ashworth, A., 2006. *Principes du droit pénal.* 6ieme ed. Oxford : Oxford University Press, p.27 ; Dubber, H., 2005. Positive Generalprävention und Rechtsgutstheorie. *Zeitschrift für die gesamte Strafrechtswissenschaft,* pp. 485-518, pp.504 et seq. ; Hassemer, W., 1980. *Theorie und Soziologie des Merbrechens.* Frankfurt a.M. ;Feinberg, J. 1984.*Nuire à d´autres.* Oxford : Oxford University Press.

9 Conseil de l´Europe. 2001. Rapport explicatif pour la Convention sur la cybercriminalité.

10 Questionnaire de l´étude sur la cybercriminalité Q40.

11 Sieber, U., 2012. Straftaten und Strafverfolgung im internet. *In* : *Gutachten des Deutschen Juristentags.* Munich : C.H. Beck, pp.C14-15.

Collecte et utilisation des preuves – le droit pénal procédural contient typiquement des dispositions sur la collecte et la recevabilité de la preuve. Quand il s´agit de preuves sous forme électronique, les données peuvent être facilement altérées. La collecte et le traitement des preuves électroniques doivent donc garantir l´intégrité, l´authenticité et la continuité des preuves durant toute la période comprise entre leur saisie et leur utilisation lors du procès – un processus souvent appelé la « chaîne de surveillance ». Les réponses du questionnaire, fournies par les pays, montrent que certains pays créent des règles spéciales de preuve pour ce qui concerne les preuves électroniques, alors que d´autres pays préfèrent leur donner le même traitement que pour d´autres formesde preuves. Dans les pays de Common Law, les lois doivent examiner plus en détail les preuves et les règles relatives à la recevabilité des preuves, alors que les pays de droit continental s´appuient souvent sur le principe de la libre évaluation judiciaire des preuves.[12] Le chapitre six (preuves électroniques et justice pénale) examine la question des preuves électroniques de manière plus approfondie.

Règlementation et risques – le droit pénal vise à traduire en justice les délinquants qui ont commis des actes criminels. D´autre part, les lois régulatrices, sur les réductions ou l´anticipation des risques visent à éviter que de futurs actes ne se produisent, ou à faciliter les enquêtes menées par les services répressifs ou à mettre en œuvre des mesures de justice pénale.[13] En ce qui concerne la cybercriminalité, plusieurs approches, dont le filtrage d´internet, la protection de données, la conservation des données, et des mesures proactives contre les infrastructure criminelles entrent dans cette catégorie. Le caractère anticipatif des lois qui autorisent plusieurs de ces mesures, exige qu´elles soient accompagnées de garanties spécifiques, afin de se prémunir contre des violations disproportionnées des droits individuels ou l´utilisation superflue de pouvoirs coercitifs.[14] Le chapitre huit (prévention) examine, parmi d´autres aspects de la prévention, plusieurs cadres réglementaires.

Juridiction et coopération internationale – plus de la moitié des pays répondants a signalé qu´entre 50 et 100 % des actes de cybercriminalité enregistrés par la police impliquaient un « élément transnational ».[15] La poursuite des actes criminels transnationaux exige que les états revendiquent deux types de « juridiction » – une juridiction de fond et d´enquête. Les états doivent tout d´abord être en mesure de faire valoir que leur droit pénal national est applicable à un acte qui n´a pas été commis, ou seulement partiellement, sur le territoire national. Puis les états doivent être en mesure de mettre en œuvre des actes d´instruction concernant le territoire d´autres pays. Dans la mesure où les enquêtes peuvent impliquer des atteintes à la souveraineté des états, les processus formels et informels de consentement et de coopération internationale sont requis. Plusieurs de ces processus se rapportent au droit international des traités bilatéraux et multilatéraux. Toutefois, les lois nationales peuvent également spécifier les procédures à appliquer, ou créer des bases de coopération conformément à leur propre droit. Le chapitre sept (coopération internationale) examine ce domaine de façon détaillée.

12 Damaska, M.R., 1973.L´obstacle de la preuve pour la condamnation et deux modèles de procédure pénale : une étude comparative. Revue juridique de l´*Université de Pennsylvanie*121(3) :506-589 (1972-73).

13 Sieber, U., 2012. Straftaten und Strafverfolgung im internet. *In* : *Gutachten des Deutschen Juristentags*. Munich : C.H. Beck, note 1, pp.69-74.14 Voir la Commission européenne. 2012. *Préserver la vie privée dans un monde connecté– un cadre européen de protection des données pour le 21ieme siècle* COM(2012) 9 final http ://ec.europa.eu/justice/datahttp ://ec.europa.eu/justice/data protection/document/review2012/com_2012_9_en.pdf

15 Questionnaire de l´étude sur la cybercriminalité Q83.

3.2 Divergence et harmonisation des lois

Principaux résultats :

- l´harmonisation des lois sur la cybercriminalité est essentielle pour, entre autres, éliminer l´impunité et faciliter la collecte globale de preuves ;
- les divergences des lois nationales sur la cybercriminalité proviennent d´un panel de facteurs qui inclut des différences juridiques et constitutionnelles sous-jacentes ;
- le domaine des peines imposées aux délits de cybercriminalité est un bon exemple des divergences existantes dans les approches nationales relatives aux actes de cybercriminalité. L´examen d´un unique délit – l´accès illégal – est suffisant pour constater de considérables différences dans le degré perçu de gravité ;
- un tiers des pays qui ont répondu au questionnaire considère que leur législation est totalement ou hautement harmonisée avec les pays considérés comme importants dans le cadre de la coopération internationale ;
- toutefois, cela varie au niveau régional, avec des niveaux plus élevés d´harmonisation dans les Amériques et en Europe ;
- ceci peut être dû dans certaines régions à l´utilisation d´instruments multilatéraux, fondamentalement conçus pour jouer un rôle dans l´harmonisation.

Différences sous-jacentes des lois

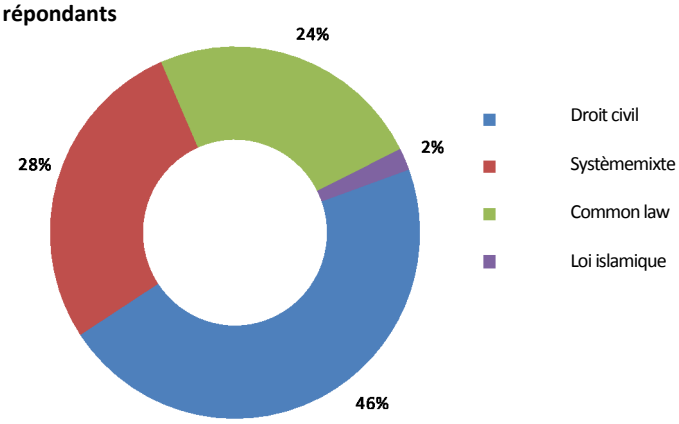
Dans le monde globalisé d'aujourd'hui, les lois consistent en une multitude de systèmes juridiques régionaux, nationaux et internationaux. Les interactions entre ces systèmes ont lieu à de multiples niveaux. De ce fait, les dispositions se contredisent parfois entre elles et entrainent des conflits juridiques, ou ne coïncident pas suffisamment et créent des lacunes juridictionnelles.[16]

16 Sieber, U., 2010. L´ordre juridique dans un monde globalisé *dans* : Von Bogdandy, A., Wolfrum, R. (eds.) *Max Planck annuaire des Nations Unies* 14, 1-49.

17 Sieber, U., 2008. Maitrise de la complexité dans le cyberespace global. *dans* :Delmas-Marty, M., Pieth, M., et Sieber, U. (eds.) *Les chemins de l´»harmonization pénale.* Paris, pp.127-202 (192-197).

Des visions globales différentes quant à l´admissibilité des formes de contenu internet offrent plusieurs alternatives théoriques. Les états pourraient choisir de restreindre la portée de leur juridiction pénale aux actes commis sur leur propre territoire national. Ils pourraient se focaliser sur les poursuites à l'encontre des personnes qui ont accès au contenu sur leur territoire, indépendamment de la source de ce contenu ou ils pourraient entreprendre une action extraterritoriale à l´encontre des producteurs de ce contenu. Ces points de vue illustrent l´importance croissante des approches et des différences juridiques en matière de cybercriminalité. Le chapitre quatre (incrimination) examine ce point de manière plus approfondie, y compris du point de vue des lois internationales sur les droits de l´homme.

Figure 3.2 : classification du système juridique national des pays répondants



Questionnaire de l´étude sur la cybercriminalité Q15. (n=54)

Les divergences entre les lois nationales remontent aux différences fondamentales entre les familles juridiques. Les principales familles juridiques généralement identifiées incluent le droit continental européen,[18] la Common Law,[19] le droit islamique,[20] et le droit mixte (comme le droit chinois).[21] Les réponses que les pays ont fournies au questionnaire de l´étude montrent qu´un vaste panel de systèmes juridiques est représenté.[22]

Les familles juridiques sont un élément important pour caractériser l'héritage juridique, qui inclut des systèmes qui partagent des caractéristiques particulières, provenant, par exemple, de racines culturelles communes.[23] Néanmoins, les lois nationales ne sont pas statiques, et des similarités entre les systèmes peuvent exister à un moment donné et postérieurement disparaître.[24] Ainsi les différences historiques peuvent disparaître ou perdre leur pertinence pratique.

18 Le droit continental européen est souvent caractérisé par des règles normatives abstraites, des structures systématiques et une forte influence de la réflexion académique. Le droit pénal est entièrement codifié par le code pénal, qui prévoit également les principes généraux de la responsabilité pénale applicable à toutes les formes de conduite criminelle. Voir Zweigert, K., Kötz, H. 1998. Droit comparé. 3ème éd. Oxford/New York : Clarendon Press, p.69. Voir aussi Weigend, T. 2011. *dans* : Heller, K.J., Dubber, M.D. (eds.) *le manuel du droit pénal comparé*, Stanford : Stanford University Press, pp.256 et seq. ; Elliott, C., *ibid*., p.213. ; Gómez-Jara Díez, C., Chiesa, L.E., *ibid*, p.493 ; Thaman, S.C., *ibid*., p.416.

19 Au contraire dans les juridictions de Common Law, les dispositions de fond sont généralement rédigées dans des termes descriptifs, garantissant l´accessibilité de la loi et reflétant la solide position des juges non professionnels dans les juridiction de Common Law. Le droit jurisprudentiel a longtemps été la source principale du droit pénal positif et reste un élément important. Néanmoins, la codification est aujourd´hui une norme répandue, parfois par le biais d´actes législatifs séparés plutôt que par un unique code pénal. Voir Legeais, R., 2004. *Grands systèmes de droit contemporains.* Paris : Litec, pp.357, 366 ; Ashworth, A. (Royaume uni). 2011, p.533, and also Robinson, P. (états unis) 2011, p.564. dans : Heller, K.J., Dubber, M.D. (eds.) *le manuel du droit pénal comparé*, Stanford : Stanford University Press ; Simester, A.P., Spencer, J.R., Sullivan, G.R., Virgo, G.J. 2010. Droit pénal. 4ème ed. Oxford/Portland : Hart Publishing, p.46 ; Ashworth, A. 2009. *Principes du droit pénal.* 6ème ed. Oxford/New York : Oxford University Press, p.8.

´20 Le droit islamique est caractérisé par la Shari »a, la loi sacrée de l´Islam, et la fiqh, la jurisprudence des juristes islamiques. Les délits sont classifiés en fonction de leurs sources juridiques et des peines prévues. Certains délits principaux sont sanctionnés par des peines fixées (hudud). D´autres délits principaux sont sanctionnés par le biais d´un raisonnement juridique basé sur la Ijmaet la Qiyas. Les lois islamiques permettent en général une grande flexibilité en matière d´incrimination avec l´évolution de diverses écoles de droit théologique. Voir Tellenbach, S., 2011. *dans* : Heller, K.J., Dubber, M.D. (eds.) *le manuel du droit pénal comparé.* Stanford : Stanford University Press, p.321.

21 Le droit pénal chinois a été influencé par plusieurs systèmes juridiques et la magistrature est habilitée à donner des interprétations judiciaires contraignantes du droit. Voir Luo, W., 2011. *Dans*Heller, K.J., Dubber, M.D. (eds.) *le manuel du droit pénal comparé.* Stanford : Stanford University Press, p.138 ; et Bu, Y., 2009. *Einfühlrung in das Recht Chinas.* Munich : C.H. Beck, p. 20.

22 Questionnaire de l´étude sur la cybercriminalité Q15.

23 Voir Ferrante, M., 2011. *In :* Heller, K.J., Dubber, M.D. (eds.) *le manuel du droit pénal comparé.* Stanford : Stanford University Press, p.13.

24 Zweigert, K., Kötz, H. 1998.*Droit comparé.* 3ieme ed. Oxford/New York : Clarendon Press, p.66.

En matière de cybercriminalité, persistent encore certaines différences juridiques historiques dans les lois de procédures pénales nationales.[25] Néanmoins, les différences dans le contenu global du droit pénal dépend moins d´une « famille juridique » spécifique – du droit civil ou de la Common Law – que des ordres constitutionnels et socio-culturels actuels. Par exemple, l´accent mis sur des valeurs telles que la liberté d´expression et la vie privée, ou sur l´individu ou la communauté, peut avoir une influence significative sur la politique et les résultats de l´incrimination. Dans le contexte de la cybercriminalité, ceci peut aboutir à différents résultats juridiques dans des domaines tels que la règlementation relative au matériel obscène ;[26] l´équilibre entre la liberté d´expression et l´expression inacceptable ;[27] les niveaux d´accès aux contenus d´internet ;[28] les règles et les obligations imposées aux fournisseurs de services d´internet ;[29] et les garanties et les limitations relatives aux enquêtes intrusives des services répressifs.[30]

Outre les effets constitutionnels et socio-culturels, l´impact des simples coïncidences historiques sur les processus de rédaction des textes juridiques, l´impact des opinions des experts et des diverses évaluations des meilleures pratiques, ne devraient pas être sous-estimés. Il peut être beaucoup plus simple de tenir compte et de traiter les différences juridiques techniques qui découlent de ces effets et des héritages de procédures légales, que celles qui dérivent des ordres constitutionnels et socio-culturels.

Harmonisation des lois

Ces différences posent la question de savoir si les différences juridiques nationales dans les lois sur la cybercriminalité peuvent ou devraient être réduites, et si c´est le cas, dans quelle mesure. En d´autres termes, jusqu´à quel point l´harmonisation des lois sur la cybercriminalité est-elle importante ? Ceci peut se faire de différentes manières, y compris avec des initiatives régionales ou internationales, contraignantes et non contraignantes. La base de l´harmonisation peut être une simple approche nationale (avec les autres parties révisant leurs lois en ligne), ou, le plus souvent, des éléments juridiques communs identifiés dans la législation de plusieurs autres états, ou exprimés dans un instrument multilatéral – comme un traité ou des normes internationales non contraignantes. En effet, comme expliqué ci-dessous, l´un des objectifs du droit international est l´harmonisation des lois nationales.

Lors de la collecte des informations pour l´étude, des questions ont été posées aux pays concernant leur perception du degré d´harmonisation de la législation sur la cybercriminalité, les réussites et les limites de l´harmonisation, et les approches utilisées pour maintenir les traditions juridiques nationales durant le processus d´harmonisation.[31] De nombreux pays, en Asie et en Amérique notamment, signalèrent que bien que l´harmonisation soit importante, le processus était soumis à d´importantes limitations. Ceci incluait le « *conflit... avec des exigences constitutionnelles,* » l´exigence que l´harmonisation ne soit pas « *en conflit avec la loi fondamentale et la Sharia* », la nécessité d´une « *application contextuelle* » des normes harmonisées et l´existence d´une législation étatique et fédérale dans un pays.[32]

---

25 Pour ce qui concerne le caractère évolutif et hétérogène du droit procédural, voir Legeais, R., 2004. *Grands systèmes de droit contemporains*. Paris : Litec,p. 389.

26 Voir, par exemple, Segura-Serrano, A., 2006. Les régulations d´internet et le rôle du droit international. *dans* : Von Bogdandy, A., Wolfrum, R. (eds.) *Max Planck annuaire du droit des Nations Unies*, 10(2006) :191-272 ; Edick, D.A. 1998. Régulation de la pornographie sur iinternet aux États-Unis et au Royaume uni : une analyse comparative. *Boston College International & Comparative. Revue juridique*21(2) :437-460.

27 Voir le rapport du *Rapporteur spécial sur la promotion et la protection du droit à la liberté d´opinion et d´expression.* A/67/357, 7 septembre 2012.

28 *Ibid.*

29 Voir le rapport du *Rapporteur spécial sur la promotion et la protection du droit à la liberté d´opinion et d´expression.* A/HRC/17/27, 16 May 2011.

30 Par exemple, en ce qui concerne les enquêtes sur les actes d´appui au délit de terrorisme liés à l´informatique ces, voir ONUDC. 2012. *L´utilisation d´internet à des fins terroristes.* paras 35, 106, 110.

31 Questionnaire de l´étude sur la cybercriminalité Q16 et Q17.

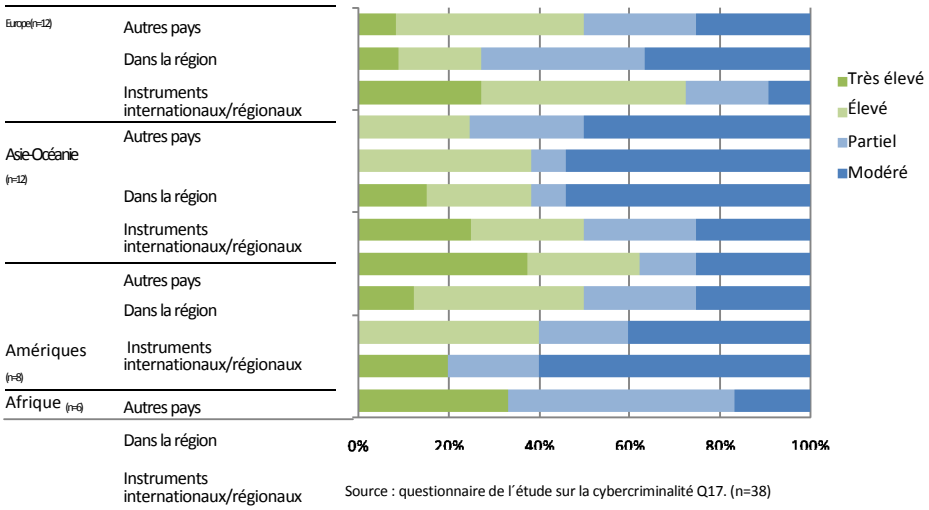
32 *Ibid.* Q16.

Les pays ont également signalé des réussites en matière d´harmonisation des législations sur la cybercriminalité. Ils ont, par exemple, déclaré que l´harmonisation faisait partie d´une « *approche intégrale qui incluait les règles matérielles et procédurales* », et que les traditions juridiques nationales pouvaient être maintenues en « *tenant compte de la spécificité de la société en termes de coutumes, de traditions et d´usages...* [et] *de la législation nationale préexistante* ».[33]

Le degré d´harmonisation des lois sur la cybercriminalité mentionné par les pays répondants varie significativement en fonction de la région et du fait que l´harmonisation soit évaluée par rapport à : (i) d´autres pays ; (ii) la région ou (iii) aux dispositions des instruments multilatéraux. La figure 3.3 montre qu´environ un tiers des pays considère que sa législation est totalement ou hautement harmonisée avec d´autres pays. Les pays restants considèrent que leur législation est partiellement ou « assez » harmonisée avec d´autres pays. La perception des niveaux d´harmonisation est plus élevée en Europe et en Amérique, qu´en Afrique, en Asie et en Océanie. Un pays d´Asie a, par exemple, directement commenté que « *la législation actuelle n´est pas harmonisée avec des pays qui sont importants... à des fins de coopération internationale* ».[34] D´autres pays ont fait référence à la situation globale. Un pays d´Europe a, par exemple, signalé que « *il existe, au niveau régional, un degré élevé d´harmonisation. Nous ignorons si c´est le cas au niveau global. Bien que des demandes de coopération judiciaire internationale nous aient été refusées en raison de l´absence de double incrimination, il semble qu´il existe des règles procédurales différentes…..liées à la coopération judiciaire internationale* ».[35]

Plusieurs pays ont mentionné l´utilité des instruments internationaux dans les processus d´harmonisation. Un pays a, par exemple, déclaré qu´il trouvait utiles les normes externes, comme celles comprises dans les instruments régionaux et internationaux, « *afin de les comparer aux dispositions de nos lois* ».[36] Un autre pays a signalé que les forums internationaux qui recherchaient des consensus sur les mesures juridiques et les stratégies internationales pour lutter contre la cybercriminalité, étaient importants car ils représentaient « *des opportunités pour partager des idées qui pouvaient être utilisées par les états membres comme des options pratiques ou législatives, utiles pour prévenir et réprimer la criminalité* ». Le même pays signalait que les processus d´harmonisation représentaient un processus à double sens, car « *dans certains cas... les idées ou les initiatives législatives locales ont été la source des éléments des normes internationales, et dans d´autres cas, les idées exprimées par d´autres états membres ont influencé la conception nationale de la cybercriminalité et ont influencé la législation nationale* »[37]

Figure 3.3 : degré d´harmonisation de la législation sur la cybercriminalité avec : (i) d´autres pays importants pour la coopération, (ii) la région (iii) les instruments multilatéraux



Source : questionnaire de l´étude sur la cybercriminalité Q17. (n=38)

33 *Ibid.*
34 Questionnaire de l'étude sur la cybercriminalité Q17.
35 *Ibid.*
36 Questionnaire de l'étude sur la cybercriminalité. Q16.
37 Questionnaire de l'étude sur la cybercriminalité. Q17.
38 Questionnaire de l'étude sur la cybercriminalité. Q16.

D´autres pays ont noté l´influence de la législation nationale existante. Par exemple, un pays d´Asie de l´est a déclaré qu´il avait « *étudié les législations étrangères...pour établir une législation nationale* ».[38] La figure 3.3 est assez peu concluante pour ce qui concerne l´impact des instruments internationaux sur l´harmonisation. La perception de niveaux élevés d´harmonisation de la législation nationale avec des instruments internationaux pour des pays d´Europe, par exemple, ne semble pas correspondre directement à des niveaux élevés d´harmonisation avec les pays de la région.

Les instruments internationaux pertinents en matière de cybercriminalité et leur influence sur la législation nationale sont examinés ultérieurement dans ce chapitre. Cependant, il est important d'examiner, tout d'abord, les raisons et les fondements de l´harmonisation de la législation sur la cybercriminalité.

Pourquoi harmoniser ?

Pour éviter l´impunité – en matière de cybercriminalité, comme pour tous les délits transnationaux, le principal avantage de l´harmonisation du droit pénal est éviter que les auteurs des cyberdélits ne puissent se soustraire aux poursuites la prévention. Comme le signalait un des pays qui a répondu au questionnaire de l´étude, « *la cybercriminalité est un problème global, et cela rend tous les pays importants pour nous, de diverses manières... nous pensons que cette coopération avec les pays en développement est importante car la cybercriminalité ne connait pas de frontières* ».[39] En effet, de tous les délits transnationaux, la criminalité présente probablement le risque le plus direct d´impunité.

Donc, si des actes préjudiciables impliquant l´internet sont, par exemple, incriminés par l´état A, mais non par l´état B, un délinquant se trouvant dans l´état B peut cibler ses victimes dans l´état A par le biais de l´internet. Dans ces cas, l´état A ne peut offrir à lui seul une protection efficace contre les effets de ces activités transnationales. Même si ses lois pénales lui permettent d´affirmer sa juridiction sur l´auteur de l´infraction de l´état B, il requiert toujours le consentement ou l´assistance de B – pour ce qui concerne la collecte des preuves ou l´extradition de l´auteur de l´infraction. Pour protéger les personnes relevant de sa juridiction, l´état B ne l´aidera probablement pas si la conduite en cause n´est pas incriminée dans son propre pays. Ce principe de double incrimination est essentiel pour plusieurs formes de coopération internationale. Il est inclus dans des traités d´extradition bilatéraux et multilatéraux ainsi que dans des lois nationales.[40]

La double incrimination joue également un rôle dans l´entraide judiciaire, comme, par exemple, dans les demandes relatives à l´interrogatoire des témoins ou à la collecte de preuves.[41] Bien que cette exigence ne soit pas incluse dans tous les accords d´entraide judiciaire entre les états, plusieurs instruments s´assurent que les mesures intrusives ou coercitives, telles que la perquisition, la saisie ou le gel des biens, soient soumises à la double incrimination.[42]

---

39 Questionnaire de l´étude sur la cybercriminalité Q17.

40 Voir, par exemple, l´Article 2(1) du Traité type d´extradition des Nations Unies, l´Article 2(1) de la Convention européenne sur l´extradition et l´Article 2 du Plan de Londres pour l´extradition entre pays du Commonwealth. Voir aussi Plachta, M., 1989. Le rôle de la double incrimination pour la coopération internationale en matière pénale. *dans* : Agell, A., Bomann, R., et Jareborg, N. (eds.) *Double incrimination, études sur le droit pénal international* Uppsala : Iustus Förlag, p.111, référence, entre autre, à, Shearer, I., 1971. *L´extradition dans le droit international.* Manchester, p. 137, et Bassiouni, M.C., 1974. *L´extradition internationale et l´ordre public mondial.* Dordrecht : Kluwer Academic Publishers, p.325.

41 Voir Capus, N., 2010. *Strafrecht und Souveränität : Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen.*
Bern : Nomos, p.406.

42 Voir, par exemple, l´Article 5(1) de la Convention sur l´entraide judiciaire du Conseil de l´Europe et l´Article 18(1)(f) de la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits de la criminalité du Conseil de l´Europe. Pour l´échange d´informations ou d´autres formes de coopération qui ne portent pas atteinte aux droits de la personne concernée, la double incrimination n´est pas exigée. Voir Vermeulen, G., De Bondt, W., Ryckman, C., 2012. *Reconsidérer la coopération internationale en matière pénale dans l´UE.* Antwerp : Maklu, p.133 ; et Klip, A., 2012. *Droit pénal européen.* Antwerp : Intersentia, p.345.

43 Plachta, M., 1989. Le rôle de la double incrimination pour la coopération internationale en matière pénale. *dans* : Agell, A., Bomann, R., Jareborg,
N. (eds.). *Double incrimination, études sur le droit pénal international* Uppsala : Iustus Förlag, pp.108-109.voir aussi : le rapport explicatif pour la Convention européenne relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits de la criminalité, qui spécifie dans la clarification de l´Art. 18(1)(f) que la double incrimination est requise par défaut pour les mesures d´enquête prévues par la Section 2, qui incluent (sans s´y limiter) les mesures d´enquête exigeant une action coercitive.

Le chapitre sept (coopération internationale) examine ce domaine de manière plus détaillée. Cependant, pour ce qui concerne l´harmonisation des lois pénales sur la cybercriminalité, un point important est que la double incrimination ne requiert pas que l´activité sous-jacente soit punie par le même type de dispositions pénales. Donc, si l´état C utilise un cyberdélit spécifique pour une conduite déterminée alors que l´état D utilise une infraction générale, les états C et D sont à même de s´engager dans une coopération internationale, si les éléments constitutifs essentiels de l´infraction sont comparables conformément au droit des deux états.[43] Comme le mentionne le chapitre sept, si les états arrivent à un certain niveau d´harmonisation entre leurs législations nationales (comme dans l´Union Européenne), le principe de la double incrimination pourrait être remplacé par la présomption par défaut de l´équivalence des lois.[44]

Pour permettre de collecter des preuves au niveau global – l´harmonisation du droit procédural est la seconde exigence indispensable pour une coopération internationale efficace. Dans l´exemple précédent, si l´état B ne dispose pas des pouvoirs procéduraux nécessaires pour la conservation rapide des données informatiques, l´état A ne pourra pas demander cette assistance par l´entremise de l´entraide judiciaire. En d´autres termes, un état requis peut seulement prêter son assistance sur son territoire, dans la mesure où il pourrait le faire pour une enquête nationale équivalente.[45] Comme pour le cas de la double incrimination, il n´est pas nécessaire que la forme juridique des pouvoirs procéduraux soit directement équivalente, pour autant que les mesures d´enquêtes puissent être mises en œuvre dans la pratique. Par exemple, la conservation rapide des données pourrait être légitimement exécutée par le biais d´une ordonnance dédiéeou d´un pouvoir général de perquisition et saisie.

Pour exprimer la « gravité » et réduire l´impunité – depuis une perspective de coopération internationale, l´harmonisation des peines prévues pour les délits pénaux n´est pas strictement requise pour les même motifs que dans le cas du droit pénal positif et des pouvoirs coercitifs du droit procédural pénal. La double incrimination ne concerne pas les sanctions respectives. Il existe néanmoins un lien spécial entre la coopération et le niveau de sanction. Les peines imposées pour un délit indiquent le niveau de gravité du délit. Au niveau international, la Convention sur la criminalité définit un « crime grave » comme une conduite constituant un délit « *puni par une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d´une peine plus lourde* ».[46] Étant donné l´important investissement que la coopération internationale exige aux états, plusieurs instruments d´extradition spécifient un seuil de gravité du délit en cause – généralement exprimé en faisant référence à la sanction possible dont ce délit pourrait être passible.[47]

44 Voir De Bondt, W., 2012. *La nécessité et la faisabilité de mesures stratégiques de l´UE*. Antwerp : Maklu, pp. 46-47.

45 Les instruments relatifs à l´entraide judicaire ne déclarent pas spécifiquement que les mesures qui n´existent pas dans l´état requis pourraient néanmoins être exécutées. Cependant, dans le cas des mesures coercitives la Décision d´instruction européenne déclare que des mesures alternatives peuvent et devront être utilisées si les mesures requises n´existent pas selon la loi de l´état requis. Voir Conseil de l´Europe. 2011. *Initiative en vue d´une Directive relative à la Décision d´instruction européenne en matière pénale*– Texte retenu comme approche générale, 18918/11, 21 décembre 2011, pp.19-20.

46 Convention sur la criminalité organisée, Art. 2. Le seuil des quatre ans est utilisé pour définir une catégorie générale de « crimes graves » auxquels s´applique la Convention (qui doivent avoir un caractère transnational et impliquer un groupe criminel organisé). Ce seuil n´est pas applicable aux infractions spécifiques établies par la Convention.

47 Schwaighofer, K., Ebensperger S., 2001. *Internationale Rechtshilfe in strafrechtlichen Angelegenheiten.* Vienna : WUV Universitätsverlag, p. 8.

48 Lagodny, O. 2012. *dans :* Schomburg, W., Lagodny, O., Gless, S., Hackner, T. (eds.) *Internationale Rechtshilfe in Strafsachen.* Munich : C.H.Beck, p. 90 § 3 IRG, at 23 ; Murschetz, V. 2007. *Auslieferung und Europäischer Haftbefehl.* Vienna/New York : Springer, p.124.

49 L´article 5(1)(b) de la Convention sur l´entraide judiciaire en matière pénale du Conseil de l´Europe prévoit que les parties contractantes peuvent exiger que ce soit un délit donnant lieu à l´extradition pour exécuter une commission rogatoire de perquisition ou de saisie des biens.

50 L´article 2(1) de la Convention sur l´extradition de l´Union européenne prévoit qu´un délit donne lieu à l´extradition s´il est passible d´une peine privative de liberté d´au moins un an en vertu de la loi de l´état requérant et d´au moins six mois en vertu de la loi de l´état requis. Il faut toutefois signaler que la Convention a largement fait place au mandat d´arrêt européen (Hackner, T., 2012. *dans* :, Schomburg, W., Lagodny, O., Gless, S., Hackner, T. (eds.) *Internationale Rechtshilfe in Strafsachen.* Munich : C.H.Beck. p.1174, III A, au 3, et pp.1178 1179, III A 1, au 9).

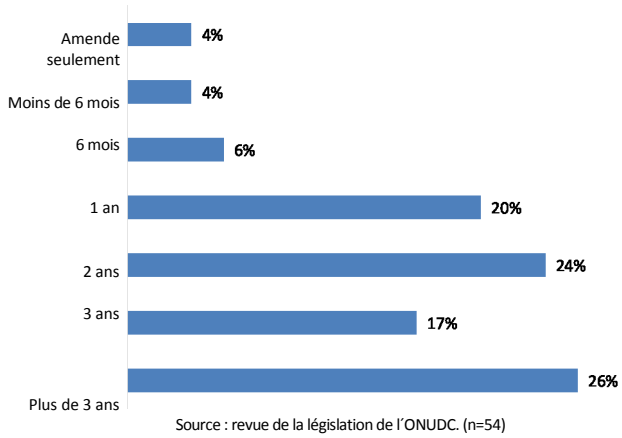
51 Les dispositions sur l´extradition de la Convention sur la cybercriminalité du Conseil de l´Europe, par exemple, s´appliquent aux délits pénaux établis conformément aux Articles 2 à11 de la Convention, s´ils sont sanctionnés conformément au droit des deux parties par une peine privative de liberté dont le maximum ne doit pas être inférieur à un an ou d´une peine plus sévère .

52 Convention sur la criminalité organisée, Arts. 2 et 16.

Le seuil de gravité représente également un mécanisme important pour la protection du principe de proportionnalité et des droits de l´accusé.[48] Des exigences similaires peuvent aussi s´appliquer à des accords d´entraide judiciaire.[49] Le seuil typique des sanctions des instruments de coopération internationale va de six moiss[50] à un an,[51] ou à quatre ans.[52] Durant la collecte des informations pour l´étude, on a demandé aux pays quelles étaient les peines imposées à divers actes de cybercriminalité, tes que des actes contre la confidentialité, l´intégrité et la disponibilité des systèmes et des données informatiques, des actes liés à l´informatique motivés par des gains financiers ou personnels, et des cyberdélits spécifiques.[53]

Les figures 3.4 et 3.5 montrent la répartition des sanctions imposées à des actes d'« accès illégal à des données ou des systèmes informatiques », et pour le même délit – lorsque les dispositions juridiques nationales[54] requièrent le « contournement des systèmes de sécurité » ou une « intention délictueuse ».

Figure 3.4 : peine maximale de prison pour l´accès illégal à des données ou des systèmes informatiques



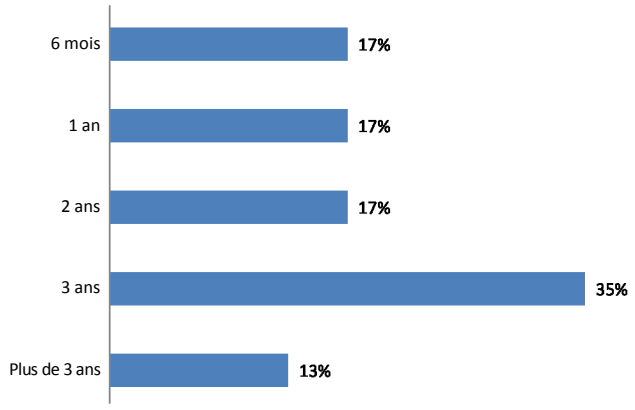
Source : revue de la législation de l´ONUDC. (n=54)

Il semble que plusieurs pays prévoient pour les deux délits des peines maximales de moins d´un an. Étant donné qu´un an représente le seuil le plus commun à des fins d´extradition (et celui qui est utilisé par des instruments tels que la Convention sur la cybercriminalité du Conseil de l´Europe, et la Convention de la Ligue des états arabes), dans certains pays la coopération internationale peut s´avérer difficile[5] [5]pour ce qui concerne ces délits.

Les peines typiques sont bien inférieures au seuil des quatre ans pour les « crimes graves » utilisé par la Convention sur la criminalité organisée.

Toutefois, pour ce qui concerne la situation des peines imposées dans la pratique, ces résultats doivent être interprétés avec précaution.

Figure 3.5 : peine maximale de prison pour l´accès illégal à des données ou des systèmes informatiques (avec intention délictueuse ou détournement des systèmes de sécurité)



Source : revue de la législation de l´ONUDC (n=23)

53 Auestionnaire de l´étude sur la cybercriminalité Q25-39. Les informations sur les peines sont recueillies par le Secrétariat à partir de sources additionnelles qui incluent la révision de la source primaire du droit.

54 Analyse limitée aux pays dans lesquels la peine maximale est prévue par l´article de loi spécifique (les pays où la sanction peut seulement être déterminée par l´analyse des dispositions générales du code pénal ne sont pas inclus).

55 Il faut noter que les pays répondants ont signalé que les actes de cybercriminalité sont largement considérés comme répondant aux normes de gravités et constituant des délits qui donnent lieu à l´extradition. Tous les pays répondants d´Europe et d´Amérique, et 90 % des pays d´Afrique, d´Asie et d´Océanie signalent que les actes de cybercriminalité constituent en général des délits qui donnent lieu à l´extradition (questionnaire de l´étude sur la cybercriminalité Q194). La divergence provient probablement du fait qu´il est rare que les auteurs des infractions soient accusés et que l´extradition soit sollicitée pour un acte « d´accès illégal » indépendamment d´autres accusations.

Il est difficile d´évaluer le niveau des sanctions imposées dans la pratique en se référant seulement aux dispositions spécifiques du droit pénal. Elles peuvent être affectées par des règles générales d´application des peines, des circonstances aggravantes ou atténuantes, ou par des directives spécifiques de qualification ou de détermination de la peine. Toutefois, ce panorama sert à souligner les difficultés générales pour ce qui concerne la définition de la portée de la coopération internationale et de l´accord commun sur la gravité des délits de cybercriminalité. L´acte de « simple accès illégal » pourrait constituer une infraction mineure mais d´autre part, l´accès illégal représente le point de départ de plusieurs cyberdélits graves, et peuvent inclure l´entrée intentionnelle non autorisée dans des systèmes informatiques– comme ceux qui sont utilisés dans des infrastructures nationales critiques. Les références aux sanctions pénales maximales possibles pour déterminer les niveaux de coopération ne caractérisent pas nécessairement la loi elle-même. Les approches alternatives comme l´établissement d´une liste de délits spécifiques auxquels s´appliquent les dispositions relatives à la coopération internationale (sans la nécessité d´un seuil pénal), sont affectées par les limitations d´une portée restreinte. En général, l´harmonisation, entre les pays, des peines pour les principaux cyberdélits spécifiques – y compris les niveaux communs de peines basés sur la gravité – pourrait vraisemblablement faciliter la coopération internationale et l´élimination de l´impunité pour les auteurs des infractions.

Synthèse

La situation actuelle de la législation sur la cybercriminalité est dynamique– avec des réformes juridiques en cours et la reconnaissance croissante de la nécessité d´une riposte juridique dans de multiples domaines : pénal, civil et administratif. Presque 60 % des pays répondants ont mentionné une législation sur la cybercriminalité nouvelle ou prévue dans leurs réponses au questionnaire de l´étude.[56] Même si le droit général traditionnel peut être appliqué à des affaires de cybercriminalité dans une certaine mesure, le caractère intangible des concepts tels que les « données informatiques » requiert également l´introduction de concepts, de définitions et d´infractions spécifiques – si des intérêts juridiques comme l´intégrité des systèmes informatiques doivent être protégés.

Alors qu´il existe un consensus sur les domaines d´intervention juridique pour la prévention et la lutte contre la cybercriminalité, les niveaux d´harmonisation de la législation avec les pays considérés importants pour la coopération, avec les régions et les instruments multilatéraux, sont perçus comme étant extrêmement variables. Ceci inclut le domaine des sanctions des cyberdélits, où l´examen d´un seul délit fondamental – l´accès illégal – montrent des divergences qui peuvent affecter une coopération internationale fructueuse. L´harmonisation est nécessaire pour, entre autres, éliminer l´impunité et pour la collecte globale de preuves. Les voies d´harmonisation incluent l´utilisation d´instruments régionaux et internationaux contraignants et non contraignants. Comme indiqué jusqu´ici dans cette étude, plusieurs de ces instruments existent. La section suivante de ce chapitre examine ce point de manière plus détaillée.

3.3 Aperçu des instruments régionaux et internationaux

Principaux résultats :

- des progrès significatifs concernant la promulgation d´instruments régionaux et internationaux visant à lutter contre la cybercriminalité sont survenus lors de la dernière décennie. Ceci inclut des instruments contraignants et non contraignants ;
- on peut mentionner cinq catégories, avec des instruments développés dans le cadre de, ou inspirés par : (i) le Conseil de l´Europe ou l´Union Européenne, (ii) la Communauté des états indépendants ou l´Organisation de coopération de Shanghai, (iii) les organisations intergouvernementales africaines, (iv) la Ligue des états arabes et (v) les Nations Unies ;
- un significatif enrichissement mutuel existe entre tous les instruments, notamment en ce qui concerne les concepts et les approches développés dans la Convention sur la cybercriminalité du Conseil de l´Europe ;
- une analyse des articles de 19 instruments multilatéraux pertinents en matière de cybercriminalité révèle des dispositions essentielles communes, mais également des divergences significatives dans des importants domaines abordés.

56 Questionnaire de l´étude sur la cybercriminalité Q14.

Des progrès significatifs concernant la promulgation d´instruments régionaux et internationaux visant à lutter contre la cybercriminalité sont survenus lors de la dernière décennie. La création, le statut juridique, la portée géographique, l´objectif principal et les mécanismes de ces instruments varient significativement.

On peut mentionner cinq catégories d´instruments– (i) des instruments développés dans le cadre de, ou inspirés par, le Conseil de l´Europe ou l´Union Européenne ; (ii) des instruments développés dans le cadre de la Communauté des états indépendants ou l´Organisation de coopération de Shanghai ; (iii) des instruments développés dans le cadre des organisations africaines ; (iv) des instruments développés par la Ligue des états arabes et (v) des instruments développés sous l´égide ou en association avec les entités des Nations Unies.

Ces catégories ne sont pas absolues et il existe un significatif enrichissement mutuel entre les instruments. Les concepts basiques développés dans la Convention sur la cybercriminalité du Conseil de l´Europe, par exemple, sont également inclus dans plusieurs autres instruments.[57] Les entités des Nations Unies comme la CEA et l´UIT, sont aussi impliquées dans le développement d´instruments dans le cadre de l´Afrique comme le projet de convention de l´Union Africaine et la loi type de la SADC.

Au sein d´une catégorie, les instruments peuvent avoir une relation directe.

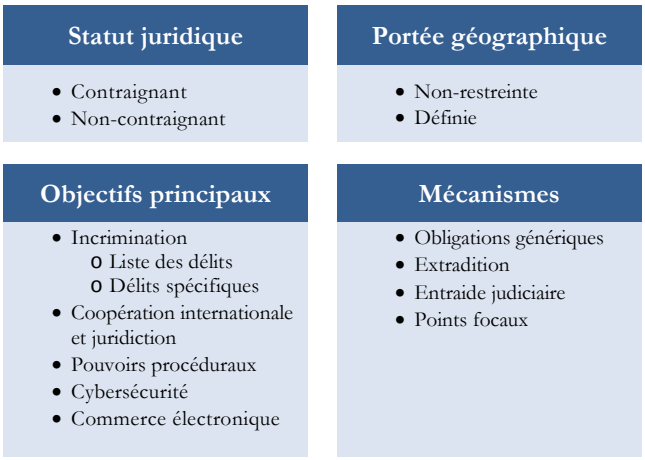
Contraignants	Non-contraignants
▪ Convention sur la cybercriminalité du Conseil de l´Europe (2001) et son protocole additionnel (2003) ▪ Convention sur la protection des enfants contre l´exploitation et l´abus sexuel du Conseil de l´Europe (2007) ▪ La législation de l´UE sur le commerce électronique (2000/31/EC), sur la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (2001/413/JHA), les données personnelles (2002/58/EC telle qu´amendée), les attaques contre les systèmes d´informations (2005/222/JHA et la proposition COM(2010) 517 final), sur la pornographie infantile(2011/92/EU)	▪ Les lois types du Commonwealth sur les délits informatiques(2002) et les preuves électroniques(2002)
▪ Accord de coopération des états indépendants (CEI) de la lutte contre les infractions dans le domaine informatique (2001) ▪ Accord de coopération dans le domaine de la sécurité de l´information au niveau international de l´organisation de coopération de Shanghai (2009)	
▪ Projet de directive sur la lutte contre la cybercriminalité de la Communauté économique des états de l´Afrique de l´ouest (CEDEAO) (2009) ▪ Projet de convention de l´Union africaine sur l´établissement d´un cadre juridique propice à la cybersécurité en Afrique (2012)	▪ Projet de cadre juridique de la CAE pour une cyberlégislation (2008) ▪ Projet de loi type sur la cyber sécurité (2011) du marché commun de l´Afrique orientale et australe (COMESA) ▪ Loi type sur la cybercriminalité et les délits informatiques (2012) de la communauté de développement de l´Afrique australe (CDAA)
▪ Convention sur la lutte contre les infractions liées aux technologies de l´information (2010) de la Ligue des états arabes	▪ Loi type de la Ligue des états arabes sur la lutte contre les infractions liées aux technologies de l´information (2004)
▪Protocole facultatif de la Convention des Nations Unies relative aux droits de l´enfant, concernant la vente d´enfants, la prostitution et la pornographie infantiles(2000)	▪ Textes législatifs types sur la cybercriminalité, les preuves et les délits électroniques(2010) de l´Union internationale des télécommunications (UIT)/la communauté des Caraïbes (CARICOM)/l´union caraïbe des télécommunications (CTU) ▪ Loi type sur la cybercriminalité (2011) de l´Union internationale des télécommunications (UIT)/Secrétariat de la communauté du Pacifique

57 L´analyse dans l´annexe trois de cette étude (« dispositions des instruments régionaux et internationaux ») démontre que plusieurs concepts fondamentaux inclus dans la Convention sur la cybercriminalité du Conseil de l´Europe – comme l´accès illégal à un système informatique, l´interception illégale de données informatiques, l´interférence illégale avec des systèmes ou des données informatiques, la conservation rapide des données informatiques, et la collecte de données informatiques en temps réel – sont également inclus dans d´autres instruments ultérieurs.

La loi type du Commonwealth, par exemple, s´inspire étroitement de la Convention sur la cybercriminalité du Conseil de l´Europe. Le projet de Convention de l´union africaine incorpore des termes du projet de directive de la CEDEAO, et l´accord de la Communauté des états indépendants et l´accord de l´organisation de coopération de Shanghai ont en commun des concepts relatifs à la sécurité informatique. Le schéma ci-dessous illustre les similarités et les différences entre les instruments et les catégories, et se concentre sur le « statut juridique », la « portée géographique », les « principaux objectifs », et les « mécanismes ».

Statut juridique

La première nuance à établir est savoir si un instrument est juridiquement contraignant. De nombreux instruments – notamment les conventions du Conseil de l´Europe, les instruments de l´Union européenne, l´accord de la Communauté des états indépendants, l´accord de l´organisation de coopération de Shanghai et la Convention de la Ligue des états arabes – sont des accords exprès entre les états, destinés à créer des obligations juridiques.[58] S´il est approuvé par l´assemblée de l´Union africaine, le projet de convention de l´Union africaine serait également ouvert à la signature, la ratification ou l´adhésion et entrerait en vigueur sous la forme d´un instrument contraignant.[59]



D´autres instruments – comme la loi type du Commonwealth, le projet de loi type du COMESA, la loi type de la Ligue des états arabes et les textes législatifs types de l´UIT/CARICOM/CTU– ne sont pas destinés à créer des obligations juridiques pour les états. Ils sont conçus pour servir d´inspiration ou de « modèles » pour le développement des dispositions législatives nationales. Toutefois, les instruments non contraignants peuvent avoir une influence significative au niveau régional ou global lorsque plusieurs états choisissent d´harmoniser leurs lois nationales avec les approches types.[60] De plus, même si les pays n´ont pas adhéré ou ratifié un instrument contraignant, ils peuvent s´inspirer d´un instrument contraignant pour établir les dispositions législatives nationales – et la portée de cet instrument sera donc plus étendue que le nombre de pays qui l´ont signé, ratifié ou qui y ont adhéré.[61]

Portée géographique

La portée géographique des instruments contraignants est typiquement déterminée par

58 Les conventions internationales, générales ou particulières, qui établissent des règles expressément reconnues, sont comprises parmi les sources de droit international applicables par la Cour internationale de justice, conformément à l´Article 38 du Statut de la Cour internationale de justice. L´Article 2 de la Convention de Vienne sur le droit des traités définit un traité comme un accord international conclu par écrit entre états et régi par le droit international, qu´il soit consigné dans un instrument unique ou dans deux ou plusieurs instruments connexes, et quelle que soit sa dénomination particulière ».

59 Le projet de convention de l´Union africaine. Partie IV, Section 2. En septembre 2012, la 4eme session ordinaire de la conférence des ministres de l´Union africaine en charge des communications et des technologies de l´information (CITMC-4) demanda que le projet de convention de l´Union africaine soit soumis aux fins d´adoption par la commission de l´Union africaine conformément aux règles de procédures de l´Union africaine. Voir l´Union africaine. 2012. *Déclaration deKhartoum* AU/CITMC-4/MIN/Decl.(IV)Rev 2, 6 septembre 2012.

60 De nombreux états du Commonwealth, par exemple, ont utilisé des dispositions de la loi type du Commonwealth isolément ou conjointement avec la convention sur la cybercriminalité du Conseil de l´Europe. Voir Conseil de l´Europe. 2012. *Etats du Commonwealth : utilisation de la convention de Budapest et de la loi type du Commonwealth. Contribution du Conseil de l´Europe au groupe de travail sur la cybercriminalité du Commonwealth.*

61 Le Conseil de l´Europe, par exemple, signale que, outre les pays qui ont ratifié, signé ou ont été invités à adhérer à la Convention européenne sur la cybercriminalité, il collabore avec au moins 55 pays en matière de coopération technique sur la base de la Convention. Voir Seger, A., 2012. 10 ans après la convention de Budapest sur la cybercriminalité : Leçons apprises ou le web est un web.

la nature et le contexte de l´organisation sous l´égide de laquelle l´instrument est développé. Par exemple, l´objectif de la convention de la Ligue des états arabes est de « renforcer et d´améliorer la coopération entre les états arabes ».[62] De même, l´accord de la Communauté des états indépendants définit « les Parties » comme les « *états membres de la Communauté des états indépendants,* »[63] et le projet de convention de l´Union africaine est destiné à être ouvert aux « *états membres de l´Union africaine* ».[64]

L´adhésion à un instrument ne coïncide pas forcément avec l´adhésion organisationnelle. Il est possible que les membres de l´organisation ne soient pas tous signataires de l´accord original,[65] et – si l´accord est soumis à ratification, adoption ou approbation [66] – que les signataires n´aient pas tous déposé ces instruments.[67] Certains instruments sont ouverts à la signature en dehors des membres de l´organisation sous l´égide de laquelle l´instrument a été développé. Par exemple, la Convention sur la cybercriminalité du Conseil de l´Europe a été ouverte à la signature des états membres du Conseil de l´Europe et « *des états non-membres qui ont participé à son élaboration* ».[68]

Les états fondateurs deviennent les états titulaires qui contrôlent l´entrée des nouveaux états candidats à l´adhésion ce ce, souvent, conformément aux règles établies dans l´accord de traité initial.[69] Un traité peut être « ouvert » et tout état peut y adhérer en exprimant son intention d´être lié par les termes du traité existants ; « semi-ouvert » et l´adhésion peut être approuvée par une majorité des états signataires et/ou contractants ; ou « fermé » et l´adhésion requiert l´approbation unanime des états signataires et/ou contractants.[70]

Pour ce qui concerne la Convention sur la cybercriminalité du Conseil de l´Europe, le Comité des ministres du Conseil de l´Europe, après avoir consulté et obtenu le consentement unanime des états contractants à la Convention, peut « *inviter tout état non membre du Conseil et n´ayant pas participé à son élaboration à adhérer à la Convention* ».[71] De même, l´Accord de la Communauté des états indépendants est « *ouvert à l´adhésion de tout état disposé à être lié par ses dispositions, sous réserve de l´accord de toutes les Parties* ».[72] L´Accord de l´organisation de coopération de Shanghai stipule également être « *ouvert à l´adhésion de tout état qui partage les objectifs et les principes de l´Accord* ».[73] Les instruments développés sous l´égide des Nations Unies ont généralement la plus vaste portée géographique.

---

62 Convention de la Ligue des états arabes, Art. 1.

63 Accord de la Communauté des états indépendants. Préambule.

64 Projet de convention de l´Union africaine. Partie IV, Section 2, Art. IV-2.

65 Les Comores, Djibouti, Le Liban et la Somalie, membres de la Ligue des états arabes n´ont pas signé la Convention de la Ligue des états arabes. Andorre, Monaco, la Fédération russe et San Marino, membres du Conseil de l´Europe n´ont pas signé la Convention sur la cybercriminalité du Conseil de l´Europe.

66 L´article 14 de la Convention de Vienne sur le droit des traités stipule que « *le consentement d´un état à être lié par un traité s´exprime par la ratification : (a) lorsque le traité prévoit que le consentement s´exprime par la ratification ; (b) lorsqu´il est par ailleurs établi que les états et les organisations ayant participé à la négociation étaient convenus que la ratification serait requise ; (c) lorsque le représentant de cet état a signé le traité sous réserve de ratification ; ou (d) lorsque l´intention de cet état de signer le traité sous réserve de ratification ressort des pleins pouvoirs de son représentant ou a été exprimée au cours de la négociation* ». La Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes stipulent expressément que l´accord est soumis à la ratification, l´adoption ou l´approbation. L´Accord de la Communauté des états indépendants et l´Accord de l´organisation de coopération de Shanghai envisagent le dépôt de notification déclarant que les parties ont accompli les procédures internes requises pour l´entrée en vigueur de l´accord. Le projet de Convention de l´Union africaine prévoit la signature, la ratification ou l´adhésion. Pour une révision générale du droit international des traités voir Shaw, M.N., 2007. *Droit international.* 6ieme ed. Cambridge : Cambridge University Press.

67 La république tchèque, la Grèce, l´Irlande, le Liechtenstein, le Luxembourg, la Pologne, la Suède et la Turquie, signataires de la Convention de la cybercriminalité du Conseil de l´Europe n´ont pas encore déposé leurs instruments de ratification, d´adoption ou d´approbation.

68 Art. 36(1) de la Convention sur la cybercriminalité du Conseil de l´Europe. Le Canada, le Japon, l´Afrique du sud et les États-Unis d´Amérique, qui sont des états non membres, ont signé la Convention sur la cybercriminalité du Conseil de l´Europe.

69 L´article 15 de la Convention de Vienne sur le droit des traités stipule que « *le consentement d´un état à être lié par un traité s´exprime par l´adhésion : (a) lorsque le traité prévoit que le consentement peut être exprimé par cet état ou cette organisation par voie d´adhésion ; (b) lorsqu´il est par ailleurs établi que les états et les organisations, ou selon le cas les organisations ayant participé à la négociation étaient convenus que ce consentement pourrait être exprimé par voie d´adhésion ou (c) lorsque toutes les parties sont convenues ultérieurement que ce consentement pourrait être exprimé par cet état par voie d´adhésion* ».

70 Malone, L.A., 2008. *Droit international.* New York : Aspen.

71 Art. 37(1) de la Convention sur la cybercriminalité du Conseil de l´Europe. Les propositions d´amendement de la procédure suivie conformément à l´Art. 37(1) ont été réalisées par le Comité (T-CY) de la Convention sur la cybercriminalité du Conseil de l´Europe et le Comité européen pour les problèmes criminels (CDPC). Les deux propositions sont actuellement examinées par le groupe de rapporteurs sur la coopération juridique du Conseil de l´Europe (GR-J). Voir le Comité de la Convention sur la cybercriminalité du Conseil de l´Europe2012. *Critères et procédures pour l´adhésion à la Convention de Budapest sur la cybercriminalité– mise à jour* T-CY (2012)12 E. 28 mai 2012.

72 Accord de la Communauté des états indépendants, Art. 17.
73 Accord de l´organisation de coopération de Shanghai, Art. 12.

La Convention relative aux droits de l´enfants et son protocole facultatif concernant la vente d´enfants, la prostitution et la pornographie infantiles, par exemple, est ouverte à « *l´adhésion de toutétat* ».[74]

Les états fondateurs ont l´avantage de pouvoir influencer le contenu des traités, mais peuvent affronter certains coûts lors du processus de négociation et d´élaboration du traité. L´adhésion, à une étape ultérieure, à un traité évite ces coûts mais offre des possibilités limitées de renégociation du contenu et des obligations du traité. Dans la mesure où les traités sont souvent conclus par des pays ayant des préférences similaires, ils peuvent ne pas être acceptables pour les états qui n´ont pas participé aux négociations, même lorsque le traité est ouvert à l´adhésion.[75]

Généralement, les traités multilatéraux reconnaissent cela par le biais des réserves exprimées au moment de la signature, la ratification ou l´adhésion.[76] La Convention sur la cybercriminalité du Conseil de l´Europe permet de spécifier les réserves concernant des articles déterminés, même si d´autres réserves ne peuvent être exprimées.[77] La Convention de la Ligue des états arabes permet d´exprimer des réserves déterminées et interdit seulement les réserves « *impliquant une violation des textes de la Convention ou une déviation de ses objectifs* ».[78] L´Accord de la Communauté des états indépendants reste silencieux au sujet des réserves,[79] et au moins un pays a exprimé une réserve.[80] S´il est adopté sous sa forme actuelle, le projet de Convention de l´Union africaine permettra des réserves concernant « *une ou plusieurs dispositions spécifiques* » et qui « *ne sont pas incompatibles avec les objectifs et les finalités de la Convention* ».[81]

Au niveau global, 82 pays ont signé et/ou ratifié des instruments contraignants sur la cybercriminalité.[82] Certains pays ont adhéré à plusieurs de ces instruments. Malgré la possibilité de participation au-delà du contexte initial d´organisation ou d´élaboration, la Figure 3.6[83] montre que – jusqu´à présent –aucun instrument (hormis le OP-CRC-SC des Nations Unies[84]) n´a reçu les signatures ou les ratifications/adhésions correspondant à une portée géographique globale. La Convention sur la cybercriminalité du Conseil de l´Europe a réuni le plus grand nombre de signatures ou de ratifications/adhésions (48 pays) y compris cinq états non membres du Conseil de l´Europe.[85] D´autres instruments ont une portée géographique plus restreinte – la Convention de la Ligue des états arabes (18 pays ou territoires), l´Accord de la Communauté des états indépendants

74 La Convention des Nations Unies sur les droits des enfants, Art. 48 ; et le OP-CRC-SC des Nations Unies, Art. 13. « État » a un sens élargi dans ce contenu et n´est pas limité aux états membres des Nations Unies. Le Saint-Siège, par exemple, est un état non membre des Nations Unies et a signé et ratifié la Convention sur les droits des enfants et le OP-CRC-SC voir :http ://treaties.un.org/Pages/Treaties.aspx?id=4&subid=A&lang=en

7 5Parisi, F., Fon, V., 2009. La formation des traités internationaux. *dans : l´économie des activités législatives*. Oxford : Oxford Scholarship en ligne .

76 La section 2 de la Convention de Vienne sur le droit des traités prévoit la formulation de réserves, l´acceptation et les objections aux réserves, les effets juridiques des réserves et des objections aux réserves, le retrait des réserves et des objections aux réserves, et les procédures relatives aux réserves. En général, les réserves incompatibles avec les « objectifs et les finalités » du traité ne sont pas permises.

77 Art. 42 de la Convention sur la cybercriminalité du Conseil de l´Europe

78 Art. 6 du chapitre V de la Convention de la Ligue des états arabes.

79 conformément à l´Article 24 de la Convention Vienne sur le droit des traités, la mesure applicable par défaut est qu´un état peut formuler des réserves à moins que cela ne soit spécifiquement interdit par le traité, ou lorsque le traité ne prévoit que des réserves déterminées ou lorsque la réserve est incompatible avec les objectifs et les finalités du traité.

80 La réserve de l´ Ukraine au point 5 de l´agenda de la réunion du Conseil des chefs d´états membres de la Communauté des états indépendants, intitulée « *Accord de coopération en matière de lutte contre les infractions dans le domaine informatique* » 1 juin 2001.

81 Projet de convention de l´Union africaine, Partie IV, Section 2, Art. IV-3.

82 Signature ou ratification de : la Convention sur la cybercriminalité du Conseil de l´Europe, la Convention de la Ligue des états arabes, l´Accord de la Communauté des états indépendants et l´Accord de l´organisation de coopération de Shanghai

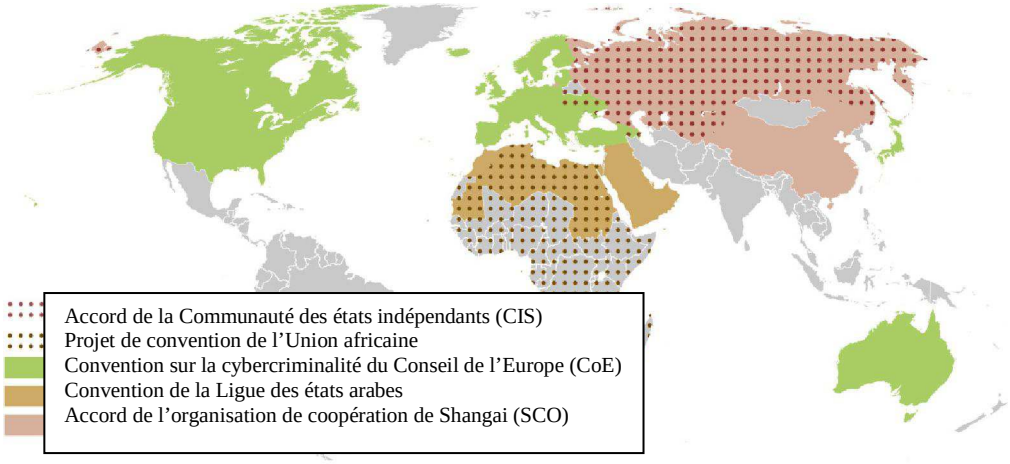
83 La carte montre tous les pays qui ont signé, ratifié ou adhéré à l´Accord de la Communauté des états indépendants (CIS), à la Convention sur la cybercriminalité du Conseil de l´Europe(CoE), à la Convention de la Ligue des états arabes (LAS) et à l´Accord de l´organisation de coopération de Shanghai (SCO). A titre de référence, la carte montre également les états membres de l´Union africaine avec le total des adhésions possibles au projet de convention de l´Union africaine, en cas d´être ouvert à la signature, la ratification ou l´adhésion.

84 176 pays ou territoires ont signé, ratifié ou adhéré au OP-CRC-SC des Nations Unies.

85 De plus, huit autres pays (l´Argentine, le Chili, le Costa Rica, la République dominicaine, le Mexique, Panama, les Philippines, et le Sénégal) ont été invités à adhérer à la Convention du Conseil de l´Europe conformément aux dispositions de l´Article 37. L´adhésion de ces pays à la Convention élargirait significativement sa portée géographique.

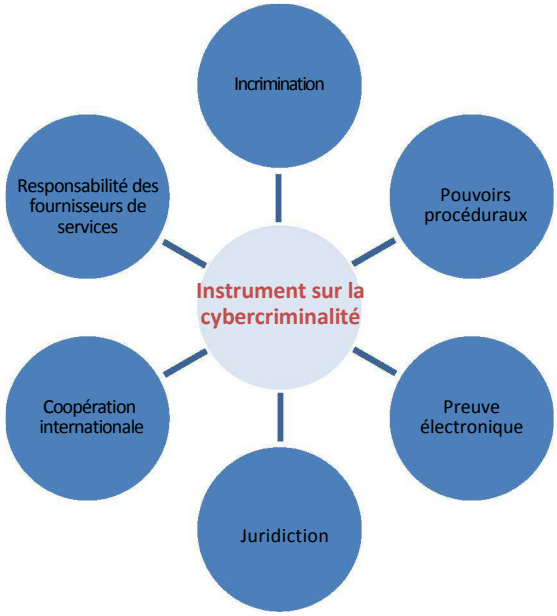
(10 pays) et l´Accord de l´organisation de coopération de Shanghai (6 pays). S´il était signé ou ratifié par tous les états membres de l´Union africaine, le projet de convention de l´Union africaine pourrait inclure jusqu´à 54 pays ou territoires.

Figure 3.6 : instruments régionaux et internationaux



Il existe donc au niveau global un certain degré de fragmentation en matière d´adhésion aux instruments régionaux et internationaux sur la cybercriminalité. Les patrons régionaux sont particulièrement clairs à cet égard. Certains pays du monde bénéficient de l´adhésion à des instruments contraignants contre la cybercriminalité – et à plus d´un instrument dans le cas de certains pays – alors que d´autres régions ne participent à aucun cadre contraignant.

Figure 3.7 : principal objectif des instruments contre la cybercriminalité



Objectif principal

Outre les différences existantes en matière de portée géographique, les instruments régionaux et internationaux présentent également – comme c´est le cas pour la législation nationale – des différences quant à l´objectif principal. Plusieurs de ces différences proviennent de la finalité sous-jacente de l´instrument. Certains instruments, comme la Convention sur la cybercriminalité du Conseil de l´Europe, la loi type du Commonwealth, la Convention de la Ligue des états arabes et l´Accord de la Communauté des états indépendants, visent spécifiquement à fournir un cadre de justice pénale pour lutter contre la cybercriminalité. D´autres tels que l´Accord de l´organisation de coopération de Shanghai et le projet de convention de l´Union africaine, ont une approche plus large, dans laquelle la cybercriminalité est juste un élément. L´Accord de l´organisation de coopération de Shanghai, par exemple, traite la coopération en matière de cybercriminalité dans le contexte de la

sécurité informatique internationale – qui inclut la guerre de l´information, le terrorisme et les menaces contre les infrastructures d´informations nationales et mondiales. [86]

Le projet de convention de l´Union africaine a une approche basée sur la cybersécurité qui inclut l´organisation des transactions électroniques, la protection des données personnelles, la promotion de la cybersécurité, la gouvernance électronique et la lutte contre la cybercriminalité .[87]

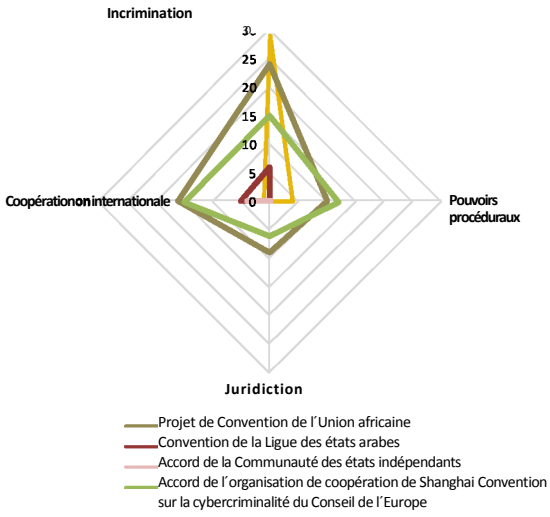
Ces différences affectent de manière significative la manière dont la cybercriminalité est « encadrée » par les ripostes juridiques régionales ou internationales. Par exemple, du fait d´être axé sur la sécurité de l´information internationale, l´Accord de l´organisation de coopération de Shanghai ne définit pas d´actes spécifiques de cybercriminalité devant être incriminés. De même – peut être en raison d´une vision de la cybercriminalité dans son ensemble plutôt que dans le cadre de la justice pénale en particulier – le projet de Convention de l´Union africaine ne cherche pas à établir les mécanismes de la coopération internationale en matière de cybercriminalité.

Du point de vue de la justice pénale et de la prévention de la criminalité, six domaines clés pourraient bénéficier d´une orientation contraignante ou non contraignante au niveau régional ou international : (i) l´incrimination ; (ii) les pouvoirs procéduraux des services répressifs ; (iii) les procédures relatives aux preuves électroniques ; (iv) la juridiction de l´état dans des affaires pénales de cybercriminalité ; (v) la coopération internationale dans des affaires pénales de cybercriminalitéet (vi) la responsabilité des fournisseurs de services.

Le contenu des instruments régionaux et internationaux – et bien sur des lois nationales – dans chacun de ces domaines, peut être analysé à trois niveaux : (1) l´existence de dispositions pertinentes dans chaque domaine ; (2) l´inclusion des dispositions dans chaque domaine et (3) le contenu des dispositions. Cette section traite les niveaux un et deux. Le niveau trois est examiné au chapitre quatre (incrimination) et au chapitre cinq (application des lois et enquêtes).

Pour ce qui concerne l´existence des dispositions pertinentes, les instruments contraignants et non contraignants internationaux et régionaux identifiés, traitent les six domaines à des degrés divers. Les dispositions relatives à l´incrimination, aux pouvoirs procéduraux, à la juridiction et à la coopération internationale sont généralement incluses dans de nombreux instruments contraignants. Par contre, les dispositions relatives aux preuves électroniques et à la responsabilité des fournisseurs de services sont généralement incluses dans des instruments non contraignants – comme la loi type du Commonwealth, le projet de loi type du COMESA et les textes législatifs types de l´UIT/CARICOM/CTU.[88]

Figure 3.8 : Structure des instruments régionaux et internationaux



86 L´article 2 de l´Accord de l´organisation de coopération Shanghai inclut la cybercriminalité dans les « principales menaces » pour la sécurité de l´information internationale. La cybercriminalité est défini à l´Annexe 1 de l´Accord comme « *l´utilisation des ressources d´information et (ou) l´impact sur ces ressources dans le cyberespace à des fins illicites* ».

87 Dans le projet de convention de l´Union africaine, la cybercriminalité est traitée dans la Partie trois : « *Promouvoir la cybersécurité et lutter contre la cybercriminalité* ». Les parties une et deux traitent les « *transactions électroniques* » et « *la protection des données personnelles* », respectivement.

88 Voir les tableaux « preuves électroniques » et « responsabilité des fournisseurs de services » à l´annexe trois de cette étude

89 Voir le projet de directive de la CEDEAO, Art. 34, et le projet de convention de l´Union africaine, Art. I(24).

Seuls les projets de directive de la CEDEAO (prévu comme un instrument contraignant) et de convention de l´Union africaine contiennent des dispositions pertinentes relatives aux preuves électroniques.[89] De même, seule la législation de l´Union européenne traite la question de la responsabilité des fournisseurs de services et la responsabilité au niveau régional ou international.[90]

Dans le domaine de l´incrimination, des pouvoirs procéduraux des services répressifs et de la coopération internationale, les instruments présentent également toute une gamme d´approches. La figure 3.8 montre la répartition relative du nombre d´articles de cinq instruments contraignants régionaux ou internationaux qui traitent chaque domaine. Les instruments comme la Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes couvrent les quatre domaines. Le projet de convention de l´Union africaine est principalement axé sur l´incrimination et inclut quelques pouvoirs procéduraux. L´Accord de la Communauté des états indépendants inclut un nombre limité d´articles sur la coopération internationale et l´incrimination. Au-delà de ces quatre domaines, l´Accord de l´organisation de Shanghai contient seulement des articles relatifs à la coopération internationale.

L´inclusion des dispositions pertinentes dans les instruments varie aussi de manière significative. L´Annexe trois de l´étude contient une analyse complète sur l´inclusion des dispositions dans chaque domaine clé, par instrument. L´analyse montre la diversité du panel de conduites incriminées par les instruments, dans l´étendue des pouvoirs procéduraux des services répressifs et dans les approches en matière de compétence et de coopération internationale. L´Annexe trois montre aussi que – bien qu´il existe des différences significatives – plusieurs instruments partagent certaines dispositions « essentielles ». Celles-ci incluent notamment : l´incrimination des actes contre la confidentialité, l´intégrité et la disponibilité des données ou des systèmes informatiques ; les pouvoirs procéduraux qui incluent des ordonnances de perquisition et de saisie des données informatiques, la collecte des données informatiques en temps réel et la conservation des données ainsi que les obligations générales de coopérer avec les enquêtes sur des affaires pénales de cybercriminalité. Le tableau ci-dessous synthétise les principaux résultats de **l´analyse de l´Annexe trois.**

Incrimination	• La plupart des instruments contiennent une longue liste d´infractions. D´autres se concentrent seulement su un domaine thématique d´infractions limité, comme les instruments concernant la pornographie infantile et l protection des enfants. Les actes contre la confidentialité, l´intégrité et la disponibilité des données u des systèmes informatique sont les plus couramment incriminés, suivis par les actes liés à la falsification ou à la fraude informatique, e la production, la distribution ou la possession de pornographie infantile liées à l´informatique. • Outre les actes identifiés au Chapitre premier de l´étude dans la section « Description de la cybercriminalité » certains instruments incriminent aussi un vaste panel d´actes, y compris les actes contre le sécurité, la moralit ou l´ordre public liés à l´informatique. • Certains instruments stipulent que commettre les délits conventionnels au moyen d´un système informatiqu serait une circonstance aggravante.
Pouvoirs procéduraux	• La perquisition, la saisie, les ordonnances relatives aux données informatiques stockées et aux informations des abonnés, la collecte des données informatiques en temps réels et la conservation rapide des données informatiques sont les pouvoirs procéduraux les plus communs. • L´accès transfrontalier aux données informatiques est envisagé par trois instruments.
Preuves électroniques	• Les quelques instruments (généralement non contraignants) qui incluent les preuves électroniques, couvrent les questions de la recevabilité des preuves électroniques, du fardeau de prouver l´authenticité, la règle de la meilleure preuve, la présomption d´intégrité et les normes de conservation.

Juridiction	• Presque tous les instruments considèrent le principe territorial et le principe de nationalité (lorsque la double incrimination existe) comme des bases pour la juridiction. • D´autres bases de juridiction, qui ne sont pas incluses dans tous les instruments, comprennent des actes dirigés contre des données ou des systèmes informatiques qui se trouvent sur le territoire, et le principe de l´intérêt de l´état. • Deux instruments fournissent une orientation pour établir le lieu où un cyberdélit a été commis.
Coopération internationale	• Les instruments tendent à traiter minutieusement la coopération internationale – en prévoyant des mécanismes relatifs à l´entraide judiciaire et à l´extradition – ou en se concentrant, de façon plus limitée, sur les principes généraux de la coopération. •De nombreux instruments envisagent l´établissement de points de contact ou de réseaux 24/7.
Fournisseurs de services	• Le nombre limité d´instruments qui traitent la responsabilité des fournisseurs de services couvre les obligations de contrôle, la fourniture volontaire de renseignements, les notifications de retrait, et la responsabilité des fournisseurs en matière d´accès, de mise en cache, d´hébergement et d´hyperliens.

90 Voir, par exemple, la directive de l´UE sur le commerce électronique, Arts. 12 à 15.

Mécanismes

Les mécanismes de coopération internationale sont particulièrement importants pour les instruments contraignants régionaux ou internationaux – car ils fournissent une obligation juridique internationale claire ou des pouvoirs en matière de coopération entre les états parties. Outre les obligations générales de coopérer,[91] certains instruments – notamment l´Accord de la Communauté des états indépendants, la Convention du Conseil de l´Europe, et la Convention de la Ligue des états arabes – établissent des mécanismes concrets de coopération. Dans le cas de ces trois accords, l´instrument lui-même peut servir de fondement pour les demandes d´assistance entre les états parties.[92] Ainsi l´instrument peut également, sans préjudice des conditions prévues par la législation nationale ou tout autre traité d´entraide judiciaire applicable, établir les raisons pour lesquelles un état partie peut refuser de prêter son assistance.[93] L´Accord de la Communauté des états indépendants définit les types d´assistance qui peuvent être sollicités en termes généraux.[94] La Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes, outre les obligations générales de s´entraider le plus possible dans le cadre des enquêtes et des procédures, incluent aussi des formes spécifiques d´assistance – comme la conservation rapide des données informatiques stockées, la divulgation rapide de données conservées, l´accès aux données informatiques stockées, la collecte de données en temps réel et l´interception de données relatives au contenu.[95]

Enfin, certains instruments établissent des registres des autorités compétentes pour ce qui concerne les demandes d´entraide judiciaire et d´extradition,[96] les procédures d´assistance rapide[97] et les points focaux pour accéder aux voies de communication fonctionnant 24 heures sur 24.[98]

91 Voir, par exemple, l´Article 23 de la Convention sur la cybercriminalité du Conseil de l´Europe qui stipule que « *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.* ».

92 Voir, par exemple, l´Article 27 de la Convention sur la cybercriminalité du Conseil de l´Europe qui stipule que « *En l »absence de traité d'entraide ou d »arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s »appliquent »* ; l´Article 34 de la Convention de la Ligue des états arabes qui

stipule que « *les dispositions des paragraphes 2 à 9 du présent article s »appliquent en l »absence de traité ou de convention de coopération ou d´entraide reposant sur la législation applicable entre les états parties requérants et les états parties requis* » ; et l´Article 6 de l´Accord de la Communauté des états indépendants qui stipule que « *la coopération dans le cadre du présent Accord sera basé sur les demandes d´assistance soumises par les autorités compétentes des parties* ».

93 Voir la Convention sur la cybercriminalité du Conseil de l´Europe, Art. 27(4), et la Convention de la ligue des états arabes, Art. 35, qui stipulent que l´assistance peut être refusée si la demande se rapporte à une infraction politique, ou si l´état requis considère que la demande porte atteinte à la souveraineté de l´état, à la sécurité, à l »ordre public ou à tout autre intérêt fondamental.

94 L´article 5 de l´Accord de la Communauté des états indépendants inclut, par exemple, l´échange d´informations sur des délits liés à l´informatique qui sont en cours de préparation ou qui ont été commis ; l´exécution des demandes relatives aux enquêtes et aux procédures en conformité avec les instruments internationaux d´entraide judiciaire ; ainsi que la planification et la mise en œuvre d »opérations et d´activités coordonnées, afin de prévenir, de détecter, de supprimer, de découvrir et d´enquêter sur des délits liés à l´informatique.

95 Voir la Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 29, 30, 31, 33 et 34 ; et la Convention de la ligue des états arabes, Arts. 37-39, 41 et 42.

96 Voir la Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 24(7) et 27(2) ; l´Accord de la Communauté des états indépendants, Art.4 ; et la Convention de la ligue des états arabes, Arts. 31(7) et 34(2).

97 Voir la Convention sur la cybercriminalité du Conseil de l´Europe, Art. 31(3) ; l´Accord de la Communauté des états indépendants, Art. 6(2) ; et la Convention de la ligue des états arabes, Art. 34(8).

3.4 Mise en œuvre des instruments multilatéraux au niveau national

Principaux résultats :

- outre la mise en œuvre et l´adhésion formelle, les instruments multilatéraux sur la cybercriminalité ont influencé indirectement les législations nationales, en servant de modèle à des états non parties ou en influençant la législation des états parties dans d´autres pays ;
- l´adhésion à un instrument multilatéral sur la cybercriminalité cause la perception d´une suffisance accrue du droit procédural et pénal national, et cela indique que les dispositions multilatérales actuelles dans ces domaines sont généralement considérées comme efficaces ;
- la fragmentation au niveau international et la diversité des lois nationales contre la cybercriminalité, peuvent être en corrélation avec l´existence de multiples instruments ayant une portée géographique et des thèmes différents.

La manière dont les instruments régionaux ou internationaux sont mis en œuvre dans la législation nationale, ainsi que l´efficacité de l´application et la mise en vigueur de nouvelles règles, peuvent être des facteurs décisifs pour la réussite, ou l´absence de réussite, de l´harmonisation.[99] Les états peuvent interpréter ou mettre en œuvre les dispositions des instruments internationaux de différentes manières, accentuant ainsi les divergences entre les pays. Ceci en soi n´est pas un problème : les pays ne mettront pas toujours en œuvre les cadres internationaux exactement de la même façon, en raison des limitations et des différentes traditions juridiques qui existent au niveau national .[100] Toutefois, le but de la mise en œuvre est de fournir un certain niveau de conformité des législations nationales avec les cadres internationaux.

Mise en œuvre verticale (directe)

La mise en œuvre « directe » d´un traité multilatéral est postérieure à la signature, la ratification ou l´adhésion au traité. Pour que la plupart des règles internationales deviennent opératives, elles doivent être appliquées par des individus ou des fonctionnaires de l´état dans le système juridique national. Les états peuvent y parvenir avec « l´incorporation verticale » des règles internationales dans la législation nationale (souvent associée avec les systèmes « monistes ») ou avec une « incorporation législative »

Mise en œuvre de la Décision de l´UE sur les attaques contre les systèmes informatiques

Un rapport sur la mise en œuvre de la décision-cadre de l´UE sur les attaques contre les systèmes informatiques (2005) révèle des différences significatives relatives à l´utilisation de l´option de ne pas incriminer « les infractions mineures»..... Par exemple les états membres :

- incriminent l´accès illégal seulement s´il y a une intention de commettre un acte d´espionnage de données ;
- incriminent l´accès illégal seulement dans les cas où les données font ensuite l´objet d´une utilisation abusive ou sont endommagées ;
- rendent obligatoire la condition de mise en danger des données consultées pour qu´il y ait responsabilité pénale.

Le rapport sur la mise en œuvre signalait qu´en général, « *une telle divergence d´interprétation et l´application de l´option de ne pas incriminer certains actes représentent un risque sérieux pour rapprocher les règles en matière pénale des états membres dans le domaine des attaques contre les systèmes informatiques*».....

Source : Commission européenne. 2008. COM (2008) 448 final.

98 Voir la Convention sur la cybercriminalité du Conseil de l´Europe, Art. 35 et la Convention de la Ligue des états arabes, Art. 43.

99 Miquelon-Weismann, M. F., 2005. La Convention sur la cybercriminalité : une mise en œuvre harmonisée du droit pénal international :quelles perspectives pour les règles de forme? *John Marshall Journal of Computer & Information Law*, 23(2) :329-61.

100 Voir Klip, A., Nelken, D., 2002. Changer les cultures juridiques. *Dans :* Likosky, M. (ed.) *procédures juridiques transnationales* Londres : Butterworths ; Graziadei, M., 2009. Les transplantations juridiques et les frontières des connaissances juridiques. *Questions théoriques sur le droit*, 10(2) : 723-743.

(dans des systèmes « dualistes »), selon lesquels les règles internationales deviennent applicables dans le système juridique national uniquement si la législation nationale pertinente est adoptée.[101]

L´incorporation de dispositions d´instruments sur la cybercriminalité dans la législation nationale impliquera souvent la modification de lois telles que le code pénal et le code de procédure pénale, afin d´introduire de nouvelles infractions spécifiques ou de modifier les existantes.

Le résultat dans la législation nationale peut être significativement différent d´un état partie à l´autre. Par exemple, un effet spécifique sur le système juridique national d´un état, découlant de la mise en œuvre d´un instrument international pourrait ne jamais avoir lieu dans le cas d´un autre état.[102] Une évaluation relative à la mise en œuvre de la Décision de l´UE sur les attaques contre les systèmes informatiques[103] illustre bien les difficultés inhérentes à l´harmonisation de la législation sur la cybercriminalité – même dans le contexte d´un cadre contraignant et de pays et de pays habitués à mettre en œuvre des lois supranationales.[104] Comme l´illustre l´encadré, l´évaluation de la mise en œuvre montrait d´importantes divergences dans les dispositions juridiques nationales destinées à mettre en œuvre la Décision. L´évaluation souligne également un autre point – à savoir que l´évaluation de la mise en œuvre d´un instrument est un processus technique et difficile, qui requiert du temps, des ressources et des informations exhaustives sur les dispositions législatives et leur application dans la pratique.[105] Évaluer la mise en œuvre des différents instruments régionaux et internationaux sur la cybercriminalité mentionnés dans ce chapitre va au-delà de la portée et du mandat de cette étude.

Mise en œuvre du projet de directive de la CEDEAO

En 2008, un pays d´Afrique de l´ouest a adopté une loi concernent les régulations prévues au niveau régional par la CEDEAO en matière de cybercriminalité. Les amendements spécifiques incluaient :

- la création d´infractions informatiques spécifiques dans le domaine de la protection pénale des systèmes informatiques et des données électroniques, du contenu illégal, des fraudes informatiques, des services d´assistance technique et de la publicité numérique ;
- la mise à jour de la législation concernant les infractions existantes afin de les adapter au nouvel environnement TI/télécommunications (dans le domaine de la protection pénale contre le vol, les dommages physiques causés aux biens, etc.) ;
- des modifications des lois sur la procédure pénale pour mettre en œuvre des instruments spécifiques sur les TI;
- La création de nouvelles directives sur la coopération en matière de cybercriminalité avec les états de la CEDEAO, le Conseil de l´Europe, et la coopération entre l´état et le réseau CEDEAO /Conseil de l´Europe /G8.

Source : Mouhamadou, L.O. 2011. Cybercriminalité, libertés civiles et vie privée dans la Communauté économique des états de l´Afrique de l´ouest. 21ème Conférence annuelle sur l´informatique, la liberté et la vie privée 2011.

Toutefois, l´analyse des réponses du questionnaire de l´étude montre que l´adhésion à un instrument multilatéral correspond à la perception accrue que le droit pénal et procédural national en matière de cybercriminalité est suffisant. La figure 3.9 démontre que les pays répondants qui ne sont pas parties à un instrument multilatéral contre la cybercriminalité déclarent plus fréquemment que le droit procédural national et l´incrimination de la cybercriminalité « sont insuffisants ».[106]

101 Cassese, A., 2005.*Droit international.* Oxford : Oxford University Press, p.220-221.

102 Klip, A., 2006. Intégration européenne et harmonisation et droit pénal. *dans :* Curtin, D.M. et al. Intégration européenne et droit : Quatre contributions sur l´interaction entre l´intégration européenne et le droit national et européen pour célébrer le 25ieme anniversaire de la faculté de droit de l´université Maastricht. Pour la discussion générale, voir Legrand, P., 1997. L´impossibilité des transplantations juridiques, *journal de droit comparé et de droit européen Maastricht*, (4) :111-124.

103 Commission européenne. 2008. *Rapport de la Commission au Conseil basé sur l´Article 12 de la Décision cadre du Conseil du 24 février 2005 sur les attaques contre les systèmes*. COM (2008) 448 final, Bruxelles, 14 juillet 2008. Il faut signaler que l´analyse de la mise en œuvre a été réalisée pour seulement 20 des 27 états membres de l´Union Européenne Union, et était basée sur l´analyse formelle de l´information fournie par les états membres.

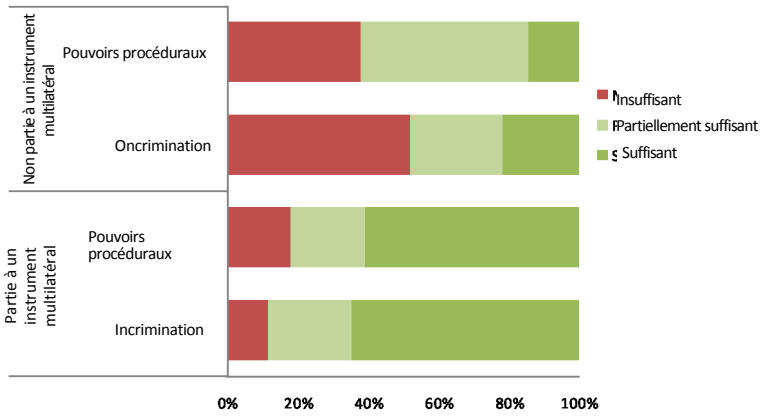
104 Calderoni, F., 2010. Le cade juridique européen sur la cybercriminalité : les efforts réalisés pour une mise en œuvre efficace. *Crime, droit et changement social*, 54(5) :339-357.

105 Le mécanisme d´évaluation de la mise en œuvre de la Convention des Nations Unies contre la corruption, par exemple, exige des termes de références détaillés pour le processus d´évaluation, ainsi que des directives pour le secrétariat et les experts gouvernementaux lors des évaluations de pays. Voir http ://www.unodc.org/documents/treaties/UNCAC/Publications/ReviewMechanism-BasicDocuments/Mechanism_for_the_Review_of_Implementation_-_Basic_Documents_-_E.pdf

106 Questionnaire de l´étude sur la cybercriminalité Q19. La figure 3.9 est calculée pour les instruments suivants signés ou ratifiés : la Convention sur la cybercriminalité du Conseil de l´Europe, la Convention de la Ligue des états arabes, l´Accord de la Communauté des états indépendants et l´Accord de l´organisation de coopération de Shanghai.

Alors qu´une relation entre la « suffisance » de la législation et « l´adhésion à l´instrument » peut être démontrée, les réponses à l´étude ne révèlent pas un patron clair entre « l´harmonisation perçue » et « l´adhésion à l´instrument ». Comme mentionné précédemment, alors que, par exemple, les pays d´Europe perçoivent des niveaux élevés d´harmonisation avec les instruments multilatéraux, ceci ne concorde pas toujours avec la perception de niveaux élevés d´harmonisation des législations nationales au sein de la région.[107]

Figure 3.9 : impact des instruments multilatéraux sur la perception d´une législation suffisante



Source : questionnaire de l´étude sur la cybercriminalitéQ19. (n=42)

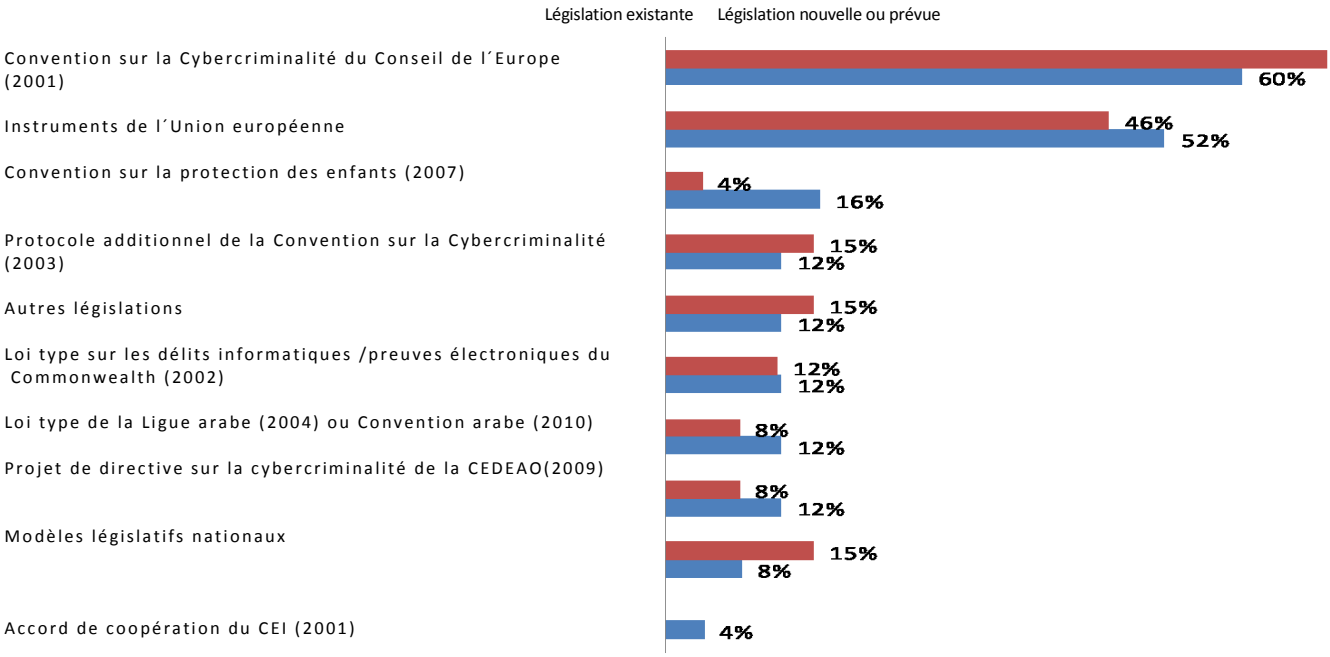
De même, les calculs basés sur les deux groupes répondants ci-dessus (« instrument » et « aucun instrument ») ne révèlent pas de différences significatives sur la perception des niveaux d´harmonisation avec d´autres pays ou au sein des régions respectives.[108] Néanmoins, les instruments multilatéraux sont généralement destinés à jouer un rôle dans l´harmonisation et il est possible que les réponses au questionnaire reflètent également des différences concernant la perception de ce qui constitue « l´harmonisation ». À cet égard, de nombreux pays ont signalé des expériences positives de mises en œuvre d´instruments multilatéraux. Pour ce qui concerne les harmonisations réussies, plusieurs pays répondants ont signalé des expériences positives d´incorporation à leur législation nationale de dispositions d´instruments tels que la Convention du Conseil de l´Europe sur la cybercriminalité.[109]

Influence indirecte

Au-delà de l´adhésion et de la mise en œuvre formelles d´instruments, des instruments multilatéraux sur la cybercriminalité ont aussi influencé indirectement les lois nationales, par le biais de leur utilisation comme modèles dans le cas des états non parties, ou par le biais de l´influence de la législation des états parties sur d´autres pays. Les pays peuvent utiliser plus d´un instrument pour élaborer la législation nationale et de nombreux pays ont déclaré que cela avait été le cas.[110] Un pays de l´Afrique de l´ouest, par exemple, avait utilisé la loi type du Commonwealth, la Convention sur la cybercriminalité du Conseil de l´Europe et le projet de directive de la CEDEAO. Un autre pays d´Asie de l´ouest a déclaré avoir utilisé la loi type de la Ligue des états arabes et les dispositions législatives nationales d´autres pays de la région.[111] De plus, comme mentionné précédemment, il existe un significatif enrichissement entre les textes des instruments multilatéraux. Par exemple, la loi type du Commonwealth et la Décision de l´UE sur les attaques contre les systèmes informatiques s´inspirent largement de la Convention sur la cybercriminalité du Conseil de l´Europe.

107 Voir ci-dessus la Section 3.2 Divergence et harmonisation des lois, harmonisation des lois.
108 Questionnaire de l´étude sur la cybercriminalité Q17.
109 Questionnaire de l´étude sur la cybercriminalité Q16.
110 Questionnaire de l´étude sur la cybercriminalité Q12 et Q14.
111 *Ibid.*

Figure 3.10 : instruments transnationaux utilisés pour élaborer ou développer la législation nationale sur la cybercriminalité, prévue ou existante



Source : questionnaire de l´étude sur la cybercriminalité Q12 et Q14. (n=26,25 ; r=51, 50)

La complexité de la mise en œuvre directe des instruments, leur influence indirecte et la combinaison des deux facteurs sont reflétées par les résultats globaux du questionnaire de l´étude. Lors de la collecte des informations pour l´étude, on demanda aux pays quels étaient les instruments régionaux ou internationaux qui avaient été utilisés pour élaborer ou développer les lois nouvelles, prévues ou existantes.[112] Un faible nombre de pays répondit à la question.[113] La figure 3.10 montre cependant que la Convention du Conseil de l´Europe, son protocole et les instruments fortement inspirés par la Convention du Conseil de l´Europe, comme les instruments de l´Union européenne, étaient les plus utilisés pour développer les législations sur la cybercriminalité. Enfin, les instruments multilatéraux issus d´autres catégories régionales ou internationales [114] – comme les instruments africains et de la Ligue des états arabes – ou d´autres législations nationales, étaient utilisés dans environ la moitié des pays.

Il faut signaler que cette évaluation est basée sur les réponses des pays et non pas sur une révision du contenu des lois nationales.[115] Ceci est cependant approprié car, en général, il est pratiquement impossible d´identifier – seulement en analysant les dispositions législatives – exactement les instruments utilisés lors de l´élaboration d´une législation. Il est uniquement possible de retrouver les influences lorsque l´approche de l´incrimination d´un délit particulier, suggérée par un cadre international spécifique, montre des différences qui la distinguent de tous les autres instruments.

112 *Ibid.*
113 La répartition régionale était la suivante : en ce qui concerne la législation existante : Europe 13 ; Asie et Océanie 7 ; Amériques 5 ; Afrique 5 ; en ce qui concerne la législation nouvelle ou prévue : Europe 7 ; Asie & Océanie 10 ; Amériques 5 ; Afrique 6.
114 Voir la sSection 3.3 aperçu des instruments régionaux et internationaux.
115 Il faut signaler que dans les chapitres quatre (incrimination) et cinq (application des lois et enquêtes) de cette étude, certains résultats présentés se basent sur l´analyse de la source primaire des législations.
116 Accord de la Communauté des états indépendants, Art. 3(1)(a) : l´accès illégal aux données informatiques protégées par la loi, quand ces actes causent la destruction, le verrouillage, la modification ou la reproduction de l´information ou la perturbation du fonctionnement de l´ordinateur, du système informatique ou des réseaux associés.

Par exemple, l´Accord de la Communauté des états indépendants [116] comprend des éléments additionnels relatifs à l´accès illégal (effets sur les données) et incrimine la distribution de virus informatiques de manière spécifique. On peut trouver les dispositions afférentes à cette approche en analysant le contenu des dispositions juridiques de plusieurs pays d´Europe de l´est et de l´Asie de l´ouest.[117]

En général, la possibilité de réussite de l´harmonisation et de la mise en œuvre du droit international dans la législation nationale est déterminée, en grande partie, par la mesure dans laquelle les pays sont à même de transposer les normes internationales dans les systèmes nationaux. Ceci est nécessaire, non seulement du point de vue juridique, mais également dans le contexte socio-politique où il existe un haut degré d´appui et d´engagement pour réaliser les réformes législatives nécessaires. C´est généralement le cas quand les pays sont à même de maintenir leurs traditions juridiques tout en respectant les obligations internationales qu´ils ont choisies d´assumer.

Un pays répondant d´Asie de l´ouest, par exemple, soulignait la nécessité de tenir compte de la « *société en termes de coutumes et de traditions* ».[118] Un pays d´Afrique de l´ouest et un pays d´Amérique signalaient également la bonne pratique de recourir aux « *consultations des intervenants* » pour s´assurer de maintenir les traditions juridiques nationales. Dans d´autres cas, les pays peuvent ne pas encore percevoir le besoin de renforcer la législation sur la cybercriminalité. Un pays d´Afrique australe, par exemple, signalait qu´étant donné que « *le développement de l´infrastructure des TIC était faible, la législation sur la cybercriminalité n´était pas considérée comme un besoin urgent* ».[119]

Toutefois, l´utilisation d´instruments contraignants et non contraignants régionaux et internationaux, offre un potentiel significatif pour tendre vers une meilleure harmonisation des lois nationales – et à long terme, renforcer la coopération internationale face à un problème mondial. Les chapitres quatre (incrimination), cinq (application des lois et enquêtes) et huit (prévention) examinent les convergences et les divergences dans ces domaines particuliers

117 Voir le chapitre quatre (incrimination).
118 Questionnaire de l´étude sur la cybercriminalitéQ16.
119 *Ibid*

CHAPITRE QUATRE : INCRIMINATION

Ce chapitre présente une analyse comparative des délits de cybercriminalité prévus par les lois nationales et internationales. Il démontre un certain consensus de base sur la nécessité d´incriminer certains actes de cybercriminalité. Cependant, un examen plus détaillé des éléments des délits montre des divergences entre les pays et les instruments multilatéraux sur la cybercriminalité. Le chapitre démontre également un effet « d´épée et de bouclier » des lois internationales sur les droits de l´homme en matière d´incrimination de la cybercriminalité.

4.1 Aperçu de l´incrimination

PRINCIPAUX RÉSULTATS :

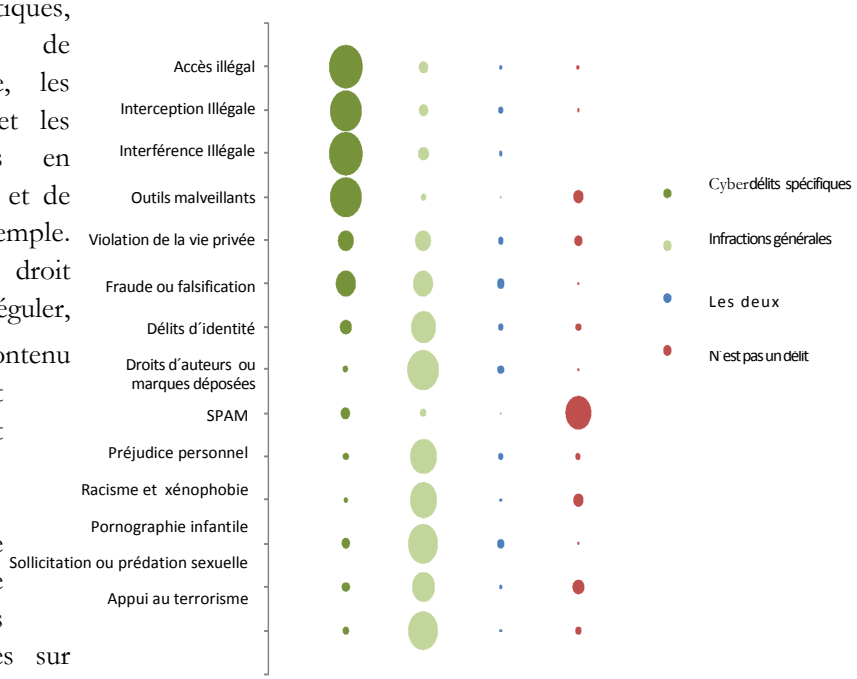
- les pays qui ont répondu au questionnaire ont décrit une incrimination généralisée de ces 14 actes, à l´exception des délits de SPAM et, dans une certaine mesure, des délits relatifs à l´usage abusif des outils informatiques, au racisme et à la xénophobie, et à la sollicitation ou à la prédation sexuelle des enfants en ligne ;
- ceci reflète un certain consensus de base sur les conduites coupables en matière de cybercriminalité ;
- les principaux actes de cybercriminalité contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques sont incriminés dans plusieurs pays comme des cyberdélits spécifiques ;
- les délits liés à l´informatique, tels que la violation de la vie privée, la falsification ou la fraude et les délits concernant l´identité, sont le plus souvent incriminés comme des infractions générales ;
- 80 % des pays d´Europe signalent que l´incrimination des actes de cybercriminalité n´est pas suffisante ;
- dans d´autres régions du monde, 60 % des pays signalent que l´incrimination des actes de cybercriminalité est insuffisante.

L´objectif de ce chapitre est de présenter une analyse comparative des délits de cybercriminalité inclus dans la législation nationale. La compréhension des approches d´incrimination utilisées et les différences entre les lois pénales nationales en matière de cybercriminalité sont importantes pour trois raisons. Tout d´abord, comme le mentionne le chapitre trois (cadres et législation), les lacunes en matière d´incrimination dans les pays peuvent favoriser l´impunité et éventuellement affecter d´autres pays au niveau global. Ensuite, les différences relatives à l´incrimination entraînent des difficultés pour une coopération internationale efficace dans des affaires pénales de cybercriminalité – notamment pour ce qui concerne le principe de double incrimination. Enfin, une analyse comparative des délits de cybercriminalité permet d´explorer les bonnes pratiques que les pays peuvent utiliser pour développer des lois nationales, en conformité avec les normes internationales émergentes dans ce domaine. Après un aperçu général de l´incrimination de la cybercriminalité, le chapitre examine les manières spécifiques par le biais desquelles les états structurent les infractions de cybercriminalité dans les lois nationales. Le chapitre conclut avec une discussion sur l´impact des lois internationales sur les droits de l´homme en matière d´incrimination de la cybercriminalité.

Cyberdélits spécifiques et infractions générales

Les actes individuels de cybercriminalité – tels que ceux identifiés au premier chapitre (connectivité et cybercriminalité) – peuvent être traités par les états de nombreuses façons. Certains actes peuvent ne pas être considérés comme des délits pénaux par les lois nationales. Si les actes sont des délits pénaux, ils peuvent être considérés comme des infractions générales (loi non informatique) ou des cyberdélits spécifiques. D´autres actes peuvent ne pas être des délits pénaux mais être punis par des sanctions administratives ou faire l´objet de recours civils. De nombreux pays répondants ont déclaré que les sanctions administratives étaient utilisées pour des actes qui n´étaient pas considérés comme des délits pénaux, et cela incluait les infractions concernant les droits d´auteurs et les marques déposées, l´envoi ou le contrôle de l´envoi de spam, les actes portant atteinte à la vie privée, et la production, la distribution ou la possession d´outils informatiques malveillants.[1] Ce chapitre n´examine pas l´utilisation de sanctions administratives ou de recours civils, mais se concentre sur l´incrimination. Le chapitre commence avec un aperçu de l´étendue de l´incrimination des différents actes de cybercriminalité, puis se focalise sur le contenu des dispositions nationales.

La figure 4.1 fournit une vision générale de l´étendue de l´incrimination des 14 catégories d´actes de cybercriminalité signalés par plus de 60 pays dans les réponses du questionnaire de .l´étude. Les réponses montraient l´incrimination généralisée de ces 14 actes, à l´exception des délits de SPAM et dans une certaine mesure des délits relatifs à l´usage abusif des outils informatiques, au racisme et à la xénophobie, et à la sollicitation ou à la prédation sexuelle des enfants en ligne.[2] Ceci reflète un certain consensus de base sur les conduites coupables en matière de cybercriminalité. Comme le mentionne le premier chapitre (connectivité et cybercriminalité), les pays signalent peu de délits additionnels, non mentionnés dans le questionnaire. Ils concernent principalement les contenus informatiques, l´incrimination de matériel obscène, les paris en ligne, et les marchés illicites en ligne, de drogues et de personnes par exemple. L´utilisation du droit pénal pour réguler, notamment, le contenu informatique et d´internet, est traité postérieurement dans ce chapitre dans le contexte de l´impact des lois internationales sur les droits de l´homme en matière d´incrimination.



Source : questionnaire de l´étude sur la cybercriminalité . Q25-38. (n=61)

Figure 4.1 : approches nationales de l´incrimination des actes de cybercriminalité

1 Questionnaire de l´étude sur la cybercriminalité Q25-39.
2 *Ibid.*

La figure 4.1 montre également un patron clair d´utilisation de lois informatiques spécifiques pour les principaux cyberdélits qui impliquent des actes contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques.

Les infractions informatiques spécifiques sont moins communément utilisées pour d´autres actes de cybercriminalité, comme les actes motivés par un gain financier ou personnel, qui causent un préjudice personnel ou liés au contenu informatique. Par contre, les infractions pénales générales sont importantes pour les dernières catégories mentionnées. Certains pays ont déclaré avoir utilisé des infractions générales pour incriminer les principaux cyberdélits, tel que l´accès illégal aux systèmes ou aux données informatiques, l´interférence illégale avec des données ou les dommages causés aux systèmes. La répartition entre les infractions générales et les cyberdélits spécifiques pour des actes déterminés est examinée de manière détaillée dans ce chapitre.

La vaste répartition entre les infractions générales et les cyberdélits spécifiques appuie l´approche établie au niveau international pour fixer la place de la « cybercriminalité » dans le spectre global de la « criminalité ». Par exemple, les travaux initiaux entrepris dans le « cadre international de classification des délits » mandaté par le Conseil économique et social des Nations Unies,[3] classent certains actes de cybercriminalité au niveau « vertical » (comme des catégories d´infractions spécifiques mutuellement excluantes), mais classent également des actes de cybercriminalité au niveau « horizontal », comme un « attribut » des délits traditionnels qui implique un élément informatique.[4]

Il importe non seulement d´examiner le caractère général ou spécifiquement informatique des infractions de cybercriminalité mais également de considérer la loi pénale générale. Dans les lois nationales, les infractions de cybercriminalité ne sont pas appliquées ni interprétées par le système de justice pénale de manière isolée, mais en se référant aux règles qui s´appliquent à toutes les infractions, telles que les règles sur la complicité, la tentative, l´omission, l´état d´esprit et les défenses juridiques. Quand il s´agit notamment de « l´état d´esprit », tout exercice de droit comparé doit être réalisé avec précaution. Les différents systèmes juridiques utilisent tout un panel de différents concepts et définitions. Les mêmes termes peuvent avoir des significations différentes dans différents systèmes juridiques. Les systèmes juridiques peuvent faire une distinction entre la volonté et la connaissance, ou définir un panel d´états d´esprit, comme « délibérément », « en ayant connaissance », « imprudemment », et « par négligence ».[5] On peut toutefois discerner dans tous les systèmes juridiques deux catégories générales de conduite délictueuse « intentionnelle » et « non-intentionnelle ».[6]

Ces différences sont importantes quand il s´agit d´infractions de cybercriminalité. De nombreux instruments régionaux et internationaux spécifient, par exemple, qu´un acte doit être considéré comme une infraction pénale « *s´il a été commis intentionnellement* ».[7] D´autres instruments considèrent que les infractions pénales peuvent avoir été commises par imprudence. Le projet de Convention de l´Union africaine déclare que chaque état membre de l´Union africaine devra prendre les mesures législatives nécessaires pour établir comme une « *infraction pénale* » le fait « *même par négligence* » de traiter des données personnelles sans suivre les règles nécessaires du traitement de données.[8] Dans certains pays africains, l´élément mental « frauduleusement » est aussi utilisé couramment dans le droit pénal. Par exemple, le projet de directive de la CEDEAO contient des articles tels que « *l´interception frauduleuse des données informatiques* » et « *l´accès frauduleux aux systèmes informatiques* ».[9] Dans ce contexte, le niveau d´intention requis pourrait être considéré l´équivalent d´une forme d´intention « malhonnête » – davantage que le terme général « intentionnellement », mais moins que l´intention spécifique d´obtenir de l´argent, des biens ou des services par tromperie ou par malhonnêteté. En raison de la vaste portée potentielle de certaines infractions de cybercriminalité, comme l´accès illégal à des données informatiques, il est important que l´élément mental des actes de cybercriminalité soit clairement défini par la loi, dans l´infraction elle-même ou dans le droit pénal général. Lorsque cela est possible, l´analyse législative réalisée dans ce chapitre tente d´identifier les similarités et les différences des éléments de l´intention des infractions.

3 Conseil social et économique des Nations Unies, 2012. Résolution 2012/18. *Améliorer la disponibilité et la qualité des statistiques sur la justice pénale et la criminalité pour le développement de politiques*.

4 Voir le Centre d´excellence d´informations statistiques sur le gouvernement, la criminalité, la victimisation et la justice, 2012. *Rapport sur la réunion de consultation pour le cadre international de classification des délits*. 17-19 octobre 2012, Mexico.

5 Pour les catégories de l´élément mental dans les pays de droit européen continental, voir, par exemple, Roxin, C., 2010. *Strafrecht AT I.* 4ieme ed. Munich. pp.436 et seq. et 1062 et seq. (Germany) ; Picotti, L., 1993. *Il dolo specific.* Milan (Italy). pour les catégories de l´élément mental dans les pays de Common Law voir Dressler, J., 2012.*Comprendre le droit pénal.* 6ieme ed. pp.117–144 (États-Unis) ; Ashworth, A., 2009. *Principes du droit pénal.* 6ieme ed. pp.75, 154-156, 170-191 (Royaume uni).

6 « Intentionnelle » inclut sciemment et délibérément. « Non-intentionnelle » va de l´imprudence à la négligence simple ou grave.

7 voir par la Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 2-9.

8 Le projet de convention de l´Union africaine, Partie IV, Section 3, Art III-29.

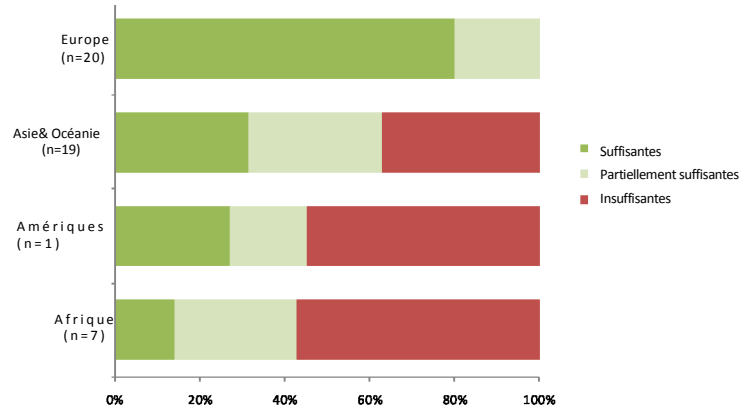
9 Le projet de directive de la CEDEAO, Arts. 2-11.

Des lois pénales suffisantes pour la cybercriminalité

Outre la diversité des approches de législation pénale, les pays montrent également des différences quant à percevoir comme suffisants les cadres d´incrimination en matière de cybercriminalité. Près de 80 % des pays d´Europe qui répondirent au questionnaire de l´étude, signalèrent que leurs lois pénales en matière de cybercriminalité étaient suffisantes et les pays restants déclarèrent qu´elles étaient partiellement suffisantes. Par contre, dans d´autres régions du monde, jusqu´à 60 % des pays signalèrent que leurs lois pénales étaient insuffisantes.

Pour ce qui concerne les principales lacunes du droit pénalen matière de cybercriminalité, plusieurs pays mentionnèrent le fait que les lois pénales, en général,n´étaient pas facilement transposables à la cybercriminalité, ou l´absence d´infractions pour des actes spécifiques de cybercriminalité. Un pays d´Afrique, par exemple, signala que « *il n´y a aucune infraction informatique ou liée à l´informatique* ». Un autre pays d´Asie de l´ouest mentionnait que le problème général était que « *les formes et les éléments essentiels des délits naturels mentionnés dans le code pénal ne peuvent s´appliquer aux délits électroniques* » Un pays d´Asie du sud notait également que « *nous avons besoin de lois spécifiques et détaillées pouvant ériger en délit différents aspects des actes liés à l´informatique. Nous sommes malheureusement dans l´attente de l´une de ces lois qui n´a pas encore été approuvée* »[10] Pour ce qui concerne les lacunes relatives à des conduits spécifiques, un pays d´Asie de l´ouest signala que « *il existe une lacune juridique en matière d´incrimination du vol de données pour obtenir un gain économique ».* Un pays des Caraïbes signalait que « *il n'y a pas de lois spécifiques qui traitent l´envoi de spam, les actes liés à l´informatiques concernant le racisme et la xénophobie, la discrimination, le harcèlement électronique et le vol d´identité etc.,* » et un pays de l´Asie du sud-est souligna que « *certains actes spécifiques de cybercriminalité tels que le spam et les attaques par déni de services (DOS) ne sont pas considérés actuellement comme des délits pénaux ».* Plusieurs pays ont déclaré avoir besoin d´une législation pour traiter les actes spécifiques de cybercriminalité. Un pays d´Europe, par exemple, a signalé que « *actuellement les botnets, l´usurpation et la sollicitation sexuelle ne sont pas incriminés* ». Un autre pays d´Asie du sud-est signalait que « *actuellement le harcèlement en ligne et certains délits liés à l´identité ne sont pas traités de manière adéquate* ».[11]

Figure 4.2 : loi nationales suffisantes pour l´incrimination



Source : questionnaire de l´étude sur la cybercriminalitéQ41. (n=57)

À l´inverse, les pays ont également signalé des points forts et des bonnes pratiques en matière d´incrimination des actes de cybercriminalité. Un pays d´Amérique du nord, par exemple, a signalé que « *l´utilisation d´un langage technologiquement neutre pour couvrir les actes de cybercriminalité* » était une bonne pratique. Un pays d´Asie du sud-est signala qu´une approche mixte avec des infractions générales et des cyberdélits spécifiques était efficace, car « *les délits contre l´intégrité informatique sont totalement couverts par la loi sur les abus informatiques et la plupart des autres formes de cybercriminalité est aussi traitée en grande partie par des lois non spécifiquement relatives à l´ informatique* ». Un pays d´Océanie signala le besoin « *d´une couverture accrue des actes de cybercriminalité »* et l´importance de la dissuasion par le biais « *de sanctions sévères* ».[12]

10 Questionnaire de l´´ étude sur la cybercriminalité Q41.
11 *Ibid.*
12 *Ibid.*

4.2 Analyse des infractions spécifiques

PRINCIPAUX RÉSULTATS :

- alors qu´existe un haut niveau de consensus en matière d´incrimination, une analyse détaillée des dispositions du droit primaire révèle des approches divergentes notoires au niveau national et parfois au niveau international ;
- les particularités des infractions de cybercriminalité ont de l'importance. Les différences des éléments des infractions peuvent créer des difficultés pour établir l´équivalence des infractions dans divers pays à des fins de coopération internationale. De légers changements dans les éléments des infractions, comme l´extension d´un état d´esprit non-intentionnel, peuvent entraîner un risque de surincrimination ;
- les infractions qui impliquent un accès illégal aux données et aux systèmes informatiques diffèrent quant à l´objet de l´infraction (données, systèmes ou informations) et en ce qui concerne l´incrimination du « seul fait » d´accéder ou bien le contournement des mesures de sécurité ou l´exigence de plusieurs tentatives pour considérer qu´un dommage ou une perte a été causé ;
- l´incrimination de l´interception illégale varie en fonction du fait que le délit se limite ou ne se limite pas à la transmission des données non publiques, et en fonction du fait que le délit se limite à l´interception « à l´aide de moyens techniques ;
- il existe des différences entre les pays pour ce qui concerne les actes qui constituent une interférence avec des données ou des systèmes informatiques. La plupart des pays requiert que l´interférence soit intentionnelle, alors que d´autres incluent l´interférence imprudente ;
- tous les pays n´incriminent pas l´usage abusif d´outils informatiques. Pour les pays qui le font, les différences surgissent en fonction du fait que le délit couvre l´utilisation d´outils informatiques et/ou les codes d´accès à l´ordinateur. Il existe aussi des différences relatives au fait que la loi exige que l´outil ait été conçu pour commettre une infraction et/ou au fait que l´auteur de l´infraction ait eu l´intention de l´utiliser pour commettre une infraction ;
- les lois nationales sur la pornographie infantile utilisent diverses terminologies mais seulement un tiers des pays inclut le matériel simulé. La majorité des pays définit la pornographie infantile en se référant à l »âge de 18 ans certains pays utilisent une limite d'âge inférieure. Environ deux tiers des pays incriminent la possession de pornographie infantile.

Cette section du chapitre contient une analyse détaillée des dispositions d´infractions spécifiques de cybercriminalité dans les lois nationales, afin d´identifier les divergences entre les pays qui pourraient poser un problème pour harmoniser la législation sur la cybercriminalité, et les éléments communs des infractions qui pourraient être considérés comme une bonne pratique. L´analyse est basée sur deux sources : (i) les réponses des pays au questionnaire de l´étude et (ii) l´analyse des sources primaires des législations d´un groupe plus important de près de 100 pays.[13] Tout au long de cette section, la source utilisée est indiquée à chaque étape.[14] En général, les réponses des pays au questionnaire sont utilisées pour évaluer l´existence d´une infraction correspondant à un acte spécifique de cybercriminalité.

13 Les sources primaires de législations ont été analysées dans le cas de 97 pays, y compris 56 pays qui ont répondu au questionnaire. La répartition régionale est la suivante : Afrique (15), Amériques (22), Asie (24), Europe (30), et Océanie (6). Il n´a pas été possible d´inclure dans la première analyse des sources primaires de législations 13 pays qui ont répondu au questionnaire car les informations sur les législations pertinentes fournies dans le questionnaire étaient insuffisantes

14 Les attributions à la source sont : (i) le questionnaire de l´étude sur la cybercriminalité et (ii) l´analyse de la législation de l´UNODC. Il faut noter que l´analyse des sources primaires de législations n´est pas à même de tenir compte facilement des interactions juridiques entre des dispositions spécifiques et des parties générales du droit pénal, ou de l´effet des décisions judiciaires ou d´autres lois interprétatives qui affectent la lecture de la disposition législative originale.

Pour les pays qui incriminent l´acte, l´analyse des sources primaires des législations est alors utilisée pour examiner les contenus des infractions dans la loi nationale, en utilisant la méthode du droit comparé fonctionnel.[15] La législation pour chaque acte spécifique de cybercriminalité n´était pas disponible pour tous les pays, afin de pouvoir effectuer l´analyse des sources primaires des législations. Le nombre de pays inclus dans cette partie de l´analyse varie donc en fonction de l´infraction de cybercriminalité examinée.[16]

Accès illégal : convention sur la cybercriminalité du Conseil de l´Europe

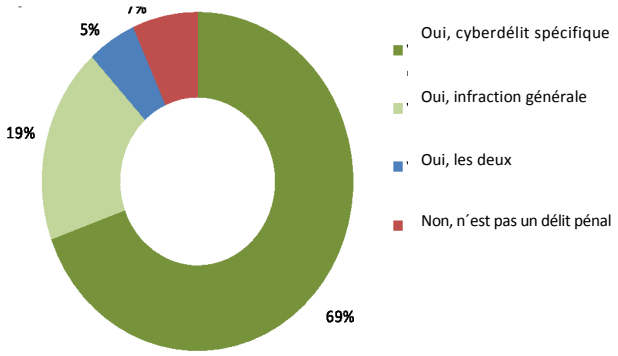
Article 2 – accès illégal

Chaque Partie adopte les 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.

Accès illégal à un système informatique

L´acte d´accéder sans autorisation à un système informatique a existé depuis le début du développement des technologies de l´information.[17] L´accès illégal menace des intérêts comme l´intégrité des systèmes informatiques. Les intérêts juridiques sont violés non seulement lorsqu´une personne non autorisée altère ou « vole » des données d´un système informatique qui appartient à une autre personne, mais également lorsque l´auteur de l´infraction se contente de « jeter un coup d´œil » dans le système informatique. Cet acte viole la confidentialité des données et peut exiger des efforts considérables de la part de la victime pour contrôler l´intégrité ou le statut du système. Le « pur » ou le « simple » accès illégal à un système informatique ne requiert pas que le délinquant ait accès aux fichiers du système ou à d´autres données stockées. L´incrimination de l´accès illégal représente donc une dissuasion importante pour d´autres actes subséquents contre la confidentialité, l´intégrité et la disponibilité des données ou des systèmes informatiques, et pour d´autres infractions liées à l´informatique comme le vol d´identité et la falsification ou la fraude informatique.[18]

Figure 4.3 : incrimination de l´accès illégal à un système



Source : questionnaire de l´étude sur la cybercriminalité .Q25. (n=59)

En conséquence, onz instruments multilatéraux requièrent l´adoption de dispositions incriminant l´accès illégal à des données ou des systèmes informatiques.[19] La législation, au niveau national, reflète bien cette exigence. La figure 4.3 montre qu´environ 70 % des pays qui ont répondu au questionnaire de l´étude

15 Pour des détails sur la méthodologie du droit pénal comparé voir Sieber, U., 2006. Strafrechtsvergleichung im Wandel. *dans :* Sieber, U.,Albrecht, H.J. *Strafrechtsvergleichung und Kriminologie unter einem Dach*. Berlin : Duncker & Humblot, pp.78 et 111-130.

16 Un nombre maximum de 90 pays fut analysé (pour les dispositions de l´accès illégal), et un nombre minimum de 70 pays fut analysé (pour les dispositions sur les outils informatiques malveillants et la pornographie infantile).

17 Voir Kabay, M., 2009. Histoire de la criminalité informatique. *dans :* Bosworth, S., Kabay, M.E. et Whyne, E., manuel de *cybersécurité* 5ieme ed. New York : Wiley ; Sieber, U., 1986. *Manuel international de criminalité informatique.* Chichester : John Wiley & Sons, pp.86-90.

18 Voir Conseil de l´Europe, 2001. *Rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe*, ETS n°. 185, para. 44 : *« l´accès illégal couvre l´infraction basique d´attaques et de menaces dangereuses contre la sécurité (la confidentialité, l´intégrité et la disponibilité) des données et des systèmes informatiques ».*

19 Projet de convention de l´Union africaine, Arts. III-15, III-16 ; projet de loi type du COMESA, Arts. 18, 19 ; loi type du Commonwealth, Art. 5 ; Convention sur la cybercriminalité du Conseil de l´Europe, Art. 2 ; projet de directive de la CEDEAO, Art. 2 ; Décision sur les attaques contre les systèmes informatiques de l´UE, Art. 2(1) ; proposition de directive sur les attaques contre les systèmes informatiques de l´UE, Art. 3 ; textes législatifs types de l´ UIT/CARICOM/CTU, Art. 4 ; Convention de la Ligue des états arabes, Art. 6 ; loi type de la Ligue des états arabes, Art. 3, 5, 15, 22 ; Accord de la Communauté des états indépendants, Art. 3(1)(a).

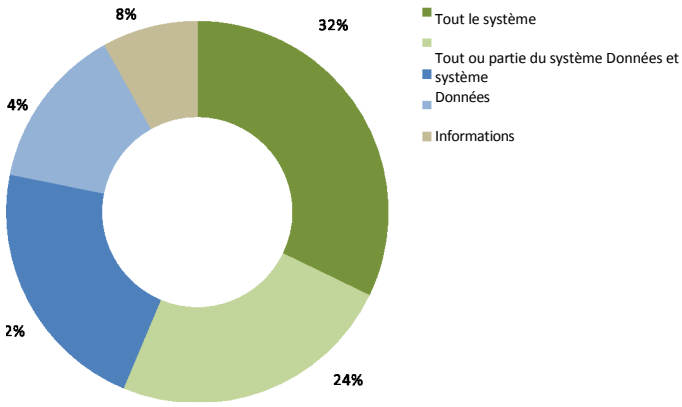
20 Questionnaire de l´étude sur la cybercriminalité Q25.

ont signalé l´existence d´un cyberdélit spécifique d´accès illégal à un système informatique.[20] De plus, environ 20 % des pays répondants ont signalé que l´acte était couvert par des dispositions générales de la loi pénale. Très peu de pays, seulement 7 %, n´incriminent pas l´accès illégal à un système informatique.

L´analyse des sources primaires de législation des dispositions sur l´accès illégal de 90 pays montre des différences transnationales relatives à l´objet de l´infraction, aux actes couverts et à l´élément mental.

Objet de l´infraction – tous les instruments régionaux et internationaux sur la cybercriminalité prévoient l´incrimination de l´accès illégal à une partie ou à la totalité d´un système informatique. Cependant, seulement 55 % des pays inclus dans l´analyse des sources primaires de législation suivent cette approche. La figure 4.4 démontre que certaines lois nationales limitent l´objet de l´accès illégal aux données ou aux informations au lieu du système, ou incriminent l´accès aux données *et* au système, parfois dans des dispositions différentes. Certaines dispositions nationales vont même plus loin en limitant l´approche. Plusieurs pays d´Asie de l´ouest et d´Europe de l´est, par exemple, incrimine l´accès illégal aux « *informations protégées par la loi* ».

Figure 4.4 : objets de l´accès illégal



Source : révision de la législation de l´ ONUDC. (n=87)

Actes couverts –

L´incrimination du « simple » accès illégal, ou l´exigence de plusieurs actes ou tentatives, représentent un autre point de divergence. Tous les instruments internationaux prévoient l´option d´incriminer le simple accès non autorisé à un système informatique. Toutefois, certains instruments prévoient des conditions supplémentaires. La Convention sur la cybercriminalité du Conseil de l´Europe[21] et les textes législatifs types de l´UIT/CARICOM/CTU,[22] par exemple, donnent aux pays la possibilité d´incorporer des conditions additionnelles – comme « contourner la sécurité » ou « intention malhonnête ». La Décision de l´UE sur les attaques contre les systèmes informatiques donne aux états membres la possibilité de ne pas incriminer les infractions mineures.[23] L´Accord de la Communauté des états indépendants requiert l´incrimination de l´accès illégal quand « *ces actes causent la destruction, le verrouillage, la modification ou la reproduction de l´information ou la perturbation du fonctionnement de l´ordinateur, du système informatique ou des réseaux associés* ».[24]

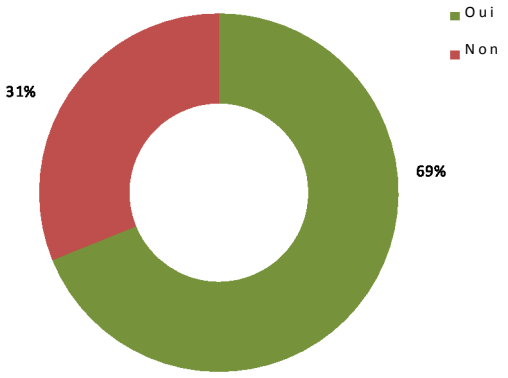
Accès illégal : exemple national d´un pays du sud de l´Europe

Celui qui accède à un système informatique sans la permission ou l´autorisation légale du propriétaire ou du détenteur des droits sur la totalité ou une partie du système, sera puni d´une peine de prison de___ ans ou d´une amende de ____.

21 Convention sur la cybercriminalité du Conseil de l´Europe, Art. 2.
22 Textes législatifs types de l´UIT/CARICOM/CTU, Art. 5.
23 Décision de l´UE sur les attaques contre les systèmes informatiques, Art. 2.
24 Accord de la Communauté des états indépendants, Art. 3(1)(a).
25 Voir, par exemple, Sieber, U., 1985. *Informationstechnologie und Strafrechtsreform.* Cologne : Carl Heymanns Verlag, p.49.

Ces conditions permettent aux états d´adopter une législation plus restrictive sur l´accès illégal. En effet, le consensus sur l´incrimination souhaitable du simple accès illégal aux systèmes non protégés n´est pas universel.[25] D´autre part, certaines conditions prévues par les approches internationales, notamment celles qui incluent l´exigence d´actes additionnels, peuvent rendre difficile la distinction entre l´accès illégal et les infractions subséquentes –avec la possible confusion des limites existantes entre l´accès illégal et des infractions telle que l´interférence avec les données ou l´espionnage de données.

Figure 4.5 : incrimination du simple accès illégal



Source : révision de la législation de l´ONUD . (n=90)

La figure 4.5 montre que, parmi les pays qui incriminent l´accès illégal, environ 70 % incriminent le seul fait d´accéder illégalement. Les 30 % restants exigent des conditions supplémentaires pour que cet acte constitue un délit. Il n´y a pas de patron régional clair pour ce résultat. Quelques pays exigent qu´il y ait une « *violation des mesures de sécurité* »ou d´autres intentions comme *« l´intention de commettre un autre délit ».* Certaines lois nationales limitent l´accès illégal aux cas de « *graves violations* » ou de « *crimes graves,* » comme dans le cas d´un pays d´Océanie.[26] De plus, certains statuts nationaux incriminent l´accès illégal seulement si les données sont « *copiées* », « *bloquées*, « *volées* », « *modifiées* » ou « *effacées* », ou si l´accès illégal est commis « *en association avec* » une interférence du système. Dans certains pays, ceci entraîne l´incrimination de l´accès illégal en tant que l´un des éléments qui constituent une infraction d´interférence avec les données ou les systèmes. Par exemple, un pays d´Europe de l´est incrimine « *l´interférence avec les données et les systèmes* » seulement si l´acte est commis « *conjointement* » avec un accès non autorisé à un système informatique. Ceci a pour effet de limiter l´incrimination de l´interférence avec les données dans les cas où l´accès illégal est la première étape dans le fait de commettre une infraction contre les systèmes et les données.

État d´esprit – tous les instruments multilatéraux exigent que le délit d´accès illégal soit commis intentionnellement ou, dans le cas de deux instruments, « *frauduleusement ».*[27] Cependant, la définition de ce qui constitue une intention repose généralement sur le pays qui l´applique. Par exemple, le rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe déclare explicitement que la signification exacte du terme « intentionnellement » doit être « *laissée aux droits internes* ».[28] À cet égard, comme cela a été mentionné précédemment, l´état d´esprit exact qui constitue le caractère intentionnel diffèrent entre les divers systèmes juridiques nationaux – en fonction du droit pénal général et du droit pénal spécial.[29] L´analyse des sources primaires de législation montre toutefois que, dans le cas des dispositions sur l´accès illégal qui mentionnent spécifiquement l´état d´esprit, l´utilisation d´éléments mentaux tels que « *intentionnellement* », « *en ayant connaissance »*, « *délibérément »*, et « *frauduleusement »*– indique que certaines formes d´intentionnalité sont généralement requises pour qu´il y ait une infraction. Dans seulement deux pays inclus dans l´analyse, situés aux Caraïbes et en Océanie, l´accès illégal peut être commis par « *imprudence ».*

26 Ce pays limite l´incrimination des actes commis avec l´intention de faciliter ou de commettre un délit grave par le biais d´un accès illégal. Un délit grave est défini comme un délit passible d´une peine de prison à perpétuité ou au moins supérieure à cinq ans.

27 Le projet de Convention de l´Union Africaine, Arts. III-15, III-16 ; le projet de directive de la CEDEAO, Arts. 2, 3.

28 Conseil de l´ Europe, 2001. Rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe, ETS n°. 185, para. 39 : *« toutes les infractions énumérées dans la Convention doivent être commises de façon intentionnelle pour que la responsabilité pénale soit engagée. Dans certains cas un élément intentionnel spécifique supplémentaire fait partie intégrante de l´infraction. Par exemple, dans l´Article 8 concernant la fraude informatique, l´intention d´obtenir un bénéfice économique est un élément constitutif de l´infraction. Les auteurs de la Convention sont convenus que le sens exact du mot « intentionnellement » devrait être laissé à l´interprétation qui lui est donnée par le droit national ».*

29 Voir, par exemple, LaFave, R.W., 2000. *Droit pénal.* 3ieme ed. St. Paul : MN. pp. 224-234 ; Fletcher, G., 1998. *Concepts basiques du droit pénal.* Oxford University Press, pp.99-100, 111-129 ; Fletcher, G., 1971. La théorie de la négligence criminelle : une analyse comparative. *Revue juridique de l´université de Pennsylvanie*119(3) :401-403.

Circonstances aggravantes–quatre instruments multilatéraux sur la cybercriminalité incluent des circonstances aggravantes dans les dispositions concernant l´accès illégal. La loi type de la Ligue des états arabes prévoit des peines aggravées si l´accès illégal est commis « *dans l´intention d´annuler, de supprimer, de détruire, de divulguer, d´endommager, de changer, ou de rediffuser des informations ou des données personnelles »* (Art. 3), ou si l´accès illégal est commis par le contrevenant « *dans l´exercice ou à cause de l´exercice de ses fonctions ou s´il a facilité le fait de commettre ces infractions à une tierce partie* » (Art. 5). La Convention de la Ligue des états arabes prévoit des circonstances aggravantes si l´accès illégal entraîne « l´*oblitération, la modification, la distorsion, la duplication, la suppression ou la destruction de données sauvegardées, d´instruments électroniques, de systèmes et de réseaux de communications, des dommages pour les utilisateurs et les bénéficiaires ou l´obtention d´informations gouvernementales secrètes* » (Art. 6). Le projet de loi type du COMESA a des dispositions additionnelles qui incriminent l´accès illégal aux « *ordinateurs du gouvernement* » ou « *aux systèmes informatiques utilisés pour les opérations des infrastructures critiques* » (Art. 19). La proposition de directive de l´UE sur les attaques contre les systèmes informatiques (Art. 10) introduit l´exigence de peines aggravées pour des délits d´accès illégal commis : (i) dans le cadre d´une « *organisation criminelle* » ; (ii) en utilisant un « *outil conçu pour lancer des attaques qui affectent un nombre significatif de systèmes informatiques* » ou des attaques qui causent des dommages considérables comme la perturbation des services de systèmes, des coûts financiers ou la perte de données personnelles ; ou (iii) en « *dissimulant l´identité réelle* » de l´auteur de l´infraction et en causant un préjudice au propriétaire légitime de l´identité.

Au niveau national, plusieurs pays qui incriminent le simple accès illégal ont aussi établi des circonstances aggravantes qui font l´objet de sanctions plus sévères. Ces circonstances varient beaucoup de pays à pays, et les circonstances identifiées incluent :

- le fait de commettre l´acte avec une intention préjudiciable ou d´obtenir un gain financier illicite ;
- l´interférence avec le fonctionnement d´un système informatique ;
- la suppression ou l´altération de données ;
- la reproduction, l´usage, la divulgation ou toute autre violation des programmes ou des données informatiques ;
- l´accès à un troisième ordinateur ;
- causer des dommages considérables ;
- créer un désordre public ;
- faciliter ou soutenir le délit de terrorisme ;
- commettre l´acte en tant que membre d´un groupe organisé ;
- combiner l´acte avec une conduite violente.

Comme cela est mentionné ci-dessus, plusieurs de ces circonstances coïncident avec d´autres infractions possibles, séparées, telles que l´interférence illégale de données ou les dommages causés au système. Toutefois, les circonstances aggravantes les plus communes, rencontrées lors de la révision des sources primaires de législations, impliquaient les ordinateurs essentiels pour le fonctionnement des infrastructures bancaires, de télécommunications, de services de santé, de services publics ou des ordinateurs du gouvernement. Plus de la moitié des lois nationales examinées prévoyait une protection spéciale avec des peines plus sévères pour l´accès illégal à des ordinateurs gérés par des autorités gouvernementales ou qui pouvaient être liés au fonctionnement des infrastructures critiques.

Se maintenir illégalement dans un système informatique

Deux instruments multilatéraux traitent non seulement l´accès illégal à un système informatique, mais également le fait de « *se maintenir* » dans un système sans en avoir le droit après que l´autorisation ait expiré.[30] Les textes législatifs types de l´UIT/CARICOM/CTU offrent aux pays la possibilité de ne pas incriminer le simple fait de se maintenir sans autorisation dans le système, s´il existe d´autres recours efficaces. Le projet de directive de la CEDEAO pour sa part, requiert l´incrimination du fait de se maintenir « *frauduleusement* » dans un système informatique.

Ces divergences se reflètent dans la législation nationale. Certaines lois incorporent le concept de maintien illégal dans les dispositions concernant l´accès illégal alors que d´autres l´incriminent séparément. Cependant, le plus souvent, le fait de se maintenir illégalement dans un système informatique n´est pas spécifiquement incriminé. Parmi tous les pays inclus dans l´analyse des sources primaires de législations, seulement neuf pays répartis dans diverses régions incriminaient le maintien illégal dans un système informatique. Huit d´entre eux l´avaient incorporé dans les dispositions relatives à l´accès illégal et l´un d´entre eux dans une disposition séparée.

Maintien illégal : projet de directive de la CEDEAO

Article 3 – se maintenir frauduleusement dans un système informatique
L´acte par lequel une personne se maintient ou tente de se maintenir frauduleusement dans tout ou partie d´un système informatique.

30 Projet de directive de la CEDEAO, Art. 3 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 5

Interception illégale de données informatiques

L´incrimination de l´interception illégale étend la protection de l´intégrité et la confidentialité des données informatiques, des données existant dans un système à toutes les données transmises. La principale crainte concernant l´interdiction de l´interception des données lors de la transmission est la violation de la confidentialité des communications privées .[31]

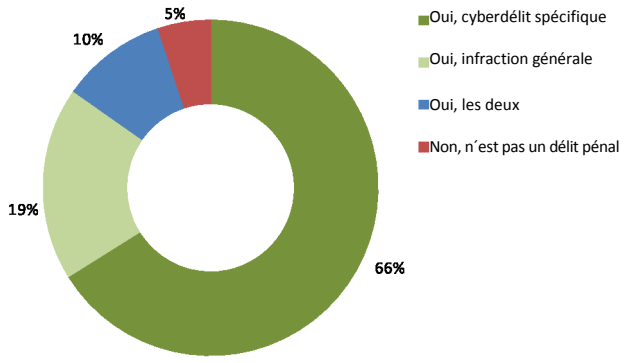
Neuf instruments internationaux incluent des dispositions spécifiques qui incriminent l´interception de données informatiques.[32] Au niveau national, alors que plusieurs pays ont des infractions spécifiques qui couvrent l´interception de données informatiques, d´autres appliquent les lois existantes, qui incluent l´interdiction d´intercepter les communications en général. Une des raisons de cette situation est le fait que l´interception de données informatiques peut être considérée du point de vue de l´intégrité des données ou de la protection de la vie privée.

Interception illégale : projet de directive de la CEDEAO

Article 6 – interception frauduleuse de données informatiques
L´acte par lequel une personne intercepte ou tente d´intercepter frauduleusement des données informatiques durant leur transmission non-publique vers, depuis ou dans un système informatique par des moyens techniques.

Les questions de l´étude sur la cybercriminalité portaient sur l´interception illégale des données informatiques dans le contexte de l´interception, l´accès ou l´acquisition de données informatiques. L´étude n´a donc pas recueilli d´informations directes séparées sur l´interception illégale. La figure 4.6 montre cependant que 85 % des pays répondants ont des dispositions qui incriminent l´interception illégale, l´accès ou l´acquisition de données informatiques. Dans 65 % des pays l´incrimination est par le biais d´un cyberdélit spécifique. Parmi les pays qui disposent d´un cyberdélit spécifique qui couvre l´interception illégale, l´analyse des sources primaires de législations montre des différences entre l´*objet* de l´infraction et les *actes* couverts.

Figure 4.6 : incrimination de l´accès illégal, de l´interception ou de l´acquisition de données informatiques



Source : questionnaire de l´étude sur la cybercriminalité Q26. (n=59)

Objet de l´infraction – la plupart des instruments multilatéraux sur la cybercriminalité définit l´objet de l´interception illégale comme une transmission « *non-publique* » de données informatiques, en limitant donc l´objet à des transmissions « privées ». Cette limitation se réfère au caractère prévu de la transmission. Par exemple, une communication qui a un caractère privé mais qui est envoyée par un réseau public Wi-Fi peut être protégé contre une interception illégale, même si la transmission est réalisée depuis un réseau public.[33] Le seul document qui ne limite pas l´incrimination à la transmission non-publique est la loi type de la Ligue des états arabes (Art. 8). Certains instruments multilatéraux, outre les transmissions non-publiques, traitent également l´interception des « *émissions électromagnétiques* » – un terme utilisé pour élargir la portée de l´infraction.[34]

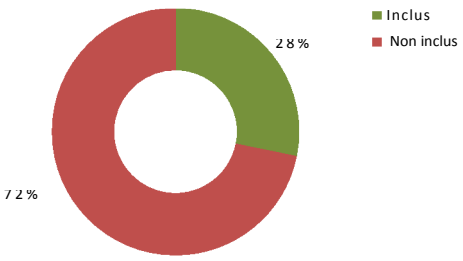
31 Walden, I., 2007. *Cyberdélit et enquêtes numériques.* Oxford : OUP, p.184.

32 Projet de convention de l´Union africaine (Art. III-23) ; projet de loi type du COMESA, Art. 21 ; loi type du Commonwealth, Art. 8 ; Convention sur la cybercriminalité du Conseil de l´Europe, Art. 3 ; projet de directive de la CEDEAO, Art. 6 ; proposition de directive de l´UE sur les attaques contre les systèmes informatiques, Art. 6 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 6 ; Convention de la Ligue des états arabes, Art. 7 ; loi type de la Ligue des états arabes, Art. 8.

33 Voir, par exemple le rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe 2001. ETS n°. 185.

Alors que la majorité des instruments multilatéraux limite l´application de l´interception illégale aux transmissions privées de données informatiques, l´analyse de la législation de 78 pays montre que, au niveau national, la portée de l´infraction dans beaucoup de cas n´est pas restreinte aux transmissions non publiques de données. La figure 4.7 montre que seuls moins de 30 % des pays examinés limitent l´interception illégale aux transmissions privées ou protégées. Toutefois, dans la pratique, en raison de l´interprétation large donnée au terme « non-publique », il est probable que cela n´élargisse pas significativement la portée de l´infraction.

Figure 4.7: transmissions privées/non-publiques restreintes



Source : révision de la législation de l´UNODC (n=78)

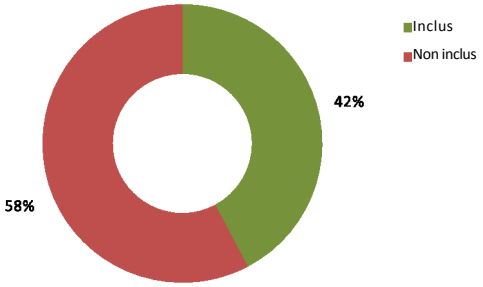
Une autre question concerne le concept de « transmission ». On peut considérer que les données sont « en cours de transmission » lorsqu´elles n´ont pas atteint leur destination finale : le système ou le destinataire visé. La transmission de données pourrait être considérée comme terminée lorsque le système informatique de destination est atteint. Sinon les données pourraient être considérées « en cours de transmission », quand elles sont stockées dans le système jusqu´à ce que le destinataire visé y ait accès. Aucun instrument multilatéral ne fournit d´orientation concernant le point final de la transmission. La distinction est importante pour ce qui concerne le stockage temporaire des données qui a lieu lorsque les données informatiques sont transmises en utilisant un protocole opéré sur une base de « stockage et émission ».[35]

Interception illégale : exemple national d´un pays d´Amérique

Une personne qui sciemment et sans justification ni excuse légitime intercepte par des moyens techniques :
(a) une transmission non publique à destination, en provenance ou à l´intérieur d´un système informatique ; ou
(b) des émissions électromagnétiques qui transportent des données informatiques d´un système informatique est coupable d´un délit et est passible, si elle est reconnue coupable, d´une amende de____ ou d´une peine de prison de____ ans ou des deux sanctions.

Plusieurs pays ont abordé cette question dans leur législation nationale. Un pays d´Océanie utilise, par exemple, une disposition juridique qui exclut « *..les communication stockées sur une base hautement transitoire qui une fonction intégrale de la technologie utilisée dans cette transmission*de la définition des communications stockées. Ces données pourraient donc être incluses dans la portée de l´infraction d´interception illégale de données informatiques.

Figure 4.8 : est-ce que les moyens techniques sont inclus comme un élément de l´infraction d´interception illégale ?



Source : révision de la législation de l´ONUDC. (n=78)

Actes couverts – les instruments multilatéraux, à l´exception d´un instrument,[36] limite les actes d´interception aux actes commis en utilisant des moyens techniques.

34 Y compris la loi type du Commonwealth ; les textes législatifs types de l´UIT/CARICOM/CTU ; la proposition de directive de l´UE sur les attaques contre les systèmes informatiques et la Convention sur la cybercriminalité du Conseil de l´Europe.
35 Walden, I., 2007. *Cyberdélits et enquêtes numériques.* Oxford : OUP, p.185.
36 Convention de la Ligue des états arabes, Art. 8.

Comme le précise le rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe, cette exigence représente une condition restrictive, afin d´éviter une surincrimination.[37] Cette limitation n´est toutefois pas toujours reflétée par les approches nationales. La figure 4.8 montre que plus de la moitié des pays dans toutes les régions du monde dont la législation a été examinée, n´inclue pas les moyens techniques comme un élément de l´infraction d´interception illégale.

Interférence illégale : décision de l´UE sur les attaques contre les systèmes informatiques

Article 4 – interférence illégale des données
Chaque état membre prend les mesures nécessaires pour veiller à ce 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 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.

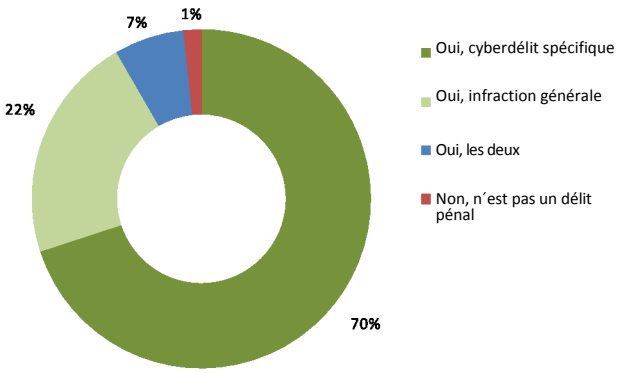
Interférence illégale : Convention sur la cybercriminalité du Conseil de l´Europe :

Article 5 – interférence 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.

État d´esprit – les instruments multilatéraux requièrent généralement que le délit d´interception illégale soit commis intentionnellement. La Convention sur la cybercriminalité du Conseil de l´Europe offre aux parties la possibilité de limiter l´infraction d´interception illégale aux cas commis avec une intention malhonnête. L´examen de la législation nationale montre que très peu de pays exigent d´autres intentions bien que certains associent l´interception avec l´intention de commettre d´autres infractions. Un pays d´Europe de l´est, par exemple, incrimine l´interception illégale des données seulement si l´acte est commis dans le but de commettre des cyberdélits spécifiques. De plus, certains pays incluent les intentions dans les circonstances aggravantes. Deux pays d´Europe de l´ouest prévoient, par exemple, des peines plus sévères si l´interception illégale est commise dans l´intention d´obtenir un bénéfice financier.

Interférence illégale avec des données ou des systèmes informatiques

Figure 4.9 : incrimination de l´interférence illégale des données ou des dommages causés au système



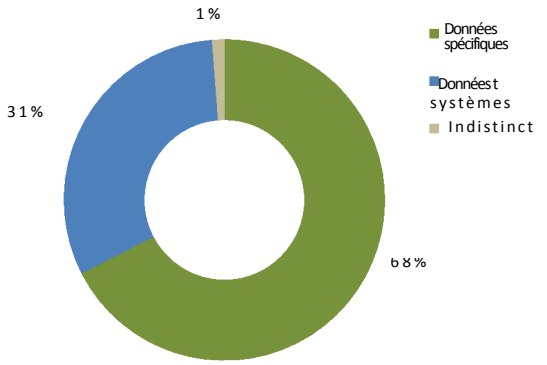
Source : questionnaire de l´étude sur la cybercriminalitéQ27. (n=60)

L´interférence avec les données ou les systèmes informatiques met en danger l´intégrité et la disponibilité des données informatiques, ainsi que le fonctionnement correct des programmes et des systèmes informatiques. En raison du caractère intangible des données informatiques, plusieurs systèmes juridiques nationaux ne sont pas à même d´appliquer les dispositions du droit pénal traditionnel qui traitent la destruction des biens physiques à l´interférence avec les données informatiques.[38] Par conséquent la plupart des instruments multilatéraux inclut des infractions spécifiques relatives à l´interférence illégale avec les données et/ou les systèmes.

37 Rapport explicatif pour la Convention sur la cybercriminalité du Conseil de l´Europe, ETS n°. 185.
38 Sieber, U., 2008. Maîtrise de la complexité dans le cyberespace global : l´harmonisation du droit pénal informatique. *dans :* Delmas-Marty, M., Pieth, M. et Sieber, U., (eds.) *Les chemins de l´»Harmonisation Pénale. Collection de L´»UMR de Droit Comparé de Paris.* Vol. 15. Paris : Société de législation comparée.

Au niveau national, la Figure 4.9 montre que 90 % des pays répondants ont une infraction pénale qui couvre l´interférence illégale avec des données ou des systèmes informatiques. Soixante-dix % de ces pays mentionnent un cyberdélit spécifique. Dans 7 % des pays déclarants, l´acte est couvert par un cyberdélit spécifique et une infraction générale. L´examen des sources primaires de législations de 83 pays présente des différences dans la législation nationale concernant l´*objet* de l´infraction, *l´état d´esprit* requis et les *circonstances aggravantes connexes*.

Figure 4.10 : objets de l´interférence de données

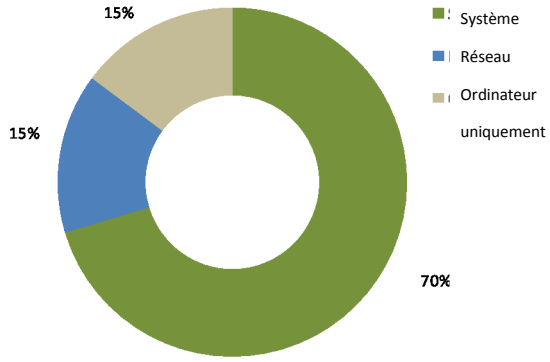


Source : révision de la législation de l´ONUDC. (n=83)

Objet de l´infraction – la plupart des instruments multilatéraux exige l´adoption de dispositions séparées pour incriminer l´interférence illégale avec les données et les systèmes informatiques.[39] Seule la loi type de la Ligue des états arabes allie les deux concepts.[40]

Pour la majorité des législations nationales examinées, l´interférence des données et l´interférence des systèmes sont incluses dans des dispositions séparées. Cependant, dans environ 30 % des pays examinés, les infractions ne sont pas clairement séparées, ou bien l´interférence des données est incriminée seulement si elle a une incidence sur le fonctionnement du système informatique. Bien que cela puisse être souvent le cas dans la pratique, l´approche pourrait entraîner des lacunes en matière d´incrimination de l´acte isolé d´interférence avec des données. Néanmoins, cela peut être couvert dans certains pays par le droit pénal général. Un pays d´Amérique utilise, par exemple, une disposition générale relative au fait de détruire ou d´endommager des biens – dans laquelle la définition de « biens » comprend les données informatiques.

Figure 4.11 : objets de l´interférence des systèmes



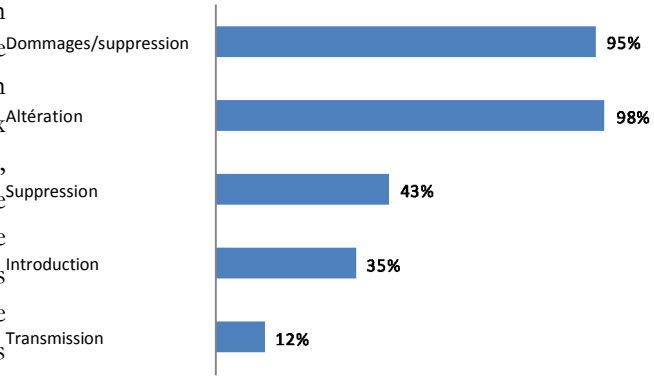
Source : révision de la législation de l´ONUDC (n=81)

En ce qui concerne l´élément « *système* » dans l´acte d´interférence illégale, l´analyse des dispositions applicables montre que les lois nationales couvrent généralement les « *systèmes* » informatiques. Toutefois, dans 30 % des pays l´infraction était limitée aux « *réseaux* » informatique ou à « *l´ordinateur* ». Ceci peut limiter l´incrimination en excluant les cas dans lesquels un ordinateur qui est endommagé ne fait pas partie d´un réseau ou les cas dans lesquels de multiples dispositifs, y compris des routeurs de réseaux, subissent une interférence par le biais d´un logiciel malveillant ou d´une attaque DDoS.

39 Projet de Convention de l´Union africaine, Arts. III-19, III-20 ; projet de loi type du COMESA, Art. 20-b ; loi type du Commonwealth, Art. 6 ;Convention sur la cybercriminalité du Conseil de l´Europe, Art. 4 ; projet de directive de la CEDEAO, Arts. 5, 7 ; Décision de l´UE sur les attaques contre les systèmes informatiques, Art. 3 ; proposition de directive de l´UE sur les attaques contre les systèmes informatiques, Art. 4 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 7 ; Convention de la Ligue des états arabes, Art. 8.

40 Loi type de la Ligue des états arabes, Art. 6.

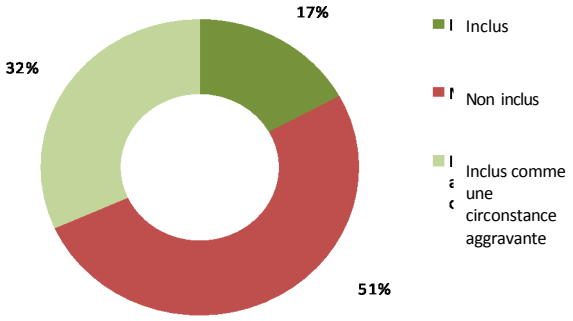
Figure 4.12 : éléments qui constituent une interférence illégale de données



Source : révision de la législation de l´UNODC. (n=83)

Actes couverts – les instruments multilatéraux couvrent l´incrimination de divers actes qui constituent une interférence, et cela inclut non seulement les dommages causés aux données mais également la « *suppression* », la « *détérioration* », « l´*altération* », et même « *l´introduction* » de données, c´est à dire qu´ils protègent l´intégritédes données au sens large. La figure 4.12 montre que la majorité des lois nationales examinées couvrent l´altération, la suppression et les dommages causés aux données. Seulement 35 % des pays incluent « l´introduction » de données dans les dispositions relatives à l´interférence. La « suppression » des données est couverte par un peu plus de 40 % des pays. Seulement 12 % des pays incriminent la « transmission » des données conformément aux dispositions relatives à l´interférence des données. On pourrait supposer que la « transmission » des données est incriminée dans les pays où l´interférence avec les données et les systèmes est couverte par une unique disposition, car la transmission de données pourrait avoir une incidence sur le système. Cependant, l´analyse montre qu´il n´y a pas de corrélation. Les pays ayant des dispositions séparées relatives à l´interférence avec les données incluent aussi la transmission dans la liste des actes interdits.

Figure 4.13 : dommages inclus sont-ils un élément nécessaire pour qu´il y ait une interférence de données ?



Source : révision de la législation de l´ONUDC. (n=83)

Certains instruments multilatéraux permettent aux pays d´exprimer des réserves concernant les effets causés par l´interférence de données. La Convention du Conseil de l´Europe sur la cybercriminalité offre, par exemple, la possibilité de limiter l´incrimination l´interférence de données aux cas où des dommages graves ont été causés.[41] La Décision de l´UE sur les attaques contre les systèmes informatiques offre la possibilité de ne pas incriminer les infractions mineures.[42]

La figure 4.13 montre qu´au niveau national seulement 17 % des pays examinés incluent la perte ou les dommages causés comme un élément nécessaire de l´ interférence de données.

Interférence de système : exemple national d´un pays d´Afrique australe

Endommager ou nier l´accès à un système informatique : toute personne qui sans justification ni autorité légitime, commet un acte qui cause directement ou indirectement :
(a) une détérioration, une défaillance, une interruption ou une entrave au fonctionnement d´un système informatique ; ou
(b) un refus d´accès ou la détérioration des programmes et des données stockées dans le système informatique, commet une infraction et est passible, si elle est reconnue coupable, d´une amende n´excédant pas ___ et d´une peine de prison n´excédant pas ___ ans.

41 Convention du Conseil de l´Europe sur la cybercriminalité, Art. 4.
42 Décision de l´UE sur les attaques contre les systèmes informatiques, Art. 3.
43 La loi type du Commonwealth, Art. 7 ; les textes législatifs types de l´ UIT/CARICOM/CTU, Art. 3(10).

En ce qui concerne les dommages causés par l´interférence de données, un peu plus de 30 % des pays prévoient des circonstances aggravantes. La moitié des lois nationales ne mentionnent pas les dommages causés par l´interférence avec les données dans les dispositions nationales pertinentes. Comme c´est le cas pour les données informatiques, les systèmes informatiques peuvent être endommagés de différentes manières, par exemple, par le biais de la transmission, l´altération ou la suppression des données, avec une interférence électromagnétique ou en privant le système d´alimentation électrique. Les dispositions des instruments multilatéraux relatives à l´interférence avec les systèmes incluent généralement les termes « *altération* ». « *suppression* » et « *transmission de données* » ou « *manipulation* » de données ou de programmes. Des définitions plus larges sont toutefois incluses dans la loi type du Commonwealth et les textes législatifs types de l´UIT/CARICOM/CTU, qui incluent non seulement la manipulation de données, mais également le fait de priver d´alimentation électrique un système informatique, de causer des interférences électromagnétiques et de corrompre le système informatique par quelque moyen que ce soit.[43]

Figure 4.14 : actes qui constituent une interférence illégale avec le système

Source : révision de la législation de l´ONUDC (n=81)

La figure 4.14 montre que les actes comme « *endommager* », « *interférer* », et « *entraver* » sont inclus dans la majorité des législations nationales examinées. Deux grandes tendances observées au niveau législatif sont l´utilisation du terme « *entraver de la manière que ce soit* », qui crée une large base pour l´incrimination de l´interférence avec les systèmes, et l´annexion de dispositions concernant l´interférence avec le système dans les dispositions relatives à l´accès illégal pour créer une base plus étroite.

Interférence illégale avec les données : exemple national d´un pays d´Asie du sud est

Modification non autorisée du contenu d´un ordinateur :

(1) une personne se rendra coupable d´une infraction si elle commet un acte dont elle sait qu´il causera une modification non autorisée du contenu d´un ordinateur.

(2) aux fins de la présente section, il importe peu que l´acte en question ne vise pas :

(a) une donnée ou un programme particulier ;

(b) une donnée ou un programme quel qu´il soit ; ou

(c) une donnée ou un programme contenu dans un ordinateur particulier.

(3) aux fins de la présente section, il importe peu que la modification non autorisée soit, ou est destinée à être permanente ou temporaire.

Aux fins de la présente loi, une modification du contenu d´un ordinateur a lieu si, en exécutant une fonction de l´ordinateur en cause ou de tout autre ordinateur :

(a) une donnée ou un programme contenu dans l´ordinateur en cause est altéré ou supprimé ;

(b) une donnée ou un programme est ajouté à son contenu ; ou

(c) il survient une entrave au fonctionnement normal de l´ordinateur,

et tout acte qui contribue à provoquer une modification en sera considéré la cause.

État d´esprit – de nombreux instruments multilatéraux sur la cybercriminalité exigent que le délit d´interférence illégale avec les données ou les systèmes informatiques soit commis « *intentionnellement* » ou « *frauduleusement* »[44] La loi type de la Ligue des états arabes ne mentionne pas l´intention dans ses dispositions relatives à l´interférence. Elle exige toutefois l´existence qu´il y ait le but spécifique de stopper le fonctionnement des données ou du système.[45] La loi type du Commonwealth a une approche différente, car elle exige explicitement l´incrimination des actes d´interférence commis par *imprudence*.[46] Ceci crée une base particulièrement large pour l´incrimination car il est souvent plus facile d´interférer involontairement avec les données informatiques ou avec le fonctionnement de systèmes informatiques, qu´avec des objets ou des biens dans le monde physique.[47] Parmi 81 pays dont les dispositions concernant l´interférence avec les données furent examinées, seulement six pays suivaient cette approche et incriminaient l´interférence avec les données commise *par imprudence* ou par *négligence*. La majorité de ces pays n´étaient pas membres du Commonwealth et se trouvaient en Amérique du sud, en Europe de l´ouest et en Afrique

44 Projet de Convention de l´Union africaine, Arts. III-19, III-20 ; projet de loi type du COMESA, Art. 20-b ; Convention sur la cybercriminalité du Conseil de l´Europe, Art. 4 ; projet de directive de la CEDEAO, Arts. 5, 7 ; Décision de l´UE sur les attaques contre les systèmes informatiques, Art. 3 ; proposition de directive de l´UE sur les attaques contre les systèmes informatiques, Art. 4 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 7 ; Convention de la Ligue des états arabes, Art. 8.

45 Loi type de la Ligue des états arabes, Art. 6.

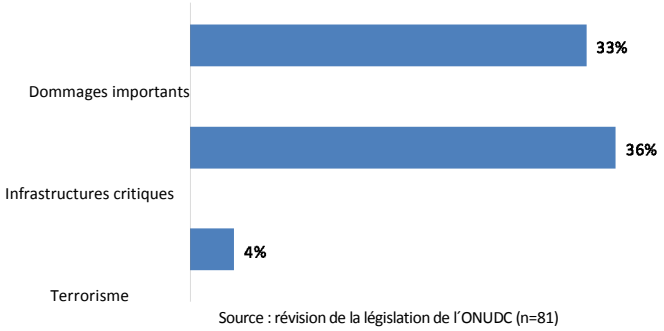
46 Loi type du Commonwealth, Art. 6.

47 De Hert, P., Fuster, G. et Koops, B. J., 2006. Lutte contre la cybercriminalité dans les deux Europes. La valeur ajoutée de la décision cadre de l´UE et la Convention du Conseil de l´Europe. *Revue internationale de droit pénal*, 77 :6.

48 Projet de loi type du COMESA, Art. 20-c, d, e, f.

Circonstances aggravantes – les instruments multilatéraux sur la cybercriminalité n´exigent pas, en général, des peines aggravées pour l´interférence illégale avec des données. Il existe deux exceptions. Le projet de loi type du COMESA prévoit des peines aggravées lorsqu´il existe l´intention de causer des dommages graves, de menacer la sécurité publique, de perturber des infrastructures critiques ou des fins terroristes.[48]

Figure 4.15 : circonstances aggravantes de l´interférence illégale avec le système



Source : révision de la législation de l´ONUDC (n=81)

La proposition de directive de l´UE sur les attaques contre les systèmes informatiques (dans le cas de l´accès illégal), exige que les pays prévoient des circonstances aggravantes lorsque des organisations criminelles sont impliquées, lorsque sont utilisés des outils conçus pour attaquer un grand nombre de systèmes informatiques ou lorsque la véritable identité de l´auteur de l´infraction est dissimulée.[49]

Au niveau national, les pays qui incriminent l´interférence avec les données ont inclus des circonstances aggravantes qui font l´objet de peines plus sévères. La figure 4.15 montre qu´il s´agit le plus souvent de *« dommages importants,* » ou d´atteinte aux « *infrastructures critiques* ». Un petit nombre de pays dont la législation a été révisée incluent aussi des circonstances aggravantes lorsque l´interférence est liée au terrorisme. Peu de lois incluent des circonstances aggravantes pour des infractions commises de façon organisée et les actes commis dans le but d´obtenir un bien. Quelques pays ont aussi créé des protections additionnelles pour des types spécifiques de données. Un pays d´Asie a par, exemple, établi une peine aggravée pour l´interférence avec des données de registres médicaux et de soins de santé.

Outils informatiques malveillants : loi type du Commonwealth

Article 9(1) – dispositifs illégaux Une personne 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, y compris un programme informatique, qui est conçu ou adapté pour permettre de commettre l'une des infractions établies conformément aux articles 5, 6, 7 ou 8

(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 5, 6, 7 ou 8 ; et

(b) en sa possession un dispositif mentionné 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 articles5, 6, 7 ou 8.

(2) Une personne jugée coupable d'une infraction contre cette section est passible d'une peine de prison d'une durée maximale de___, ou d'une amende maximale de _____, ou des deux.

49 Proposition de directive de l´UE sur les attaques contre les systèmes informatiques Art. 10.

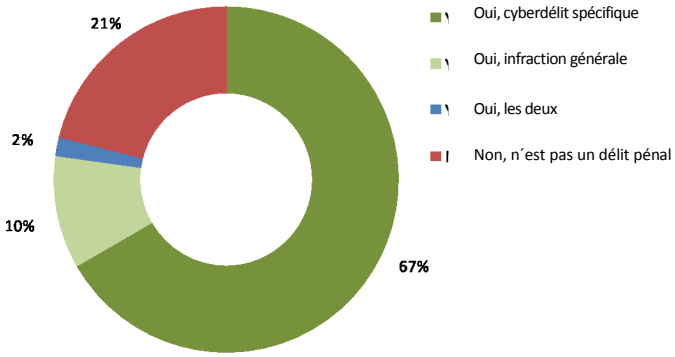
50 Europol, 2011. *Évaluation des menaces (abrégée). Criminalité organisée facilitée par internet*. iOCTA. File n°. : 2530–264. la Hague. 7 janvier.
Disponible sur : https ://www.europol.europa.eu/sites/default/files/publications/iocta.pdf ; Fallmann, H., Wondracek, G. et Platzer, C., 2010. *Sonder clandestinement les marchés de l´économie souterraine*. Laboratoire de systèmes de sécurité de l´Université technique de Vienne. Disponible sur : http ://www.iseclab.org/papers/dimva2010_underground.pdf

51 Voir Fletcher, G., 1978. *Reconsidérer le droit pénal*. Boston : Little, Brown & Co. pp.199-202.

Outils informatiques malveillants

Les logiciels et d´autres outils utilisés pour commettre des délits dans l´environnement numérique, ainsi que les codes d´accès et les mots de passe des victimes, sont devenus des marchandises illicites des marchés clandestins de la cybercriminalité.[50]

Figure 4.16 : incrimination de la production, la distribution ou la possession d´outils informatiques malveillants



Source : questionnaire de l´étude sur la cybercriminalité Q28. (n=57)

L´incrimination de ces « objets du délit » fait face à de nombreuses difficultés, et la frontière floue entre le concept de « préparation » et de « tentative » d´une infraction pénale ainsi que la question des objets à « double usage » pouvant être utilisés à des fins innocentes ou criminelles, ne sont pas les moindres. Il existe cependant des précédents en matière de contrôle de la criminalité « classique » concernant l´incrimination des « outils d´effraction »[51] et des instruments multilatéraux sur la cybercriminalité ont développé des infractions similaires. Le rapport explicatif pour la Convention du Conseil de l´Europe sur la cybercriminalité, signale, par exemple, qu´un des fondements pour l´incrimination des outils informatiques malveillants est de cibler les actes qui précèdent l´infraction tels que le « piratage » et d´éviter la création de marchés clandestins pour ces articles.[52] Afin de prévenir la surincrimination de la possession intentionnelle, ou sans en avoir connaissance, d´outils informatiques malveillants, les instruments régionaux et internationaux exigent généralement l´intention spécifique d´utiliser ces outils pour commettre une infraction.

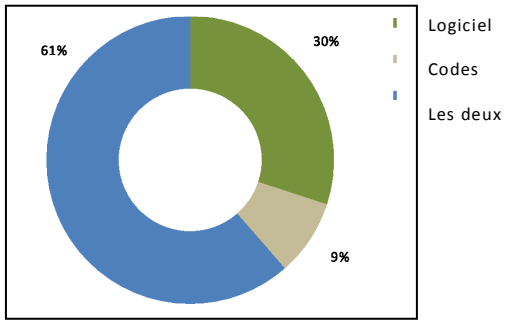
La figure 4.16 montre que plus de la moitié des pays qui ont répondu au questionnaire de l´étude incriminent les outils informatiques malveillants, en utilisant, généralement, à cette fin un cyberdélit spécifique. Près de 20 % des pays répondants n´incriminent pas les outils informatiques malveillants. L´analyse de la source primaire de législation de 70 pays qui n´ont pas de telles dispositions, révèle des approches différentes relatives à l´objet du délit, aux actes couverts et à l´état d´esprit requis.

Objet de l´infraction – les instruments multilatéraux sur la cybercriminalité incluent des dispositions concernant deux types d´outils informatiques malveillants : (i) les logiciels et les dispositifs et (ii) les mots de passe et les codes qui permettent d´avoir accès aux données et aux systèmes informatiques. Neuf instruments multilatéraux sur la cybercriminalité requièrent l´incrimination des logiciels et des codes. Un instrument, toutefois, (l´Accord de la Communauté des états indépendants) requiert l´incrimination de l´utilisation et de la distribution de logiciels malveillants, ce qui exclut le matériel informatique et les codes de l´objet de l´incrimination.[53] Lorsqu´il est utilisé, le terme « dispositif » couvre le matériel informatique ainsi que le logiciel.

Outre les dispositions qui couvrent les outils utilisés pour commettre des cyberdélits en général, certains instruments multilatéraux couvrent aussi des dispositifs et des articles utilisés pour commettre des délits spécifiques. La Décision de l´UE sur la fraude et la contrefaçon des moyens de paiement autre que les espèces inclut l´incrimination des « *instruments, des objets, des programmes d´ordinateur et tout autre procédé destiné à commettre un délit visé à l´article 2(b)* » (contrefaçon ou falsification d´un instrument de paiement dans le

but d´être utilisé frauduleusement) ainsi que les « *programmes d´ordinateur dont le but est d´être utilisés pour commettre un délit visé à l´article 3* » (infractions liées à l´informatique et en particulier la fraude informatique).[54]

Figure 4.17: Types d´outils informatiques malveillants

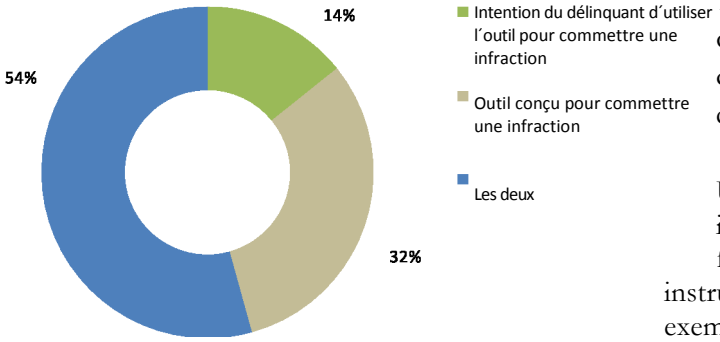


Source: revision de la legislation de l' ONUDC (n=70)

52 Conseil de l´ Europe, 2001. *Rapport explicatif pour la Convention du Conseil de l´Europe sur la cybercriminalité*, ETS n°. 185.
53 Accord de la Communauté des états indépendants, Art. 3(1)(b).

Les approches nationales concernant l´objet des infractions relatives aux dispositifs illégaux sont diverses. La figure 4.17 montre que la majorité des pays examinés incrimine les dispositifs et les codes. Un nombre significatif de statuts nationaux limitent l´incrimination soit aux dispositifs uniquement (30 %) soit aux mots de passe et aux codes uniquement (environ 10 %). Une approche différente de l´objet est utilisée dans d´autres pays qui incriminent la création et la diffusion de virus informatiques plutôt que, ou en plus, les logiciels et les codes. Plusieurs pays incriminent également les actes liés à la possession et la distribution « *d´articles destinés à la fraude informatique* ». 12 des 70 pays examinés comptaient avec des dispositions qui incriminent ce type de dispositifs.

Figure 4.18 : intention requise pour établir une infraction concernant les outils informatiques malveillants



Source : révision de la législation de l´ONUDC. (n=70)

Une autre caractéristique importante de l´infraction est la finalité de l´outil. La plupart des instruments multilatéraux exige, par exemple, que le dispositif ait été essentiellement conçu pour commettre une infraction.

De plus, divers instruments exigent aussi que le délinquant ait l´intention d´utiliser l´outil pour commettre un délit. Deux instruments multilatéraux (le projet de Convention de l´Union africaine et l´Accord de la Communauté des états indépendants) abordent seulement la finalité de l´outil et non l´intention du délinquant. La figure 4.18 monte qu´au niveau national plus de 50 % des pays examinés exigent aussi que l´outil soit essentiellement conçu pour commettre une infraction, et que le délinquant ait l´intention de l´utiliser à cette fin.[55] Certaines approches nationales se concentrent toutefois soit sur la finalité de l´outil, soit sur l´intention du délinquant.

Outils informatiques malveillants : exemple national d´un pays d´Océanie

Infractions informatiques et liées aux télécommunications-

(1) Nul ne devra : ...

(f) intentionnellement, sans droit et avec une intention malhonnête ou illicite, utiliser, posséder, produire, vendre, obtenir pour utilisation, importer, distribuer ou mettre à disposition autrement ou bien tenter d´utiliser, de posséder, de produire, de vendre, d´obtenir pour utilisation, d´importer, de distribuer ou de mettre à disposition un dispositif, incluant sans s´y limiter, un programme informatique, en vue de commettre une infraction établie par les paragraphes (a), (b), (c), (d) ou (e) ;

(g) intentionnellement, sans droit et avec une intention malhonnête ou illicite, utiliser, posséder, produire, vendre, obtenir pour utilisation, importer, distribuer ou mettre à disposition autrement ou bien tenter d´utiliser, de posséder, de produire, de vendre, d´obtenir pour utilisation, d´importer, de distribuer ou de mettre à disposition un code d´accès, un mot de passe ou toute autre donnée informatique similaire permettant d´accéder à la totalité ou à une partie d´un système informatique ou d´un réseau de télécommunications, avec l´intention d´utiliser ce réseau ou ce système pour commettre une infraction établie par les paragraphes (a), (b), (c), (d) or (e) ; ...

(2) toute personne qui agit à l´encontre des dispositions du paragraphe (1) commet une infraction et est passible des peines prévues par la section___.

Actes couverts – les instruments multilatéraux incluent un large éventail d´actes liés aux outils informatiques malveillants, et cela inclut : « *produire* », « *vendre* », « *importer* », « *posséder* », « *distribuer*, « *diffuser* », « *offrir* », « *transférer*, et « *mettre à disposition* » ces outils.

54 Décision cadre de l´UE 2001/413/JAI du 28 mai 2001 (Décision de l´UE sur la fraude et la contrefaçon).
55 Révision de la législation de l´UNODC.

Comme l´illustre la Figure 4.19, l´analyse des lois nationales montre que plus de 80 % des pays incriminent la « diffusion ». La « possession » des outils informatiques malveillants est incriminée dans environ 65 % des pays. Certaines lois nationales incluent aussi l´incrimination d´actes qui ne sont pas prévus par les instruments régionaux ou internationaux mais que l´on peut considérer comme étant concernés par les dispositions sur les outils informatiques malveillants. Plusieurs pays dans la région des Caraïbes incriminent, par exemple, l´acte de « *divulguer sans autorisation* » les mots de passe ou les codes d´accès.

Figure 4.19 : actes concernant les outils informatiques malveillants

Source : révision de la législation de l´ONUDC (n=70)

Spam

On estime que le spam représentait environ 70 % du trafic global de courriels sur internet au milieu de l´année 2012.[56] Le spam concerne la question du consentement plutôt que du contenu. Il est souvent défini comme l´envoi massif de messages non sollicités.[57] Les problèmes causés par le spam vont bien au-delà du simple désagrément causé aux utilisateurs d´internet.[58] Le spam consomme des ressources telles que la bande passante, la capacité du serveur et l´infrastructure du réseau, et représente un point d´entrée pour la propagation de logiciels malveillants et pour l´hameçonnage des codes d´accès et des informations financières. Il est donc lié à des actes d´interférences avec les systèmes et les données – et met en danger directement et indirectement l´intégrité et la disponibilité des systèmes et des données informatiques.

Spam : projet de loi type du COMESA

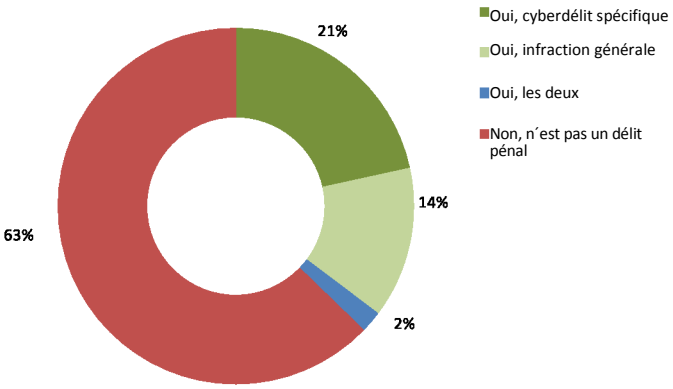
Article 19 – accès non autorisé à des programmes informatiques, des données informatiques, des données relatives au contenu, des données relatives au trafic

...

(g) envoi de spam

Une personne qui transmet des informations électroniques non sollicitées à une autre personne à des fins de commerce illicite ou de toute autre activité illégale commet une infraction pénale sanctionnée par une amende de [montant]_____ et/ou une peine de prison de_____ans

Figure 4.20 : incrimination de l´envoi ou du contrôle de l´envoi de SPAM



Source : questionnaire de l´étude sur la cybercriminalité Q33. (n=51)

56 Rapport de renseignements Symantec, Juin2012 ; rapport de Kaspersky Lab, juin 2012.
57 Pour une définition pratique (plutôt que juridique) voir http ://www.spamhaus.org/consumer/definition/
58 Sorkin, D., 2001. Approches techniques et juridiques concernant le courrier électronique non sollicité. *Revue juridique de l´université de San Francisco*, 35(2) :325
384
59 De Hert, P., Fuster, G., Koops, B. J., 2006. Lutte contre la cybercriminalité dans les deux Europes. La valeur ajoutée de la décision cadre de l´UE et la Convention du Conseil de l´Europe. *Revue internationale de droit pénal* 77(3-4) :503-524.

Néanmoins, l´harmonisation des approches juridiques concernant le spam est loin d´être achevée.[59] Deux instruments multilatéraux (non contraignants) sur la cybercriminalité proposent l´incrimination du spam – le projet de loi type du COMESA (Art. 19), et les textes législatifs types de l´UIT/CARICOM/CTU (Art. 15). Aucun des instruments multilatéraux contraignants sur la cybercriminalité n´inclut de dispositions pénales sur le spam, bien que le préambule de la directive de l´UE stipule que « *il importe d´interdire d´émettre des messages non sollicités à des fins de prospection directe sous une fausse identité, une fausse adresse de réponse ou un faux numéro* ».[60] De plus l´Article 13(3) de cette directive requiert que les états « *prennent les mesures appropriées* » pour veiller à ce que « *sans frais pour l´abonné, les communications non sollicitées par celui-ci et effectuées à des fins de prospection directe* » ne soient pas autorisées sans le consentement de l´abonné. Néanmoins, la directive ne requiert pas explicitement que soit établie une infraction spécifique en conformité avec le droit interne des états membres.

Peines pour les dommages causés à un ordinateur, un système informatique, etc. Si une personne...

(h) à des fins publicitaires relatives à des biens et des services, génère ou cause la génération de courriels non sollicités ou envoie des messages électroniques non sollicités sans la permission de l'émetteur ou de l´abonné ;...
(2) toute personne qui agit à l´encontre des dispositions du paragraphe (1) commet une infraction et est passible des sanctions prévues au paragraphe ___.

Les réponses fournies au questionnaire de l´étude sur la cybercriminalité indiquent que l´envoi de spam est une infraction pénale dans environ un tiers des pays répondants. Les cyberdélits spécifiques et les infractions générales sont utilisées. Une révision de la source primaire des législations permit d´identifier seulement neuf pays sur presque une centaine ayant des dispositions pénales spécifiques relatives au spam. L´*objet* des infractions de *spam* varie des « *messages massifs non sollicités* » à l´incrimination de la falsification des « *en-têtes sou de l´origine des messages* ». Un pays d´Amérique a, par exemple, adopté des dispositions pénales qui sanctionnent la falsification de la ligne mentionnant l´objet du courriel. Il y a, dans certains pay,s des sanctions administratives qui sont imposées à l´envoi ou au contrôle de l´envoi de spam.

La « *transmission* » de multiples courriels non sollicités est l´un des principaux actes incriminés comme spam ainsi que les actes qui induisent en erreur le destinataire du message – comme, par exemple, en manipulant l´en-tête ou les informations relatives à la provenance. En ce qui concerne l´élément mental, le projet de loi type du COMESA exige que l´acte soit intentionnel et soit commis à des fins illicites. Les textes législatifs types de l´UIT/CARICOM/CTU requièrent également l´incrimination des actes intentionnels. Le caractère intentionnel est également requis par les dispositions nationales pouvant être identifiées et analysées.

Bien que le problème du spam ne soit pas explicitement abordé par les instruments internationaux contraignants, de nombreux éléments de la menace que représente le spam, comme les logiciels malveillants et l´hameçonnage, sont couverts par les dispositions régionales et internationales qui protègent l´intégrité, la disponibilité et la confidentialité des systèmes et des données informatiques.

60 Directive de l´UE sur la protection des données, Préambule (43).

61 Sieber, U., 1998. *Aspects juridiques des délits liés à l´informatique dans la société de l´information - étude COMCRIME*. Disponible sur :www.edc.uoc.gr/~panas/PATRA/sieber.pdf.

62 Projet de convention de l´Union africaine, Art. III-26, III-41 ; projet de loi type du COMESA, Art. 24 ; Convention du Conseil de l´Europe sur la cybercriminalité, Art. 8 ; projet de directive de la CEDEAO, Art. 10 ; Décision de l´UEsur la fraude et la contrefaçon, Art. 2 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 12 ; Convention de la Ligue des états arabes, Arts. 10, 11 ; loi type de la Ligue des états arabes, Arts. 10-12).

Contrefaçon et fraude informatiques

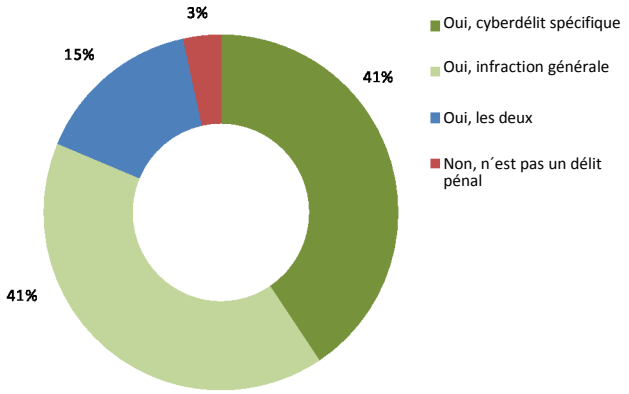
Fraude informatique : Convention du Conseil de l´Europe sur la cybercriminalité

Article 8

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 intérêts juridiques protégés dans des délits contre l´intégrité, la disponibilité et la confidentialité des systèmes et des données informatiques, sont les informations et les données informatiques elles-mêmes. Par contre, les dispositions pénales relatives à la contrefaçon et la fraude informatiques protègent les intérêts relatifs aux biens, aux avoirs financiers et à l´authenticité des documents.[61] Au niveau régional et international, huit instruments comprennent des dispositions sur l´incrimination des fraudes informatiques.[62] Les actes couverts par les instruments sont la manipulation des données informatiques ou l´interférence avec un système informatique, qui procurent des bénéfices économiques au délinquant ou à d´autres personnes.

Figure 4.21 : incrimination de la fraude ou la contrefaçon informatique



Source : questionnaire de l´étude sur la cybercriminalité Q30. (n=59)

Six instruments contiennent aussi des dispositions relatives à la contrefaçon.[63] Les actes couverts par les dispositions relatives à la contrefaçon incluent l´altération, la suppression, la transmission et toute autre manipulation des données informatiques, pour obtenir de fausses données destinées à être traitées ou utilisées comme si elles étaient authentiques.

Contrefaçon informatique : projet de Convention de l´Union africaine Article III – 8

Chaque état membre de l´Union africaine prendra les mesures législatives pour ériger en infraction pénale le fait de produire ou de fabriquer des données numériques en introduisant, en effaçant ou en supprimant les données informatisées contenues, traitées ou transmises par un système informatique, et en obtenant ainsi de fausses données avec intention que ces données soient tenues en compte et utilisées à des fins illicites comme s´il s´agissait de données authentiques.

Cependant, au niveau national, la situation concernant l´existence de dispositions spécifiques sur la fraude et la contrefaçon informatiques varie beaucoup. Les pays qui ont répondu au questionnaire de l´étude ont signalé que la fraude et la contrefaçon informatiques sont couvertes par la législation générale existante (plus de 40 %). Presque la même proportion a mentionné l´existence d´un cyberdélit spécifique et 15 % des pays utilisent les deux approches.[64]

63 Projet de convention de l´Union africaine, Art. III-24 ; Convention du Conseil de l´Europe sur la cybercriminalité, Art. 7 ; projet de loi type du COMESA, Art.23 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 11 ; loi type de la Ligue des états arabes, Art. 4 ; projet de directive de la CEDEAO,Art.8

64 Questionnaire de l´étude sur la cybercriminalité. Q30.

65 Sieber, U., 2008. Maitrise de la complexité dans le cyberespace global : l´harmonisation du droit pénal informatique. *dans* :Delmas-Marty, M., Pieth, M. et Sieber, U., (eds.) *Les chemins de l »Harmonisation Pénale/Harmoniser le droit pénal. Collection de L »UMR de Droit Compare de Paris.* Vol. 15. Paris : Société de législation comparée.

66 *Ibid.*

Cette diversité provient en partie des différences entre les systèmes juridiques nationaux dans la mesure où les infractions « traditionnelles » peuvent être appliquées à un cyber environnement. Par exemple, les infractions de fraudes classiques exigent souvent que la fraude soit commise directement par une « *personne* » et le transposer à des actes commis en manipulant des données ou un système informatique peut être difficile .[65]De même, les infractions classiques de contrefaçon requièrent souvent qu´il y ait une altération d´une « *représentation visuelle* », une exigence qui pourrait, selon l´approche juridique nationale, ne pas être satisfaite avec l´altération de données intangibles sur des dispositifs électroniques [66] Afin de traiter ces difficultés juridiques, les dispositions nationales spécifiques en matière de fraude informatique nationale se basent souvent sur la manipulation des données informatiques avec une intention frauduleuse ou malhonnête, plutôt que sur l´élément de fraude commise par un individu. Dans certains pays, les dispositions relatives à la fraude informatique incriminent aussi l´utilisation non autorisée de données, outre l´utilisation de fausses données (voir l´exemple de l´encadré sur un pays d´Asie du sud). Ceci peut, par exemple, entraîner une application généralisée des dispositions relatives à la fraude informatiques dans tous les cas d´enrichissement illicite lié à l´informatique.[67] De nombreux pays poursuivent la modification de leurs lois nationales, afin d´y introduire des cyberdélits spécifiques concernant la fraude informatique. Par exemple, un pays d´Europe de l´est a adopté, récemment, dans son code pénal, un nouvel article sur la fraude informatique après plus d´une décennie où les cas de fraudes informatiques étaient poursuivis en utilisant des dispositions générales mixtes sur la fraude et l´accès illégal. Même si cette approche avait été soutenue antérieurement, c´est la Cour suprême qui a engagé cette réforme, afin de garantir des poursuites plus efficaces et d´éliminer toute incertitude juridique sur l´applicabilité des dispositions traditionnelles sur la fraude.

Fraude et contrefaçon informatiques : exemple national d´un pays d´Afrique australe

(1) Une personne qui commet l´un des actes mentionnés par la présente partie, afin d´obtenir un avantage illicite en produisant des données contrefaites, dans l´intention qu´elles soient traitées ou considérées comme si elles étaient authentiques, commet une infraction et est passible, si elle est reconnue coupable, d´une amende de ___ et/ou d´une peine de prison de ____.
(2) Une personne qui, dans l´intention d´obtenir un avantage pour elle-même ou pour un tiers, provoque frauduleusement la perte d´un bien d´une autre personne en :
(a) introduisant, altérant, effaçant ou supprimant des données ; ou
(b) en causant une interférence avec le fonctionnement d´un ordinateur ou d´un système informatique,
commet une infraction et est passible, si elle reconnue coupable, d´une amende de ____ et/ou d´une peine de prison de _____.

Contrefaçon informatique : exemple national d´un pays d´Europe du sud

Article --- Contrefaçon informatique
(1) Toute personne qui, sans autorisation, développe, installe, altère, supprime ou rend inutilisable des programmes ou des données informatiques qui sont importants pour les relations juridiques, afin de les utiliser comme s´ils étaient authentiques, ou toute personne qui utilise ces programmes ou ces données sera passible d´une amende ou d´une peine de prison n´excédant pas _____.
(2) Si l´infraction pénale mentionnée au paragraphe 1 du présent Article est commise en relation avec des programmes ou des données informatiques d´un organe gouvernemental, d´une institution publique ou d´une entreprise qui présente un intérêt public particulier, ou bien si des dommages importants ont été causés, l´auteur de l´infraction sera puni d´une peine de prison de---- .

Certains pays appliquent aussi des dispositions sur le vol dans les cas de fraude informatique, car ils considèrent que les données informatiques répondent à la définition de « *biens* » ou de « *choses* ». Cette approche est utilisée par certains pays d´Europe de l´ouest, d´Europe du nord, et d´Amérique du nord. Plusieurs pays ont des dispositions sur le « *vol qualifié* ou le vol simple qui inclut l´utilisation de systèmes informatiques pour commettre l´infraction (voir l´exemple de l´encadré sur un pays d´Asie de l´ouest.

Les dispositions nationales sur la contrefaçon informatique requièrent typiquement deux éléments nécessaires : (i) l´*altération* ou la *manipulation* de données informatiques et (ii) l´intention spécifique d´utiliser les données comme si elles étaient authentiques. Sinon, les pays peuvent élargir la définition de l´objet pour ce qui concerne la contrefaçon classique. De nombreux pays d´Europe

traitent, par exemple, la contrefaçon informatique en élargissant la définition de « *document »,* afin d´y inclure les données informatiques. D´autres pays appliquent à la contrefaçon informatique des dispositions générales sans amender la législation si les dispositions traditionnelles sur la contrefaçon peuvent être interprétées, afin d´y inclure des documents, des signatures et des données numériques.

67 Voir Sieber, U., 1985. *Informationstechnologie und Strafrechtsreform.* Cologne : Carl Heymanns Verlag, p.39.

Infractions concernant l´identité

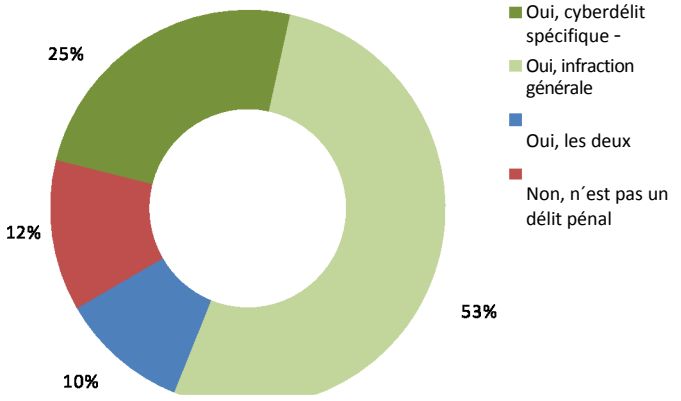
La connectivité globale, l´automatisation du traitement des données et le développement des transactions à distance ont généré des opportunités accrues de vol de données personnelles et de renseignements relatifs à l´identité par le biais des systèmes informatiques.[68] Ces délits visent les renseignements « traditionnels » relatifs à l´identité ainsi que de nouveaux types de renseignements relatifs à l´identité, comme les numéros de cartes de crédit, les renseignements relatifs aux comptes bancaires, les numéros de passeport et de permis de conduire, les adresses IP et les mots de passe des comptes d´internet. Ces informations peuvent faire l´objet de divers actes qui constituent des vols d´identité, ainsi que l´obtention, le transfert et l´utilisation des renseignements relatifs à l´identité. Les données peuvent être obtenues par le biais de l´accès illégal à des systèmes informatiques, en utilisant des logiciels malveillants, par le biais de l´hameçonnage (qui constitue souvent par ailleurs une infraction de contrefaçon informatique) ou avec l´acquisition illégale de données informatiques par le biais des initiés d´une entreprise.

Infractions relatives à l´identité : textes législatifs types de l´UIT/CARICOM/CTU

Article 14

Une personne qui, intentionnellement et sans justification ni excuse légitime ou en les outrepassant, et en utilisant un système informatique à n´importe quelle étape de l´infraction, transfère, possède ou utilise intentionnellement un moyen d´identification d´une autre personne avec l´intention de commettre, ou d´aider ou d´encourager, ou en rapport avec une activité illicite qui constitue un délit, commet une infraction et est passible, si elle est reconnue coupable, d´une peine de prison n´excédant pas […ans] et/ou d´une amende n´excédant pas […].

Figure 4.22 : incrimination des infractions informatiques relatives à l´identité



Source : questionnaire de l´étude sur la cybercriminalité Q31. (n=57)

Il existe de multiples approches pour ce qui concerne les réponses pénales aux actes d´obtention, de transfert et d´utilisation de données relatives à l´identification à des fins criminelles. Au niveau régional et international, il existe un seul instrument (non contraignant) incluant des dispositions relatives au vol d´identité – les textes législatifs types de l´UIT/CARICOM/CTU(Art.14).Cette disposition couvre les actes, commis en utilisant un ordinateur à n´importe quelle étape de l´infraction, impliquant le transfert, la possession ou l´utilisation, sans justification ni excuse légitime, du « *moyen d´identification d´une autre personne* » avec « *l´intention de commettre, ou d´aider ou d´encourager, ou en rapport avec une activité illicite qui constitue un délit* ».

Infraction concernant l´identité : exemple national d´un pays des Caraïbes

Vol d´identité. Article ---

Une personne qui utilise un ordinateur ou fait sciemment en sorte que l´ordinateur exécute une fonction en vue de garantir l´accès à un programme ou à des données contenues dans cet ordinateur ou dans tout autre ordinateur avec l´intention d´usurper ou de voler l´identité d´une autre personne, commet une infraction et est passible, si elle est reconnue coupable, d´une amende de ____ et d´une peine de prison de_____.

68 ONUDC, 2011. *Manuel sur les délits liés à l´identité.* Disponible sur : http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

Au niveau national, les réponses au questionnaire de l´étude fournies par les pays, montrent qu´une proportion des pays relativement faible – 25 % – signale l´existence d´une disposition spécifique pour les infractions informatiques concernant l´identité. Par contre, plus 50 % des pays mentionnent l´utilisation de dispositions générales. Environ 10 % des pays déclarent que les actes relatifs à l´identité ne constituent pas une infraction pénale.

L´analyse des sources primaires de législations montre que, en ce qui concerne les cyberdélits spécifiques concernant l´identité, l´*objet* du vol d´identité est généralement défini comme « *données* » (ou « *données personnelles* ») ou « *renseignements d´identification* ». Lorsque ces dispositions existent, elles ne couvrent pas toujours tous les actes qui peuvent constituer d´éventuels éléments de vol d´identité. Certains pays n´incluent pas, par exemple, le « transfert » des données personnelles et limitent l´incrimination aux actes « d´utilisation » et « d´obtention » des moyens d´identification. D´autres couvrent seulement » l´obtention » ou bien n´incluent ni l´obtention ni l´utilisation (voir l´exemple de l´encadré sur un pays des Caraïbes). Certaines lois nationales vont plus loin et incriminent également la création de fausses données personnelles. En général, l´examen des sources primaires des législations suggère que le nombre de pays ayant des cyberdélits spécifiques concernant l´identité est relativement faible, et parmi ces pays il existe des différences significatives dans les approches. Lorsque les infractions concernant l´identité sont couvertes par des lois générales, de nombreuses dispositions différentes peuvent être appliquées, y compris les dispositions relatives à l´accès illégal, à l´interférence illégale avec les données, aux outils informatiques malveillants, à la contrefaçon et à la fraude informatiques.

Infractions concernant la pornographie infantile

Presque toute les images contenant de la pornographie infantile sont transmises électroniquement, au moyen d´échanges bilatéraux et multilatéraux.[69] Les intérêts protégés par l´incrimination de la pornographie infantile incluent la protection des mineurs contre les abus et l´interruption des marchés d´images de pornographie infantile, qui pourraient encourager les délinquants à produire et à fournir davantage d´images.[70] Au niveau régional et international, neuf instruments identifiés incluent des dispositions qui incriminent les actes liés à la pornographie infantile.[71] Bien que les cadres internationaux présentent plusieurs similarités en matière d´incrimination de la pornographie infantile, il existe aussi des différences relatives à l´objet, l´âge de l´enfant et aux actes couverts.

Pornographie infantile : protocole facultatif à la Convention relative au droit de l´enfant

Article 3

1.Chaque État Partie veille à ce que, au minimum, les actes et activités suivants soient pleinement couverts par son droit pénal, que ces infractions soient commises au plan interne ou transnational, par un individu ou de façon organisée : ...
(c)le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de vendre ou de détenir aux fins susmentionnées, des matériels pornographiques mettant en scène des enfants, tels que définis à l'article 2. ...
3.Tout État Partie rend ces infractions passibles de peines appropriées tenant compte de leur gravité.

Au niveau national, plus de 80 % des pays qui ont répondu au questionnaire de l´étude, ont signalé que la pornographie infantile est une infraction pénale. La majorité des pays a signalé que ces actes sont incriminés par une infraction générale. Étant donné que les actes liés à la pornographie infantile peuvent être commis en utilisant divers médias – y compris des images « hors ligne » – de nombreux pays préfèrent une approche générale « neutre quant aux techniques et aux médias » plutôt qu´une approche spécifiquement informatique. De nombreuses réponses que les pays ont fournies au questionnaire de l´étude suggèrent que la pornographie infantile est incriminée dans le contexte de la pornographie en général. Ceci a été confirmé avec l´analyse des sources de législations, durant laquelle ont été identifiés deux pays qui comptaient avec des dispositions générales sur la pornographie et sur la pornographie infantile. Les pays qui n´ont pas de dispositions spécifiques

relatives à la pornographie infantile peuvent engager des poursuites en utilisant des lois ayant une portée plus large sur l´obscénité ou le matériel offensant.

69 ONUDC, 2010. *La globalisation du crime : évaluation des menaces de la criminalité organisée transnationale chapitre 10.* Disponible sur : http ://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf, p.212.

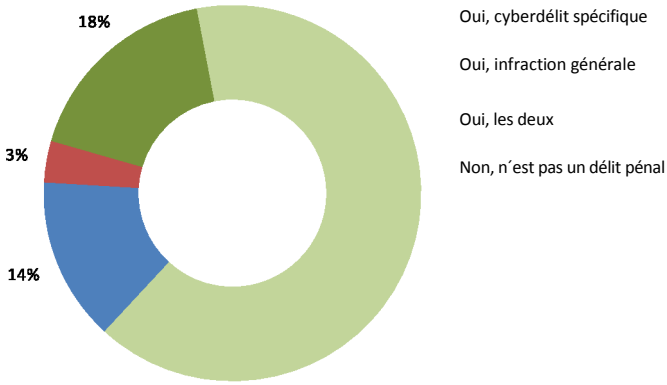
70 Voir Hamilton, M., 2011-2012. La croisade de la pornographie infantile et ses effets d´élargissement du filet. *Cardozo Law Rev,* 33(4) :1679-1732.

71 Projet de Convention de l´Union africaine, Art. III-29 à III-32 ; loi type du Convention du Conseil de l´Europe sur la protection des enfants, Art. 20 ; projet de directive de la CEDEAO, Arts. 14-17 ; Directive de l´UE sur l´exploitation des enfants, Art. 5 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 13 ; Convention de la Ligue des états arabes, Art. 12 ; OP-CRC-SC des Nations Unies, Art. 3.

L´analyse de la législation des pays ayant des dispositions spécifiques relatives à la pornographie infantile montre des similarités ainsi que des différences pour ce qui concerne *objet de l´infraction* et les *actes couverts*.

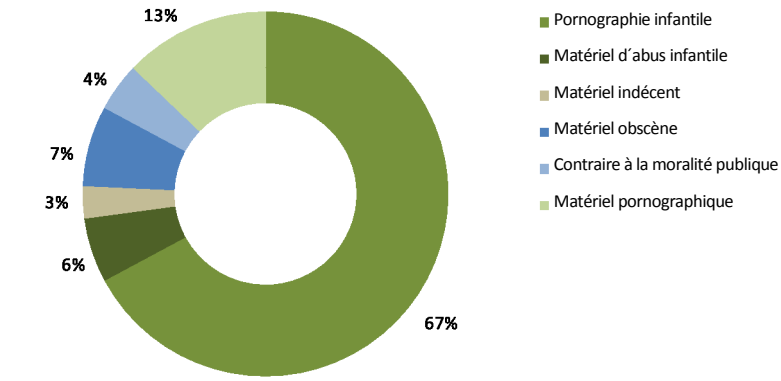
Objet de l´infraction – la plupart des instruments régionaux et internationaux utilise le terme « *pornographie infantile* » pour définir l´objet de l´infraction. La Convention de la Ligue des états arabes utilise le terme « *matériel pornographique mettant en scène des enfants* ». La figure 4.24 montre que la terminologie varie au niveau national. Parmi 70 pays dont les dispositions furent examinées, presque 70 % utilisent le terme « *pornographie infantile* ». Un peu plus de 10 % utilisent « *matériel pornographique mettant en scène des enfants* » ». D´autres variantes sont « *matériel obscène mettant en scène des enfants* » « *matériel illustrant des abus d´enfants,* » « *matériel contraire à la moralité publique mettant en scène des enfants,* » et « *matériel indécent mettant en scène des enfants* ».

Figure 4.23 : incrimination de la production, la distribution ou la possession de pornographie infantile, liées à l´informatique



Source : questionnaire de l´étude sur la cybercriminalité Q36. (n=57)

Figure 4.24 : terminologies utilisées dans les dispositions relatives à la pornographie infantile liée à l´informatique



Source : révision de la législation de l´ONUDC. (n=70)

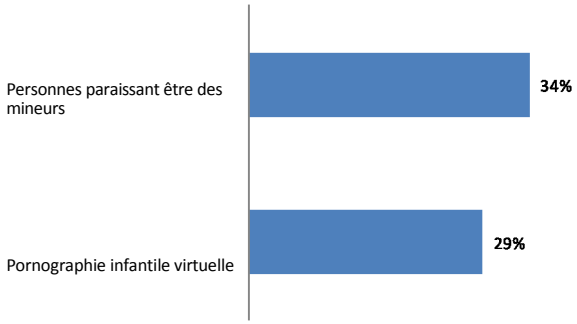
On ne peut pas évaluer à partir des seuls textes législatifs si les différences entre les termes employés se traduisent par des différences pratiques quant au caractère du matériel incriminé. La législation put toutefois définir les médias inclus dans l´infraction. Certains instruments régionaux et internationaux mentionnent, par exemple, le terme « *matériel visuel* » et « *textes* » en se référant à la pornographie infantile. Cependant, définir de cette manière les médias inclus risquerait d´exclure le matériel audio.

Pornographie infantile : exemple national d´un pays d´Europe de l´ouest

Une peine de prison n´excédant pas __ ans ou une amende de ___ sera imposée à toute personne qui diffuse, offre, affiche publiquement, fabrique, importe, transmet, exporte, acquiert ou possède une image – ou un support de données contenant une image – d´un acte sexuel impliquant ou paraissant impliquer une personne âgée de moins de dix-huit ans, ou qui se procure un accès à cette image au moyen d´un système ou d´un dispositif informatique ou par le biais d´un service de communication.

De nombreux instruments (y compris les textes législatifs types de l´UIT/CARICOM/CTU et la Directive de l´UE sur l´exploitation infantile) font référence à « *toute représentation, par n´importe quel moyen* ». La Convention du Conseil de l´Europe sur la cybercriminalité et la loi type du Commonwealth font référence au matériel qui « *illustre visuellement* » la pornographie infantile et en excluant, donc, le matériel audio. Au niveau national la révision des sources de la législation montre qu´environ un tiers des pays examinés limite l´objet de l´incrimination au matériel visuel ou à la représentation visuelle. Les pays restants incluent les textes, les fichiers audio (moins fréquemment) ou font référence à toute représentation quelle qu´elle soit.[72]

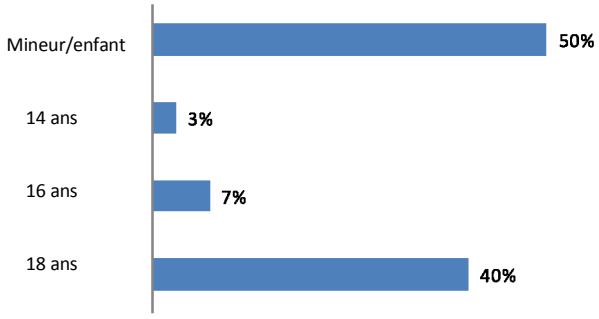
Figure 4.25 : incrimination de la production, la distribution ou la possession de matériel simulé de pornographie infantile, liées à l´informatique



Source : révision de la législation de l´UNODC. (n=70)

Une seconde différence entre les approches juridiques concerne le matériel qui n´implique pas un enfant lors de sa production. Ceci inclut des représentations ou des images réalistes d´un enfant qui n´existe pas ; simulées par ordinateur, ou du matériel impliquant des personnes qui ont atteint l´âge de la majorité (pour ce qui est de l´interdiction concernant la pornographie infantile) mais qui paraissent être des mineurs. La majorité des instruments régionaux ou internationaux inclut ce type de matériel dans le champ de l´incrimination,[73] bien que certains instruments permettent aux pays de ne pas incriminer les images réalistes.[74] Au niveau national, cette approche n´est pas suivie par tous les pays. 34 % des législations des pays examinés couvrent les photos réalistes d´adultes qui « *paraissent être des mineurs*, » ou qui « *impliquent apparemment des mineurs*, » ou qui sont des « *images réalistes de mineurs* ». Seulement 29 % des pays examinés prévoient l´incrimination de la pornographie infantile « *fictive* » ou « *virtuelle* ».

Figure 4.26 : spécifications concernant l´âge des victimes dans les dispositions sur la pornographie infantile liée à l´informatique



Source :révision de la législation de l´UNODC. (n=70)

L´âge des enfants mis en scène dans les représentations pornographiques constitue la troisième différence. L´Article 1 de la Convention des Nations Unies sur les droits des enfants définit un enfant comme un être humain âgé de moins de dix-huit ans. Il inclut toutefois la condition suivante : « sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable ».[75]

72 Révision de la législation de l´ONUDC.

73 Couvert explicitement par : le projet de convention de l´Union africaine, Art. III-1 ; la loi type du Commonwealth, Art. 10 ; .la Convention du Conseil de l´Europe sur la cybercriminalité, Art. 9 ; la Convention du Conseil de l´Europe sur la protection des enfants, Art. 20 ; le projet de directive de la CEDEAO, Art. 1 ; la Directive de l´UE sur l´exploitation infantile, Art. 2(c) ; les textes législatifs types de l´UIT/CARICOM/CTU, Art. 3(4) ; OP-CRC- SC des Nations Unies, Art. 2(c).

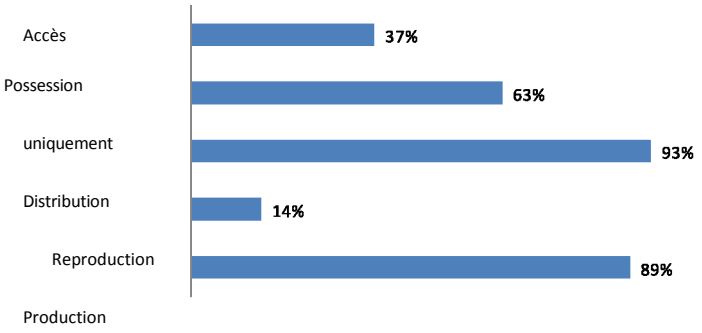
74 La Convention du Conseil de l´Europe sur la cybercriminalité ; la Directive de l´UE sur l´exploitation infantile– quand le matériel est utilisé à des fins de production et ne risque pas d´être diffusé.

75 Convention des Nations Unies relative aux droits des enfants, Art.1.

76 Voir, par exemple, CRC/C/OPSC/MNE/CO/1 (2010) ; CRC/C/OPSA/NOR/CO/1 (2005) ; CRC/C/OPSC/YEM/CO/1 (2009) ;et CRC/C/CUB/CO/2/ (2011).

Bien que les états parties soient en principe libres d´établir une limite d´âge inférieure à 18 ans dans les définitions de la pornographie infantile, le Comité des Nations Unies des droits de l´enfant a recommandé à plusieurs reprises que les définitions couvrent *tous* les enfants âgés de moins de 18 an.[76] D´autres instruments mentionnent des limites d´âge différentes. La Convention du Conseil de l´Europe sur la cybercriminalité spécifie, par exemple, que le terme « *mineur* » devrait inclure toutes les personnes âgées de moins de 18 ans, mais permet que les états parties fixent une limite d'âge inférieure, qui, toutefois, « *ne devra pas être inférieure à 16 ans* ». D´autres instruments, comme la Convention de la Ligue des états arabes ou la loi type du Commonwealth utilisent le terme « *enfant* » ou « *mineur* » sans établir une limite d »âge.

Figure 4.27 : actes constituant des infractions de pornographie infantile



Source : révision de la législation de l´ONUDC (n=70)

Au niveau national il n´est pas simple d´identifier l'âge auquel s´appliquent les dispositions relatives à la pornographie infantile. Plusieurs pays mentionnent le terme « *mineur* » ou « *enfant* » sans spécifier un âge dans l´article. De plus, d´autres parties de la législation nationale mentionnent des âges pertinents – par exemple, la législation relative à la protection de l´enfant ou aux droits de l´enfant. La figure 4.26 montre qu´il n´a pas été possible d´identifier aisément l'âge pertinent en examinant plusieurs dispositions du droit pénal (sans analyser de manière détaillée d´autres parties du droit national). Dans les cas où il a été possible d´identifier un âge dans le droit pénal national, la majorité des dispositions mentionnent l'âge de 18 ans. Dans quelques pays seulement, les lois pénales mentionnent l'âge de 14 ans ou de 16 ans dans le cadre de la définition de la pornographie infantile. À cet égard, le Comité des Nations Unies pour les droits de l´enfant s´est montré particulièrement préoccupé par l´utilisation d´une limite d »âge de 14 ans.[77]

Actes couverts – la majorité des instruments régionaux et internationaux exigent l´incrimination d´un vaste panel d´actions associées à la pornographie infantile, en incluant « *la production* », « *l´offre »,* « *la mise à disposition »*, *« la distribution* », « *la transmission* » et « *la possession* ». Certains instruments incriminent aussi le fait « *d´accéder* » sciemment à la pornographie infantile.[78] Il y a une diversité dans les lois nationales quant aux actes qui y sont inclus. Comme l´illustre la figure 4.27, « *la production* » et *« la distribution* » de pornographie infantile sont les actes les plus souvent incriminés –par environ 90 % des dispositions législatives nationales examinées. Plus de 60 % des pays examinés incriminent la « *possession, »* et presque 40 % incluent des dispositions relatives à l´acte « *d´avoir accès »* à de la pornographie infantile. Dans certains pays, la mesure dans laquelle les dispositions relatives à la « possession » peuvent s´appliquer au visionnage en ligne d´images fixes ou mobiles, n´est pas claire...

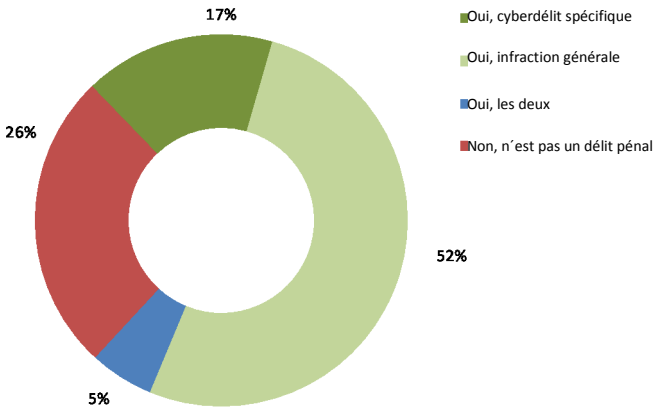
77 Voir, par exemple, CRC/C/OPSC/EST/CO/1 (2010) et CRC/C/OPSC/AUT/CO/1 (2008). Le Comité considère également que l´utilisation de conditions comme « l´intention de diffuser » et « lorsque le mineur ne consent pas » pour des infractions de pornographie infantile impliquant des enfants âgés de14 à 18 ans est incompatible avec le Protocole facultatif à la Convention sur les droits de l´enfant.

78 Le projet de Convention de l´Union africaine ; la Convention du Conseil de l´Europe sur la protection de l´enfant ; la directive de l´UE sur l´exploitation infantile ; les textes législatifs types de l´UIT/CARICOM/CTU.

79 Eneman, M., Gillespie, A. A., Bernd, C. S., 2010. Technologie et abus sexuel : une révision critique des cas de prédation sexuelle sur internet.
ICIS 2010 Procédures. Document 144 ; Kool, R., 2011. Prévention par tous les moyens? Une comparaison juridique de l´incrimination de la prédation sexuelle en ligne et son application. *Revue juridique Utrecht*, 7(3) :46-69.

De nombreux pays d´Europe incluent le visionnage de la pornographie infantile en ligne dans la catégorie de la possession car le visionnage inclut forcément la reproduction d´images dans la mémoire de l´ordinateur et/ou les fichiers cachés internet temporaires. D´autres pays ont créé des solutions telles que l´exigence d'« *activités habituelles* » de la part du délinquant.

Figure 4.28 : incrimination de la sollicitation ou la prédation sexuelle des enfants liées à l´informatique



Source : questionnaire de l´étude sur la cybercriminalité Q37. (n=54)

Sollicitation ou prédation sexuelle des enfants liée à l´informatique

Les lois pénales sur la prédation sexuelle des enfants en ligne représentent une forme d´incrimination des actes préparatoires d´abus sexuel contre les enfants « hors ligne ».[79] Deux instruments multilatéraux, dans la région de l´Europe – la Convention du Conseil de l´Europe relative à la protection des enfants (Art. 23) et la Directive de l´UE sur l´exploitation infantile (Art. 6) – exigent l´incrimination de ces actes. Les éléments essentiels de l´infraction incluent la « *proposition intentionnelle à travers les technologies de communication et d´information,* » formulée par un adulte de « *rencontrer* » un enfant afin de commettre une infraction. Pour que l´infraction soit commise, les deux instruments requièrent aussi qu´il y ait des « actes matériels » conduisant à ladite rencontre.

Prédation sexuelle : exemple national d´un pays d´Europe du sud

Quiconque par internet, par téléphone au moyen de toute autre technologie de l'information et de la communication entre en relation avec un mineur de treize ans et lui propose de fixer une rencontre, afin de commettre l'un des quelconques délits décrits aux articles------, du moment que cette proposition est accompagnée d'actes matériels orientés vers le rapprochement, est puni de la peine de ____ d'emprisonnement ou d'amende de-----,sans préjudice des peines correspondant aux délits commis le cas échéant. Les peines sont prononcées en leur moitié supérieure quand le rapprochement est obtenu au moyen de contrainte, intimidation ou tromperie.

Prédation sexuelle : Convention du Conseil de l´Europe sur la protection des enfants

Article 23 – sollicitation d´enfants à des fins sexuelles

Chaque Partie prend les mesures législatives ou autres nécessaires pour ériger en infraction pénale le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication, et d'»information, une rencontre à un enfant n'ayant pas atteint l'âge fixé en application de l'article 18, paragraphe 2, dans le but de commettre, à son encontre, une infraction établie conformément aux articles 18, paragraphe 1.a, ou 20, paragraphe 1.a, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre.

Au niveau national, les réponses fournies par les pays au questionnaire de l´étude montrent des approches divergentes. Presque 70 % des pays déclarent que la prédation sexuelle est une infraction, bien que la majorité de ces pays utilise une infraction générale plutôt qu´un cyberdélit spécifique. Pour plus de 25 % des pays, cet acte ne constitue pas une infraction pénale.

Une analyse des sources primaires des législations disponibles entraîna l´identification de dispositions spécifiques qui couvrent la sollicitation sexuelle des enfants en ligne dans 17 pays sur 97. Près de la moitié de ces pays se trouve en Europe. Ceci reflète probablement l´influence des dispositions sur la prédation sexuelle de la Convention du Conseil de l´Europe relative à la protection de l´enfant et la Directive de l´UE sur l´exploitation infantile. L´incrimination de la

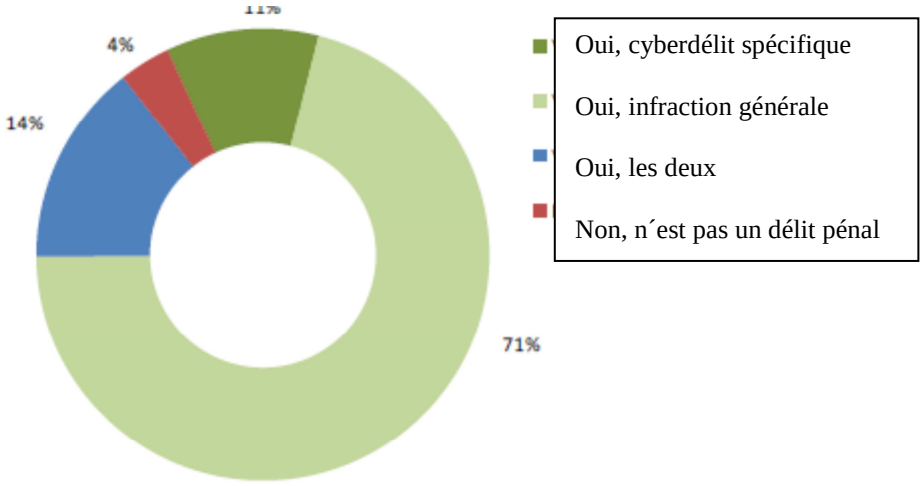
prédation sexuelle a toutefois été identifiée dans certaines lois nationales de pays d´Asie, d´Afrique, d´Amérique et d´Océanie.

80 *Accord sur les aspects commerciaux des droits de propriété intellectuelle (ADPIC)*, adopté le 15 avril 1994.
81 *Traité sur les droits d´auteurs de l´organisation mondiale de la propriété intellectuelle,* signé le 20 décembre 1996.

Infractions concernant les droits d´auteurs et les marques déposées liées à l´informatique

Le cadre international dans le domaine des lois sur la propriété intellectuelle est un peu plus vaste que les instruments régionaux et internationaux sur la cybercriminalité directement pris en compte par la présente étude. Les instruments et les intervenants essentiels sont l´Organisation mondiale du commerce et l´Accord ADPIC,[80] (qui pour la première fois inclut des dispositions au niveau international sur les violations des droits d´auteurs commerciaux), ainsi que le traité sur les droits d´auteurs de l´Organisation mondiale de la propriété intellectuelle (OMPI)[81] et le traité sur les interprétations et les phonogrammes.[82] Plus récemment l´Accord commercial anti-contrefaçon (ACAC) visait à consolider les dispositions pénales sur les contrefaçons délibérées de marques ou de droits d´auteurs ou sur la piraterie à l´échelle commerciale.[83] le Parlement européen a voté contre l´accord en 2012. Au niveau de l´Union européenne de nombreux textes législatifs abordent des aspects des droits d´auteurs et des droits connexes, mais aucun texte n´inclut explicitement des dispositions pénales.[84] En 2005, le Parlement européen a élaboré une proposition pour une décision cadre et une directive sur les mesures concernant des infractions pénales en matière de droits d´auteurs commises à l´échelle commerciale.[85] Cette directive a été révisée en 2006 mais n´a pas encore été adoptée.[86]

Figure 4.29 : incrimination des infractions relatives aux droits d´auteurs et aux marques déposées liées à l´informatique



Source : questionnaire de l´étude sur la cybercriminalitéQ32. (n=55)

Au niveau national les avancées durant la dernière décennie ont été caractérisées par une augmentation des sanctions imposées aux infractions relatives aux droits d´auteurs, en particulier dans le cas des actes commerciaux et organisés. La Convention du Conseil de l´Europe sur la cybercriminalité prévoit, par exemple, l´incrimination de la violation des droits d´auteurs et des actes qui y sont liés s´ils sont « *commis délibérément à une échelle commerciale et au moyen d´un système informatique* ».[87] Au niveau national, les pays qui ont répondu au questionnaire de l´étude sur la cybercriminalité nt signalé un niveau élevé d´incrimination des infractions concernant les droits d´auteurs et les marques déposées, et plus de 80 % des pays ont déclaré que ces actes pourraient être des délits. La majorité de ces pays utilise des infractions générales plutôt que des cyberdélits spécifiques. Dans la pratique la grande quantité de matériel contrevenant sur internet (voir le chapitre deux (la perspective d´ensemble)) signifie souvent que les ressources des services répressifs ne sont pas suffisantes pour poursuivre la multitude de cas possibles. Pour cette raison plusieurs états soutiennent les nouveaux concepts impliquant des mesures de droit civil, tels que les avertissements écrits, les demandes d´indemnisation et le droit à l´information. De plus certains pays ont développé des modèles de « deux fautes » et de « trois fautes ». Ces concepts obligent les fournisseurs de services internet à enregistrer les adresses IP des contrevenants qui violent les droits d´auteurs, à envoyer des avertissements à ceux qui commettent cette infraction pour la première fois et à assumer la

responsabilité de sanctionner les récidivistes ou à collaborer en le notifiant aux autorités ou aux titulaires des droits.[88]

82 *Traité sur les interprétations et les phonogrammes de l´OMPI*, signé le 20 décembre 1996.
83 Voir les Arts. 23 et seq. De *l´Accord commercial anti-contrefaçon (ACAC)*.
84 Sieber, U., Brüner, F.H., Satzger, H., Von Heintschel-Heinegg, B. (eds.) 2011. *Europäisches Strafrecht*, pp.442 et seq.
85 Proposition d´une directive sur les mesures pénales visant à garantir l´application des droits de propriété intellectuelle et la proposition d´une décision cadre pour renforcer le cadre du droit pénal afin de lutter contre les infractions relatives à la propriété intellectuelle du 12 Aout 2005, COM (2005)276 final.
86 Proposition amendée pour une directive sur les mesures pénales visant à garantir l´application des droits de propriété intellectuelle du 26.4.2006, COM (2006) 168 final.
87 Convention du Conseil de l´Europe sur la cybercriminalité Art.10.
88 Voir Bridy, A., 2010. Une réponse nuancée et le tour des ordonnances privées pour appliquer les droits d´auteurs en ligne .*Revue juridique Oregon*, 89 :81-132 ; Stamatoudi, I., 2010. *Application des droits d´auteurs et internet*. Alphen aan den Rijn, Netherlands : Kluwer droit International ; Haber, E., 2011. La Révolution française 2.0 : les droits d´auteurs et la politique des trois fautes. *Harvard Journal of Sports & Entertainment Law,* 2(2) :297-339.

Discussion

L´analyse ci-dessus montre des similarités et des divergences dans les approches nationales d´incrimination de la cybercriminalité. Il est clair que dans certains cas les divergences qui apparaissent au niveau national existent également au niveau international. Les exemples comprennent l´ inclusion, ou non, dans des instruments multilatéraux du fait de « rester illégalement » ; la limitation, ou non, de l´interception des transmissions « non-publiques » ; la possibilité d´incriminer l´interférence « par imprudence » avec le système ou les données ; et l´inclusion, ou l´exclusion, des « codes d´accès » dans les dispositions relatives aux outils informatiques malveillants. Comme cela a été mentionné au chapitre trois (cadres et législation), il est difficile de déterminer l´influence exacte des instruments contraignants et non contraignants sur la législation nationale. Il est possible dans certains cas, qu´un processus fonctionne dans les deux sens– lorsque les approches législatives nationales influencent le développement d´instruments régionaux et internationaux et *vice versa.* Bien que cette analyse puisse être perçue comme étant purement technique, les détails relatifs aux infractions pénales de cybercriminalité sont importants. Comme cela a été mentionné au chapitre sept (coopération internationale), dans certains cas les détails relatifs aux infractions tels que le terme « utilisation de moyens techniques » pour commettre une infraction (dans le cas de l´interception illégal, par exemple) peuvent être considérés comme des *éléments constitutifs* du délit– cela signifie qu´il n´existe aucun délit à moins qu´ils ne soient présents. Dans ces circonstances les détails du délit peuvent avoir un impact sur les exigences de double incrimination et par conséquent sur une coopération internationale efficace.

Par ailleurs, l´analyse détaille révèle de nombreuses bonnes pratiques dans le développement des lois pénales pour les actes de cybercriminalité. Il est important de faire une claire distinction dans les lois nationales entre *accès* illégal à, et l´*interférence* avec des données et des systèmes informatiques afin de veiller à ce que les actes séparés puissent être distingués correctement. L´utilisation des circonstances aggravantes peut être un mécanisme efficace pour adapter les infractions principales aux circonstances nationales particulières, tout en maintenant les infractions basiques qui peuvent être harmonisées avec les normes régionales et internationales. Afin d´éviter une surincrimination, plusieurs pays veillent à ce que les dispositions relatives aux outils informatiques malveillants requièrent que l´outil soit essentiellement conçu pour commettre une infraction, et que le délinquant ait l´intention de l´utiliser à cette fin. Les exigences relatives à l´intentionnalité pour ce qui concerne l´interférence illégale avec les systèmes et les données informatiques sont également importantes afin de garantir que les actes commis par imprudence ou par négligence ne fassent pas l´objet de sanctions pénales disproportionnés.

L´équilibre d´une incrimination appropriée est encore plus difficile quand il s´agit d´infractions liées au contenu informatique que cela ne l´est pour les infractions commises contre la confidentialité, l´intégrité et la disponibilité des systèmes informatiques. Même dans un domaine couvert par les normes internationales comme, par exemple, dans le cas de la pornographie infantile, les approches de l´état montrent des divergences concernant l´inclusion ou l´exclusion de matériel simulé et l »âge de l´enfant protégé. Les lois internationales sur les droits de l´homme sont une des normes externes qui offrent une orientation dans ce domaine. La prochaine section de ce chapitre examine la contribution que cet organisme de droit international peut apporter en aidant les états à trouver un équilibre acceptable entre le contrôle et la prévention de la criminalité et la protection des libertés individuelles.

4.3 Incrimination et lois internationales sur les droits de l´homme

PRINCIPAUX RÉSULTATS :

- l´utilisation accrue des médias sociaux et des contenus internet créés par des usagers a entraîné des mesures de caractère règlementaire de la part du gouvernement, ainsi que l´utilisation du droit pénal et des appels au respect des droits de liberté d´expression
- les pays mentionnent plusieurs limites à la liberté d´expression, concernant la diffamation, les outrages, les menaces, l´incitation à la haine, les insultes aux sentiments religieux, le matériel obscène et les atteintes portées à l´état
- L´élément socio-culturel de certaines limitations se reflète non seulement dans la législation nationale mais également dans les instruments multilatéraux. Certains instruments régionaux contre la cybercriminalité, par exemple, incluent une vaste gamme de délits relatifs à la violation à la moralité publique, au matériel pornographique, et aux valeurs ou aux principes religieux ou familiaux
- Les lois internationales sur les droits de l´homme servent à la fois d´arme et de bouclier, en requérant l´incrimination de formes extrêmes d´expression, alors qu´elles protègent d´autres formes d´expression. Certaines prohibitions sur la liberté d´expression, comme l´incitation au génocide, l´appel à la haine constituant une incitation à la discrimination, l´hostilité ou la violence, l´incitation au terrorisme et la propagande en faveur de la guerre, sont exigées aux états parties aux instruments internationaux pertinents relatifs aux droits de l´homme
- Pour d´autres, la « marge d´appréciation » accorde aux pays de la latitude pour déterminer les limites acceptables de la liberté d´expression en conformité avec leurs propres cultures et traditions juridiques
- Toutefois, le droit international relatif aux droits de l´homme interviendra à un certain moment. Les lois pénales sur la diffamation, les insultes et l´outrage à autorité, par exemple, qui s´appliquent à la liberté d´expression en ligne, feront face à un seuil élevé de limites pour démontrer que les mesures sont proportionnées, appropriées et aussi peu invasives que possible
- Si le contenu est illégal dans un pays mais s´il est légal de de le produire et de le diffuser dans d´autres pays, les états devront se concentrer sur les mesures de justice pénale dans la juridiction nationale à l´encontre des personnes qui accèdent à ce contenu, plutôt que sur un contenu produit hors du pays

Les lois internationales sur les droits de l´homme préconisent et interdisent à la fois l´incrimination en matière de cybercriminalité. La jurisprudence dans le domaine de la liberté d´expression est particulièrement développée et aide les pays à fixer des limites à l´incrimination de l´expression dans des domaines tels que les discours de haine, l´incitation au terrorisme, la diffamation, l´obscénité et les insultes.

Les droits de l´homme servent de « bouclier » et « d´épée »

Il y a plus de 30, le président du Comité des Nations Unies pour le contrôle et la prévention de la criminalité [89] déclarait que « *la criminalité est la définition qu´en donne la loi. La définition par ailleurs doit tenir compte de l´existence et du respect des droits de l´homme et ne pas être seulement l´expression d´un pouvoir arbitraire* ».[90] En d´autres termes, les lois pénales nationales ne doivent pas être exclues de la surveillance exercée par les lois internationales sur les droits de l´homme.[91]

89 Le Comité a été établi par la résolution du Conseil économique et social des Nations Unies en mai 1971. Voir la résolution du Conseil économique et social des Nations Unies 1548(L), 1971.

90 López-Rey, M., 1978. Criminalité et droits de l´homme. *Probation fédérale*43(1) :10-15, p.11.

Avec quelques notables exceptions (comme l´obligation d´ériger en infraction pénale tous les actes de torture et l´interdiction des infractions pénales rétroactives),[92] les lois internationales sur les droits de l´homme ne précisent pas en général les actes qui pourraient constituer des infractions pénales dans la législation nationale.[93]Cependant, la jurisprudence relative aux lois internationales sur les droits de l´homme traite de plus en plus la question de savoir si l´incrimination de certaines conduites est compatible avec, ou même requise par, les droits de l´homme individuels. A cet effet les lois internationales sur les droits de l´homme peuvent agir comme un « bouclier » et une « épée » – en neutralisant ou en déclenchant le droit pénal.[94]

Bien que l´état qui est partie aux traités sur les droits de l´homme ait l´obligation d´établir les lois et les systèmes pénaux suffisants pour dissuader et répondre aux attaques contre les personnes,[95] il ne doit pas en arriver à dénier des droits individuels en incriminant une conduite spécifique.[96] Dans une telle évaluation, les dispositions de droit pénal doivent être examinées sur la base de chaque droit[97] afin de vérifier que leurs contenus ne portent atteinte aux droits individuels – comme le droit de ne pas être l´objet d´une ingérence illégale ou arbitraire dans la vie privée, la famille, le domicile ou la correspondance,[98] le droit à la liberté de pensée, de conscience et de religion,[99] ou le droit de réunion pacifique.[100]

L´acte d´équilibre

Ce type d´évaluation exige généralement que les organismes internationaux de droits de l´homme considèrent soigneusement de nombreux intérêts. Plusieurs dispositions des lois internationales sur les droits de l´homme ne sont pas absolues. Les droits à la liberté de pensée, de conscience, de religion, d´expression et d´association, par exemple, peuvent être soumis à des restrictions (y compris des restrictions de droit pénal)[101] qui sont nécessaires pour de multiples intérêts, incluant la sécurité nationale, la sureté publique, l´ordre public, la protection de la santé ou de la moralité publique, ou la protection des droits et des libertés d´autrui.[102]

Les interférences permises avec les droits de l´homme doivent généralement être : (i) prescrites ou en conformité avec la loi ; (ii)poursuivre des objectifs légitimes ; (iii) être nécessaires dans une société démocratique.[103]

---

91 Aux fins de la présente étude, les droits de l´homme contenus dans le droit international coutumier, les neufs principaux traités internationaux sur les droits de l´homme et leurs protocoles, ainsi que les traités de trois mécanismes régionaux sur les droits de l´homme et les interprétations faisant autorité de ces instruments par le biais de mécanismes établis à des fins de promotion et de mise en œuvre, sont considérés comme la principale expression des « lois internationales sur les droits de l´homme ». Y compris : ICCPR ; ICESCR ; ICERD ; CEDAW ; CAT ; CRC ; ICRMW ; CPED ; et CRPD. De plus les protocoles facultatifs de ICESCR, ICCPR, CEDAW, CRC, CAT, et CRPD couvre des domaines comme l´abolition de la peine de mort (ICCPR-OP2), l´implication des enfants dans des conflits armés (OP-CRC-AC), ainsi que la vente des enfants, la prostitution et la pornographie infantiles (OP-CRC-SC) (également mentionné comme instrument sur la « cybercriminalité » dans cette étude). Au niveau régional cela inclut : EHCR et ses 15 protocoles, y compris ceux sur la protection des biens et le droit à l´éducation, la liberté de circulation, l´abolition de la peine de mort, et une interdiction général de discrimination, l´ACHR en Amérique et l´ ACHPR en Afrique. Il n´y a jusqu´à présent aucune convention sur les droits de l´homme en Asie.

92 CAT, Art. 4, et ICCPR, Art. 15(1).

93 Il faut toutefois signaler que les lois internationales sur les droits de l´homme exigent la réparation des violations des droits de l´homme et cela peut impliquer la promulgation de lois pénales appropriées suffisantes pour dissuader et répondre à certaines violations.

94 Tulkens, F., 2011. Les relations paradoxales entre le droit pénal et les droits de l´homme. *Journal de la justice pénale internationale,* 9(3) :577-595.

95 Voir, par exemple, ECtHR. Demande n° 23452/94. 28 octobre 1998, dans laquelle le tribunal jugea que le droit à la vie (ECHR, Article 2(1)) incluait l´obligation de mettre en place *« des dispositions efficaces de droit pénal pour dissuader de commettre des infractions contre la personne en s´appuyant sur un mécanisme d´application conçu pour prévenir, supprimer et sanctionner les violations de ces dispositions »*

96 Commission des Nations Unies sur les stupéfiants et la Commission sur la justice pénale et la prévention de la criminalité, 2010. *Les drogues, la prévention du crime et la justice pénale envisagés dans l´optique des droits de l´homme.* Note du directeur exécutif E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1. 3 mars 2010.

97 *Ibid.*

98 ICCPR, Art. 17.

99 ICCPR, Art. 18.

100 ICCPR, Art. 21.

101 La Cour européenne des droits de l´homme a jugé que l´ existence de l´interdiction pénale d´une conduite déterminée peut être suffisante pour s´immiscer continuellement avec les droits de l´homme dans ce cas, le droit à la vie privée) même s´il existe une politique cohérente de ne pas procéder à des poursuites pénales. Voir ECtHR. Demande n° 15070/89. 22 avril 1993.

102 Voir, par exemple, ICCPR, Art. 21.

103 Voir, par exemple, les formulations utilisées dans ECHR, Arts. 8-11.

104 ECtHR. Demande n° 5493/72. 7 décembre 1976.

105 pour une révision générale voir Legg, A., 2012. *La marge d´appréciation des lois internationales sur les droits de l´homme.* Oxford : Oxford Monographies sur le droit international.

Dans le contexte européen, pour déterminer la question de la nécessité, la ECtHR évalue si l´interférence est *proportionnelle* à un « besoin social impérieux » identifié.[104] À cet effet une « marge d´appréciation » est accordée à l´état.[105] La marge dépend du contexte – en particulier pour ce qui concerne la nature des droits en cause et l´objectif que l´interférence en question cherche à poursuivre.

Cybercriminalité – droit pénal et droits de l´homme

L´effet de « bouclier » et « d´épée » des lois internationales sur les droits de l´homme s´applique également à l´incrimination des actes de cybercriminalité. La « cybercriminalité » représentés un vaste domaine d´incrimination– incluant des actes contre la confidentialité, l´intégrité et la disponibilité des systèmes ou des données informatiques, des actes commis pour un profit personnel ou financier, ou pour porter préjudice liés à l´informatique, et les actes liés au contenu informatique. Certaines de ces dispositions pénales peuvent mettre en cause les obligations des lois internationales sur les droits de l´homme dans une plus grande mesure que d´autres.

Les délits liés au contenu informatique notamment, peuvent impliquer les droits fondés sur les traités comme le droit à la liberté d´expression,[106] les droits concernant les biens,[107]et les obligations positives des états qui garantissent la sécurité de la personne et la protection contre le préjudice physique.[108] Le contenu disponible sur internet est en principe soumis au même régime des droits de l´homme que les médias traditionnels, comme dans le cas des discours et des contenus imprimés. La résolution 20/8 du Conseil des Nations Unies des droits de l´homme stipule que « *les mêmes droits dont jouissent hors ligne les personnes doivent être protégés en ligne, en particulier la liberté d´expression, qui est applicable sans considération de frontières et quel que soit le moyen choisi ».*[109]

Toutefois, le contenu en ligne a des caractéristiques particulières – y compris le fait que l´impact et la durée des informations peuvent être multipliés lorsque le contenu est placé sur internet, que le contenu est facilement accessible aux mineurs, et que le développement des médias sociaux et le contenu internet créé par les usagers ont commencé à remettre en question les monopoles traditionnels de l´information.[110] Par conséquent l´interprétation des dispositions sur les droits de l´homme doit tenir compte du caractère spécifique d´internet en tant que vecteur de diffusion de l´information.[111]

La cybercriminalité et le droit à la liberté d´expression

L´importance de la liberté d´expression sur internet a été souligné lors de nombreux cas récents très médiatisés, et par le biais du travail effectué par les mécanismes sur les droits de l´homme au niveau régional et international.[112]

106 ICCPR, Art. 19 ; ECHR, Art. 9 ; ACHR, Art. 13 ; ACHPR, Art. 9.
107 ECHR, Protocole 1, Art. 1 ; ACHR, Art. 21 ; ACHPR, Art. 14.
108 ICCPR, Arts. 7 et 17 ; ECHR, Arts. 3 et 8 ; ACHR, Arts. 5 et 11 ; ACHPR, Art. 5.
109 Conseil des Nations Unies sur les droits de l´homme, 2012. Résolution 20/8 sur la *promotion, la protection et la jouissance des droits de l´homme sur internet,*A/HRC/RES/20/8, Conseil des Nations Unies sur les droits de l´homme, 2012. *Résumé de la réunion-débat du Conseil des droits de l´homme sur la promotion et la protection de la liberté d´expression sur internet. Rapport du haut commissariat des Nations Unies aux droits de l´homme,* A/HRC/21/30, 2 juillet 2012.
111 ECtHR, Division de la recherche, 2011. *internet : jurisprudence de la Cour européenne des droits de l´homme.*
112 Voir, par exemple, le rapporteur spécial des Nations Unies sur la liberté d´opinion et d´expression, le représentant de l´OSCE pour la liberté des médias, le rapporteur spécial de l´OEA sur la liberté d´expression, et le rapporteur spécial de la CADHP sur la liberté d´ expression et l´accès a l´information. Déclaration conjointe sur la liberté d´expression et internet. disponible sur http ://www.osce.org/fom/78309
113 Questionnaire de l´étude sur la cybercriminalité Q20.

Durant la collecte des informations, on demanda aux pays comment la liberté d´expression sous forme électronique était protégée par la loi, et de spécifier si, et dans quelles circonstances, la liberté d´expression pouvait être restreinte à des fins de prévention ou de lutte contre la cybercriminalité. Presque tous les pays qui répondirent à cette question (environ 50 pays) déclarèrent que la liberté d´expression était en général protégée– généralement par le droit constitutionnel– et que cette protection s´appliquait de façon égale à l´expression électronique et non-électronique.[113] De nombreux pays mentionnèrent également des lois sur « l´information », des lois sur « la presse et les publications », des lois sur « l´audio-visuel », et des lois sur « les médias » qui contenaient des protections pertinentes.[114]

Liberté d´expression sur internet – exemple

En novembre 2011, la Cour européenne de justice (ECJ) a statué
fournisseurs de service internet ne seraient pas tenus de filtrer le cor
des fins concernant les droits d´auteurs, car cela violerait les droits rela
vie privée et à la liberté d´expression des abonnés. Selon la Cou
injonction non seulement enfreindrait la directive de l´UE sur le cor
électronique, mais aussi '*enfreindrait les droits fondamentaux des clients des fou
de services, notamment les droits relatifs à la protection des données personnelles
liberté de recevoir ou de transmettre des informations...[], une injonction r
l´installation d´un système de filtrage impliquerait l´analyse systématique de tout le
ainsi que la collecte et l´identification des adresses IP des usagers auxquels est
contenu illicite du réseau. En second lieu, cette injonction pourrait potentiellement
liberté d´information car ce système ne pourrait pas distinguer de manière adéquate
contenu licite et le contenu illicite, et ceci donnerait lieu au blocage des communicatio*
Une entreprise qui représentait des créateurs d´œuvres musicales et au
des tierces parties à utiliser leur matériel protégé par des droits d´auteu
engagé des poursuites à l´encontre d´un fournisseur de services qui per
d´accéder à internet sans offrir d´autres services tels que les télécharg
ou le partage de fichiers. Cette entreprise avait demandé que le fournis
services contrôle et bloque les transferts de fichiers P2P concer
matériel créé par les clients européens qu´elle représentait.

Source: ECJ Cas No. C-70/10

Pour ce qui concerne les limitations à la liberté d´expression, les pays répondants mentionnèrent une vaste gamme de possibles restrictions. Celles-ci incluaient des limitations génériques incluses dans les lois internationales sur les droits de l´homme, telles que la protection de la « sécurité nationale », « la sureté publique et la prévention des troubles et des crimes, » « l´ordre public, » « la santé publique, » et la « moralité publique ». Elles incluent aussi des limitations plus spécifiques, telles que « la violation de la confidentialité, » le « privilège juridique, » la « diffamation, » les « menaces contre les personnes ou les biens, » « incitation au crime, » « l´aide matérielle au terrorisme, » « la propagande en faveur de la guerre, » « l´incitation au génocide, » « l´incitation à la haine raciale, religieuse ou nationale, » « les insultes aux sentiments religieux, » « l´outrage, la calomnie ou la diffamation des religions protégées, » « le matériel qui met en risque les relations harmonieuses entre les peuples, les castes, les tribus et les communautés, » « l´obscénité, » « la pornographie, » « porter atteinte au prestige de l´état ou saper la confiance dans sa situation financière, » et « la divulgation de secrets officiels ».[115]

De nombreux pays mentionnèrent des lois régionales et internationales comme étant la source de certaines de ces limitations, et cela incluait la décision cadre du Conseil de l´Europe contre le racisme et la xénophobie,[116] et le protocole de la Convention du Conseil de l´Europe sur la cybercriminalité.[117] D´autres pays mentionnèrent seulement des lois nationales. Certains pays fournirent des informations sur la manière dont la légitimité des limitations est déterminée.[118] Toutefois, la plupart des pays ne fournit pas d´informations sur l´approche utilisée pour déterminer la légitimité des restrictions de la liberté d´expression. Certains pays ont clairement indiqué que les limitations spécifiques à la liberté d´expression provenaient des interdictions pénales. Mais en général les pays répondants ne spécifièrent pas si les limitations étaient de caractère pénal, administratif ou civil.

114 *Ibid.*

115 *Ibid.*

116 La décision cadre du Conseil de l´Europe 2008/913/JHA du 28 novembre 2008 sur la lutte contre certaines formes et expressions de racisme et de xénophobie au moyen du droit pénal, OJ L 328 du 6 décembre 2008.

117 Les articles 3 à 6 du protocole de la Convention du Conseil de l´Europe sur la cybercriminalité exigent que les états parties adoptent ces mesures législatives et toute autre mesure nécessaire pour ériger en infraction pénale la diffusion par le biais de systèmes informatiques, de menaces, d´insultes et de matériel raciste et xénophobe, ainsi que la diffusion de la négation, de la minimisation grossière, de l´approbation ou de la justification de génocides ou de crimes contre l´humanité,.

118 Un pays d´Afrique a, par exemple, déclaré que « *les droits de la Charte des droits ne peuvent être limités que par une loi d´application générale dans la mesure où la limitation est raisonnable et justifiable dans une société ouverte et démocratique basée sur la dignité humaine, l´égalité et la liberté, en tenant compte de tous les facteurs pertinents, y compris – (a) la nature du droit ; (b) l´importance de l´objectif de la limitation ; (c) la nature et la portée de la limitation ; (d) la relation entre la limitation et son objectif ; et (e) les moyens les moins restrictifs pour atteindre cet objectif ».* questionnaire de l´étude sur la cybercriminalitéQ20.

Limitations de la liberté d´expression et droit international

Certaines limitations à la liberté d´expression citées par les pays répondants bénéficient d´un important soutien des lois internationales sur les droits de l´homme. Au degré le plus extrême, la fonction « d´épée » des lois internationales sur les droits de l´homme *exige* l´interdiction de certaines formes d´expression (limitées). Le rapporteur spécial des Nations Unies pour la promotion et la protection du droit à la liberté d´opinion et d´expression, identifie quatre formes d´expression qui doivent être interdites par les lois internationales : la pornographie infantile ;[119] l´incitation directe et publique à commettre un génocide ;[120]la promotion de la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l´hostilité ou à la violence ;[121]et l´incitation au terrorisme.[122] Le rapporteur spécial pourrait aussi avoir ajouté la propagande en faveur de la guerre.[123] Comme cela est mentionné ci-après, d´autres limitations à la liberté d´expression bénéficient de moins d´appui des lois internationales sur les droits de l´homme.

Incrimination requise par les lois internationales sur les droits de l´homme
ICCPR, Article 20(2), ICERD, Article 4, et ACHR, Article 13 Tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à[la discrimination, l´hostilité ou la violence (ICCPR)]/[la violence anarchique ou à toute autre action analogue (ACHR)]/[la discrimination raciale, ou à des actes de violence contre une race ou un groupe de personnes d´une autre couleur ou origine (ICERD)] sera [interdit par la loi (ICCPR)] [considéré comme une infraction punissable par la loi (ACHR et ICERD)]
OP-CRC-SC, Article 3 Produire, distribuer, diffuser, importer, exporter, offrir, vendre ou posséder de la pornographie infantile aux fins susmentionnées sera entièrement couvert par le droit pénal ou criminel, que ces infractions soient commises au plan interne ou transnationalpar un individu ou de façon organisée
ICCPR, Art 20(1) et ACHR, Article 13 Toute propagande en faveur de la guerre [sera interdite par la loi (ICCPR)]/[sera considérée une infraction punissable par la loi (ACHR)]
Incrimination acceptable en conformité avec les décisions sur les droits de l´homme
ECtHR demande No 5446/03 La Cour considéra qu´une condamnation pour une publication de matériel sur internet qui constituait un acte d´obscénité ne violait pas le droit à la liberté d´expression, même si le matériel pouvait être légal dans le pays tiers où le site internet site était opéré et contrôlé. Le requérant ne contesta pas que le matériel était obscène conformément à la loi, et la Cour jugea que l´ingérence était proportionnée, et tenait compte de la nature commerciale du site internet.
ECtHR demande No 10883/05 La Cour considéra qu´une condamnation pour des déclarations publiées par le maire de la ville sur le site web du conseil municipal qui constituaient un acte d´incitation à la discrimination nationale, raciale ou religieuse ne violait pas le droit à la liberté d´expression. Les déclarations appelaient au boycott des produits d´un tiers état. La Cour jugea que l´ingérence étaitsuffisante et pertinente relevant et tenait compte de la charge publique occupée par le requérant.
Incrimination non requise en conformité avec les décisions sur les droits de l´homme
ECtHR demande No 31358/03 Le pays répondant n´était pas tenu d´enquêter sur une plainte présentée a la to présentée à la police concernant la réception de SPAM non sollicité au contenu pornographique, si les lois pénales existantes ne couvraient pas cette conduite

Le tableau présente de nombreux cas et dispositions concernant les droits de l´homme, en fonction du résultat– c´est à dire si l´incrimination est *requise*, *acceptable*, *non requise*, ou potentiellement *incompatible* avec les lois internationales sur les droits de l´homme. Le tableau souligne que–du moins d´après la jurisprudence internationale disponible– les états peuvent légitimement restreindre la liberté la liberté de parole pour ce qui concerne les discours de haine et l´obscénité. D´autre part les restrictions qui sont trop générales, qui manquent de certitude juridique, ou qui freinent les débats pluralistes peuvent être incompatibles avec les normes internationales sur les droits de l´homme. Dans ce contexte les lois internationales sur les droits de l´homme font office de *bouclier*– et préviennent une surincrimination.

119 Nations Unies OP-CRC-SC, Art. 3.
120 Convention sur le génocide, Art. 3 ; Statut de Rome, Art. 25(3)(e) ; Statut de la cour pénale internationale pour l´ancienne Yougoslavie,Art. 4(3)(c) ; Statut de la cour pénale internationale pour le Rwanda, Art. 2(3)(c).
121 ICCPR, Art. 20(2).
122 Résolution du Conseil de sécurité des Nations Unies1624 (2005), Para 1.S/RES/1624 (2005), 14 septembre 2005.
123 ICCPR, Art. 20(1).
124 Il faut signaler que l´article 20 de l´ ICCPR ne *requiert* pas l´incrimination mais l´interdit en vertu de la loi. L´ACHR et l´ICERD, par ailleurs, exigent que cette incitation soit considérée une infraction punie par la loi.

Discours de haine

Au niveau international, l´article 20 de l´ICCPR stipule que « *tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, l´hostilité ou la violence sera interdit par la loi aw ».*[124] lorsqu´on leur posa la question sur l´incrimination des actes liés à l´informatique impliquant du racisme ou de la xénophobie, trois quarts des pays répondants signalèrent qu´il existait à cet effet des infractions pénales pertinentes. Les pays restants ne considéraient pas ces actes comme un délit.[125]

Lorsque ces actes étaient incriminés, la majorité des infractions étaient classifiées comme générales plutôt que comme des cyberdélits ». Dans ce domaine les approches de l´incrimination montraient une grande diversité. Certains pays avaient des infractions qui couvraient l´incitation à la haine raciale *et* religieuse, alors que d´autres couvraient seulement les questions raciales ou ethniques.[126]Les postures vont des étroites limitations concernant seulement les discours destinés à « créer la peur de futurs préjudices, » jusqu´à la vaste incrimination couvrant le fait de « formuler des remarques insultantes » sur un groupe de personnes pour un motif de race, de religion ou de croyance, de sexe, d´orientation sexuelle ou de handicap.[127]

Limite de l´incrimination en conformité avec les décisions sur les droits de l´homme
ECtHR Demande No 13290/07 La Cour considéra que la condamnation pénale pour diffamation d´un fonctionnaire public concernant des commentaires publiés sur un site web sur les décisions prises par ce fonctionnaire représentait une ingérence disproportionnée avec le droit à la liberté d´expression. La Cour déclara que les fonctionnaires élus devaient être particulièrement tolérants envers les critiques qui leur sont dirigées et les excès verbaux qui y sont associés.
UN-HRC Communication CCPR/C/103/D/1815/2008 Le Comité conclut que la condamnation pour diffamation d´un radiodiffuseur constituait une restriction illégitime du droit à la liberté d´expression. Le Comité souligna que ces lois devraient inclure la défense de la vérité et ne devraient pas être appliquées à des expressions qui ne pourraient pas faire l´objet d´une vérification.
ECtHR Demande 2034/07 La Cour considéra qu´une condamnation pénale pour de 'graves insultes contre le Roi' représentait une ingérence disproportionnée avec le droit à la liberté d´expression et signala qu´une telle sanction, de par sa nature, aurait inévitablement un effet inhibant.
UN-HRC Communication CCPR/C/85/D/1180/2003 Le Comité conclut que la condamnation du requérant pour insulte criminelle publiée dans un article sur le chef d´un parti représentait une ingérence disproportionnée avec le droit à la liberté d´expression. Le Comité souligna que dans le cas de personnalités de la sphère politique, le Pacte accordait une grande valeur à la liberté d´expression.
ECtHR Demande 27520/07 La Cour considéra qu´une condamnation pour 'dénigrer la nation, la république, la grande assemblée nationale, le gouvernement de la république ou les organes judiciaires de l´état' représentait une ingérence disproportionnée avec le droit à la liberté d´expression et signala que le terme était trop vague et trop ample et ne permettait pas aux individus de régler leur conduite ou de prévoir les conséquences de leurs actes.
ECtHR Demande 35071/97 La Cour considéra qu´une condamnation pour 'incitation à la haine ou à l´hostilité pour un motif de classe sociale, de race, de religion, de culte ou de région' concernant des commentaires qui critiquaient les principes démocratiques et appelaient à introduire la loi de la Sharia représentait une ingérence disproportionnée avec le droit à la liberté d´expression et souligna que les commentaires étaient formulés dans le contexte d´un débat pluraliste.

125 Questionnaire de l´étude sur la cybercriminalité Q35.

126 Haut commissariat des Nations Unies aux droits de l´homme, 2012. *Plan d´action de Rabat relatif à l´interdiction de l´apologie de la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, l´hostilité ou la violence.* Conclusions et recommandations des quatre ateliers régionaux d´experts organisés par l´OHCHR, en 2011, et adoptées par les experts à Rabat, Maroc le 5 octobre 2012.

127 OSCE, 2011. *Liberté d´expression sur internet : une étude des pratiques et des dispositions juridiques relatives à la liberté d´expression, à la libre circulation de l´information et à la pluralité des médias sur internet dans les états membres de l´OSCE ;* et Halpin, S., 2010. Discours de haine raciale : une analyse comparative de l´impact des lois internationales sur les droits de l´homme sur le droit du Royaume Uni et des États-Unis. *Revue juridique Marquette,* 94(2) :463-497.

128 Voir, par exemple, http ://www.bbc.co.uk/news/world-middle-east-19606155 ethttp ://www.bbc.co.uk/news/uk-england-gloucestershire-20560496

129 Haut commissariat des Nations Unies aux droits de l´homme, 2012. *Plan d´action de Rabat relatif à l´interdiction de l´apologie de la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination,l ´hostilité ou la violence.* Conclusions et recommandations des quatre ateliers régionaux d´experts organisés par l´OHCHR, en 2011, et adoptées par les experts à Rabat, Maroc le 5 octobre 2012

L´augmentation de l´utilisation des médias sociaux a causé de nombreux cas récents sur internet qui soulèvent des questions de discours de haine, de vidéos au contenu anti-islamique et des messages de Twitter incitant au racisme.[128] Alors que l´article 20 de l´ICCPR impose l´obligation de combattre ce type d´expression, il est important de signaler que l´article 20 de l´ICCPR exige un seuil élevé. Les restrictions doivent satisfaire les rois conditions du critère de légalité, proportionnalité et nécessité. Lors de l´évaluation de la gravité de l´incitation à la haine – et donc la justification pour restreindre la liberté d´expression – une évaluation du seuil devrait inclure : (i) le contexte de la déclaration ; (ii) la position ou le statut de l´énonciateur ; (iii) l´intention (la négligence et l´imprudence ne devraient pas être suffisants) ; (iv) le contenu ou la forme de la déclaration (v) la portée de la déclaration ; et (vi) le niveau de risque du préjudice résultant.[129] Les principes non contraignants soulignent que les termes « haine » et « hostilité » utilisés dans l´article 20 de l´ICCPR font référence à « *des émotions intenses et irrationnelles d´opprobre, d´hostilité ou d´inimitié envers le groupe visé* ».[130] Au niveau européen la ECtHR souligne qu´il doit exister une réelle et grave incitation à l´extrémisme, et non simplement des idées qui offensent, choquent ou perturbent les autres personnes.[131]

Discours de haine : exemple national d´un pays d´Europe de l´ouest

Incitation à la haine
(1)Quiconque, d'une manière pouvant troubler la paix publique :
1. incite à la haine des parties de la population ou qui provoque des actes violents ou arbitraires contre eux, ou qui
2. attaque la dignité humaine d'autres personnes en insultant, en avilissant de manière mal intentionnée ou en diffamant des parties de la population d'une manière pouvant troubler la paix publique, sera puni d'emprisonnement de trois mois à cinq ans.

(2) Quiconque :
1. en ce qui concerne les ouvrages incitant à la haine des parties de la population ou d'un groupe national, racial, religieux ou ethnique, provoquant des actes violents ou arbitraires contre eux ou attaquant la dignité humaine des autres en insultant, en avilissant de manière mal intentionnée ou en diffamant des parties de la population ou un tel groupe :
(a) distribue ;
(b) expose, affiche, présente ou rend publiquement accessible ;
(c) offre à un mineur, lui laisse ou rend accessible ;
(d) produit, fait venir, livre, stocke, offre, annonce, préconise, entreprend d'importer ou d'exporter ces ouvrages, afin de les utiliser en tout ou en partie dans le sens des sous-paragraphes (a) à (c) ; ou

2. celui qui diffuse par la radio, les services de médias ou de télécommunications une présentation ayant un contenu énoncé au No 1sera passible d´une peine de prison n´excédant pas trois ans ou d´une amende. ..

Quand il s´agit de « haine religieuse, » en particulier, le Comité des Nations Unies pour les droits de l´homme souligne que les interdictions de montrer « un manque de respect envers une religion ou un autre système de croyance, y compris les lois sur le blasphème » sont incompatibles avec l´ICCPR, sauf dans les circonstances spécifiques prévues par l´article 20 de l´ICCPR 0.[132] Le Comité signale qu´il ne serait pas permis que les interdictions soient utilisées pour « *prévenir ou punir les critiques envers les dirigeants religieux ou les commentaires sur la doctrine religieuse et les dogmes de foi* ».[133]

Incitation au terrorisme

De nombreux instruments au niveau régional et international appellent les états à interdire l´incitation au terrorisme– en utilisant des termes tels que « la provocation publique à commettre une infraction terroriste » ou « l´incitation à commettre un acte terroriste ».[134] Lorsqu´on leur demanda sur quelles infractions s´appuyait l´incrimination du terrorisme (en incluant l´acte « d´incitation au terrorisme » lié à l´informatique), presque 90 % des pays déclarèrent qu´il existait à cet effet des infractions pertinentes. Lorsque ces actes étaient incriminés, environ 80 % des pays dirent qu´une « infraction générale » était utilisée. Seulement 15 % des pays mentionnèrent l´existence de cyberdélits spécifiques concernant le terrorisme et 5 % des pays dirent utiliser des infractions générales et des cyberdélits spécifiques.[135]

130 Article 19. 2009. Les principes de Camden sur la liberté d´expression et l´égalité. Principe 12.
131 Conseil de l´Europe, 2012. *Fiche d´information – discours de haine.*
132 Comité des Nations Unies sur les droits de l´homme, 2011. *Commentaire général n°. 34.* Article 19. Liberté d´opinion et d´expression. CCPR/C/GC/34, 12 septembre 2011. para. 48.
133 *Ibid.*
134 Voir, par exemple, la Convention du Conseil de l´Europe sur la prévention du terrorisme, Art. 5 ; Décision cadre du Conseil de l´Union européenne 2002/475/JHA du 13 juin 2002 sur la lutte contre le terrorisme (telle qu´amendée par la décision cadre du Conseil 2008/919/JHAdu 28 novembre 2008), Art. 3 ; et la résolution du Conseil de sécurité des Nations Unies 1624 (2005), Para 1.S/RES/1624 (2005), 14 septembre 2005.
135 Questionnaire de l´étude sur la cybercriminalité Q38.
136 Voir, par exemple, http ://www.justice.gov/opa/pr/2011/February/11-nsd-238.html et http ://www.cps.gov.uk/news/press_releases/137_07/

Comme dans le cas des discours de haine, l´internet et les médias sociaux créent de nouvelles plateformes ayant une large diffusion pour inciter au terrorisme.[136] Étant donné que les gouvernements appliquent les lois existantes et développent de nouvelles lois, il est fondamental que– comme l´établit la publication de l´ONUDC sur l´utilisation de l´internet à des fins terroristes – les états « *trouvent le juste équilibre entre les exigences du respect de la loi et la protection des libertés et des droits de l´homme* » dans ce domaine.[137] Les rapports soumis par les états membres au Comité de lutte contre le terrorisme des Nations Unies United sur la mise en œuvre de la résolution 1624 (2005) du CSNU montrent une grande diversité pour ce qui concerne la manière dont la législation nationale définit l´incitation au terrorisme et l´interdit.[138] Les réponses nationales peuvent notamment inclure ou exclure des actes tels que la justification ou la glorification des actes terroristes.[139]

Incitation au terrorisme – exemple de cas

En 2011, une personne âgée de 22 ans d´un pays d´Amérique du nord fut inculpée pour son implication dans la diffusion d´informations relatives aux explosifs, et l´incitation à commettre un acte de violence sur le territoire du pays. Des accusations additionnelles portées contre lui incluaient l´agression contre des officiers des services répressifs et la possession d´une arme à feu pour commettre un acte de violence. Le défendeur était un administrateur actif d´un site web islamique extrémiste internationalement connu, où il avait publié de nombreux messages qui exprimaient ses affinités avec les points de vue radicaux et encourageait les autres membres qui professaient la même foi à commettre des actes de violence dans ce pays d´Amérique du nord, en prenant pour cibles des postes de police, des bureaux de poste, des synagogues, des installations militaires, et des infrastructures de transport. Pour réaliser ces attaques il avait publié un lien vers un long document contenant les étapes détaillées pour fabriquer des explosifs. Le défendeur se déclara coupable d´avoir incité à commettre des crimes de violence et de posséder une arme à feu destinée à commettre un crime de violence durant l´été 2011, la condamnation fut reportée à janvier 2013.

Du point de vue des droits de l´homme, l´utilisation de termes vagues tels que « glorifier » ou « promouvoir » le terrorisme peut représenter un problème lorsqu´on restreint l´expression.[140]Le concept de « glorification », notamment, peut ne pas être étroit ou précis pour servir de base à des sanctions pénales en conformité avec les exigences du principe de légalité. De plus l´incitation peut être interprétée comme un appel direct à s´impliquer dans le terrorisme, avec l´*intention* que cela favorise le terrorisme, et dans un contexte dans lequel l´appel est *directement* la cause de l´augmentation des risques de survenue d´un acte terroriste.[141] Le rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d´opinion et d´expression déclare notamment que la formulation de la Résolution 1624 (2005) du CSNU (« interdire en vertu de la loi l´incitation à commettre des actes terroristes ») est mieux nuancée en déclarant que « est considérée une infraction la diffusion intentionnelle et illicite ou toute autre forme de mise à disposition du public d´un message, avec l´intention d´inciter à commettre un acte terroriste, qui préconise directement ou non de commettre des infractions terroristes, et qui crée un danger qu´une ou plusieurs de ces infractions puissent être commises ».[142]

137 ONUDC, 2012. *L´utilisation d´ internet à des fins terroristes*, p.41.

138 Les rapports des états membres sur les mesures en place pour prévenir et interdire en vertu de la loi l´incitation à commettre un acte terroriste sont disponibles sur : http ://www.un.org/en/sc/ctc/resources/1624.html,pour une vue d´ensemble, voir aussi van Ginkel, B., 2011. Incitation au terrorisme : une affaire de prévention ou de répression ? *Document de recherche ICCT*. La Hague : Centre international de lutte contre le terrorisme,

139 *Ibid.* Voir, par exemple, les rapports présentés par le Brésil, l´Egypte, la Lettonie, l´Espagne, le Royaume Uni et l´Irlande du nord

140 L´assemblée générale des Nations Unies, 2008. *La protection des droits de l´homme et des libertés fondamentales lors de la lutte contre le terrorisme*. Rapport du Secrétaire général A/63/337, 28 août 2008.

141 *Ibid.*

142 L´assemblée générale des Nations Unies, 2011. *La promotion et la protection du droit à la liberté d´opinion et d´expression*. Rapport du Rapporteur spécial A/66/290, 10 Août2011.

143 Questionnaire de l´étude sur la cybercriminalité Q34, Q36 et Q39.

Autres formes d´expression et le défi des traditions juridiques et de la juridiction

D´autres formes d´expression généralement interdites font encore moins l´objet d´un consensus entre les lois nationales et internationales et les approches régionales. Lors de la collecte des informations pour l´étude, de nombreux pays– de toutes les régions du monde–faisaient référence à des lois pénales générales qui avaient une incidence sur la liberté d´expression et qui incluaient : des lois sur la diffamation et les outrages ; le matériel obscène ou pornographique ; la débauche, les bonnes mœurs et les publications indésirables.[143] Étant donné que l´internet et les médias sociaux deviennent de plus en plus importants pour les activités politiques et l´expression socio-culturelle, il existe une nécessité émergente (i) d´éclaircissements nationaux relatifs au droit pénal applicable aux formes d´expressions en ligne (ii) de discussion concernant les différences en matière d´incrimination qui proviennent de questions juridictionnelles et de diverses traditions juridiques.

Face à la recrudescence des délits dans les médias sociaux,[144] certains pays ont émis récemment des orientations provisoires sur les poursuites impliquant des communications envoyées par le biais des médias sociaux.[145] Ces orientations insistent sur le fait que les dispositions pénales doivent être interprétées conformément au principe de la liberté d´expression et peuvent aider à clarifier la portée de l´expression acceptable. A cet égard, la doctrine des droits de l´homme sur la « marge d´appréciation » accorde aux pays de la latitude pour déterminer les limites acceptables de la liberté d´expression en conformité avec leurs propres cultures et traditions juridiques.[146] Toutefois, le droit international relatif aux droits de l´homme interviendra à un certain moment. Le Comité des droits de l´homme des Nations Unies considère, par exemple, que les lois pénales sur la diffamation peuvent porter atteinte au droit de la liberté d´expression et devraient inclure des défenses comme la défense de la vérité.[147] Le Comité a également exprimé sa préoccupation pour ce qui concerne les lois en matière de lèse-majesté, de desacato (outrage à une personne investie de l´autorité) d´outrage à l´autorité, d´offense au drapeau et aux symboles, de diffamation du chef de l´état et de protection de l´honneur des fonctionnaires publics.[148]

---

144 En Angleterre et dans le pays de Galles, par exemple, en 2008 il y avait 556 rapports sur des délits sur les médias sociaux et 46 personnes étaient accusées. En 2012, il y eut 4,908 rapports et 653 personnes furent accusées. Voirhttp ://www.bbc.co.uk/news/uk-20851797. En Asie de l´ouest de nombreux cas récents de délits liés au contenu d´internet et des médias sociaux ont également été signalés, voirhttp ://www.bbc.co.uk/news/worldmiddle-east-20587246

145 Service des poursuites judiciaires de la Couronne, 2012. *Orientations provisoires sur les poursuites impliquant des communications envoyées par le biais des médias sociaux*. Élaborées par le Directeur des poursuites publiques, 19 décembre 2012.

146 Lorsqu´une valeur ou un droit important est en jeu, la marge d´appréciation accordée à un état sera en général restreinte (ECtHR. Demande n° 44362/04. 18 avril 2006). Si au contraire l´objectif poursuivi ne jouit pas d´un consensus universel– comme la signification du terme « protection de la moralité » – la marge d´appréciation sera vaste (ECtHR. Demande n° 10737/84. 24 mai 1988). La ECtHR emploie, entre autre, un test commun (Européen) de consensus pour déterminer la marge disponible – lorsqu´il n´y a pas de consensus sur la signification ou le besoin de limitations de droits spécifiques, la marge s´élargit. Lorsqu´au contraire il existe un consensus, cela signifie que la signification « principale » du droit est étroitement définie et la marge se réduit. La marge nationale d´appréciation va donc de pair avec une « supervision européenne » – pour ce qui concerne l´objectif et la nécessité d´ingérence. La doctrine de la marge d´appréciation est moins développée dans le travail de la Cour interaméricaine des droits de l´homme et du Comité des droits de l´homme des Nations Unies. Les commentateurs signalent néanmoins que la marge d´appréciation a un rôle de plus en plus important dans le système interaméricain, et que d´amples preuves appuient la proposition d´incorporer la doctrine aux pratiques du Comité des droits de l´homme des Nations Unies (Legg, A., 2012. *La marge d´appréciation des lois internationales sur les droits de l´homme.* Oxford : Oxford Monographies sur le droit international).

147 Voir la Communication CCPR/C/85/D/1180/2003 du Comité des droits de l´homme des Nations Unies, et le *Commentaire général n°. 34*. Article 19 : liberté d´opinion et d´expression. CCPR/C/GC/34, 12 2011 du Comité des droits de l´homme des Nations Unies, septembre 2011. para. 47.

148 *Ibid.* para. 38.

149 ECtHR Demande n°. 5446/04.

150 Dans l´affaire *Licra v Yahoo!*, un tribunal national ordonna à Yahoo! Inc. de prendre des mesures pour éviter que les usagers de ce pays n´aient accès à un site web d´enchères situé dans un pays tiers, qui vendait des objets Nazi (Ordonnance de référé rendue le 20 novembre 2000. Tribunal de grande Instance de Paris. n°. RG : 00/05308). Lors de procédures ultérieures dans le pays qui hébergeait le site, un tribunal national a déclaré en appel national qu´il n´y avait pas de chefs de compétence, à moins que ou jusqu´à ce que, les tribunaux nationaux se saisissent du jugement rendu par le tribunal étranger pour son exécution, et qu´un argument relatif à la liberté d´expression ne pourrait donc pas être pris en considération dans ce cas (*Yahoo Inc. v La Ligue Contre le Racisme et l »Antisémitisme.* n°. 01-17424. Cour d´appel des états unis, neuvième circuit.)

151 ECtHR n°. 5446/04.

152 Commissaire aux droits de l´homme du Conseil de l´Europe, 2012. *Médias sociaux et droits de l´homme* .Document de discussion. DH, 8 février 2012.

153 *Ibid.* p.17.

Quand il s´agit du contenu global d´internet, les affaires telles que *Perrin*[149]et *LICRA v Yahoo!*[150] mettent en évidence les difficultés qui surgissent quand le contenu internet qui est généré et est acceptable dans un pays, devient disponible dans un pays tiers. Dans l´affaire *Perrin*, par exemple, la Cour européenne des droits de l´homme jugea que l´application de lois sur l´obscénité du pays défendeur, concernant le contenu internet d´un site opéré et contrôlé par un pays tiers ne considérant pas le contenu comme illégal, n´excédait pas la marge d´appréciation du pays défendeur.[151] Les commentateurs ont soutenu que dans ce cas, la Cour européenne avait appliqué une marge d´appréciation excessivement large et n´avait pas suffisamment traité la question juridictionnelle– en sanctionnant potentiellement la vaste portée juridictionnelle des pays plutôt que les producteurs de contenus se trouvant dans d´autres pays, conformément à leurs propres normes sur les contenus.[152] La Cour n´a pas examiné la proximité du lien entre le requérant, l´entreprise propriétaire du site basé dans un pays tiers et le pays défendeur.[153] À cet égard la Déclaration conjointe des mécanismes internationaux pour la promotion de la liberté d´expression et d´internet recommande que la juridiction dans les affaires liées au contenu internet soit restreinte aux « *états avec lesquels ces affaires ont une relation réelle et substantielle ».* Ceci a lieu « *normalement lorsque l´auteur de l´infraction y réside, le contenu y est téléchargé et/ou le contenu s´adresse spécifiquement à cet état* ».[154]

> *« Les procureurs devraient tenir compte du fait que le contexte dans lequel a lieu un dialogue interactif dans les médias sociaux est très différent du contexte dans lequel d´autres types de communications ont lieu...*
> *Les communications destinées à quelques-uns peuvent toucher des millions de personnes. Dans ce contexte les procureurs pourront seulement traiter ces affaires... lorsqu´ils sont convaincus que la communication en question n´est pas seulement : offensive, choquante ou perturbatrice ; ou un commentaire satirique, iconoclaste ou impoli; ou l´expression d´une opinion démodée ou impopulaire sur des questions sérieuses ou triviales, ou des plaisanteries ou de l´humour même si ceux qui en font l´objet le trouvent détestable ou douloureux»...*
>
> Directives pour engager des poursuites dans des cas impliquant des communications envoyées par le biais de médias sociaux (un pays d´Europe du nord)

En général les différentes approches nationales de l´incrimination du contenu des médias sociaux et d´internet peuvent s´adapter aux lois internationales sur les droits de l´homme international, dans certaines limites. Ceci inclut les interdictions pénales permises sur la pornographie infantile ; l´incitation directe et publique à commettre un génocide ; l´apologie de la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, l´hostilité ou la violence ; l´incitation au terrorisme et la propagande en faveur de la guerre. Les infractions pénales liées à la diffamation, au matériel obscène et aux insultes seront vraisemblablement soumises à un seuil élevé – même dans la marge d´appréciation– pour déterminer si les mesures, conformément au principe de proportionnalité, sont appropriées pour remplir leur fonction de protection, et sont les instruments les moins invasifs entre les divers instruments pouvant offrir une protection.[155]De plus, si les états tentent de faire valoir leur juridiction sur le contenu internet en se basant sur leurs propres normes nationales, il est probable que le droit international concrétisera de plus en plus la nécessité de démontrer que le contenu créé ou hébergé dans d´autres pays est spécifiquement visé, ou que des personnes de l´état d´exécution y ont fréquemment accès. Lorsque le contenu est illicite dans un pays, mais qu´il est légal de le produire et le diffuser dans un autre pays, les lois internationales sur les droits de l´homme offrent un outil important– faisant office d´épée et de bouclier – et aident à définir une expression acceptable. Etant donné que les systèmes internationaux et régionaux des droits de l´homme développent leur jurisprudence, il est possible que, du moins dans certains domaines, un « consensus » sur les droits de l´homme puisse définir la taille de la marge d´appréciation au niveau international. S´il est impossible de réconcilier les différences nationales, les états devront se concentrer sur les meures de justice pénale applicables aux personnes qui accèdent à ce contenu au sein de leur juridiction nationale, plutôt que sur les producteurs de contenu se trouvant *hors* de leur juridiction nationale.

154 Le rapporteur spécial des Nations Unies sur la liberté d´opinion et expression, le représentant de l´OSCE pour la liberté des médias,
Le rapporteur spécial de l´OEA sur la liberté d´expression, et le rapporteur spécial de la CADHP sur la liberté d´expression et l´accès à l´information. Déclaration conjointe sur la liberté d´expression et internet. Disponible sur : http ://www.osce.org/fom/78309

155 Comité des Nations Unies sur les droits de l´homme, 2011. *Commentaire général n°. 34.* Article 19 : liberté d´opinion et d´expression. CCPR/C/GC/34, 12 septembre 2011. para. 34.

CHAPITRE CINQ : APPLICATION DES LOIS ET ENQUÊTES

Ce chapitre examine l´application des lois et les enquêtes menées en matière de cybercriminalité selon divers points de vue, en incluant les pouvoirs juridiques pour les mesures d´enquêtes, la protection de la vie privée, les bonnes pratiques et les difficultés en matière d´enquête, les interactions entre le secteur privé et les services répressifs, et la capacité et la formation des services répressifs. Il démontre la complexité des enquêtes sur la cybercriminalité et la nécessité de cadres juridiques efficaces ainsi que l´obtention de ressources et de compétences pratiques pour les services répressifs.

5.1 Application de la loi et cybercriminalité

PRINCIPAUX RÉSULTATS :

- plus de 90 % des pays qui ont répondu au questionnaire signalent que les autorités d´application de la loi prennent généralement connaissance des actes de cybercriminalité par le biais de rapports présentés par des personnes ou des entreprises qui en sont victimes ;
- ces pays estiment que la proportion actuelle de la victimisation de la cybercriminalité signalée à la police dépasse 1 %. Une enquête globale du secteur privé suggère que 80 % des personnes qui sont victimes des principaux délits de cybercriminalité ne signalent pas le délit à la police ;
- les autorités des services répressifs envisagent de traiter la sous déclaration avec une série de mesures qui incluent des actions de sensibilisation et de vulgarisation ;
- une réponse aux incidents de cybercriminalité doit toutefois être accompagnée d´enquêtes tactiques à long et moyen terme qui se concentrent sur les marchés criminels et les architectes du système criminel ;
- la proportion des actes de cybercriminalité détectés par le biais des enquêtes proactives est faible, maidse de nombreux pays se concentrent sur des opérations stratégiques d´infiltration.

Le rôle des services répressifs

L´Article 1 du Code de conduite des Nations Unies pour les responsables de l´application de la loi [1] souligne que le rôle des services répressifs est de remplir le devoir que leur impose la loi, *« en servant la communauté* » et « *en protégeant toutes les personnes contre les actes illégaux* ». Ce devoir s´étend à une vaste gamme d´interdictions prévues par les lois pénales.[2] Étant donné que les actes de cybercriminalité sont de plus en plus fréquent,[3] les services répressifs font face chaque fois davantage à la question de la signification de « servir » et de « protéger » dans le contexte de la dimension internationale des délits.

1 *Code de conduite pour les responsables de l´application de la loi*, Art.1. Annexe à la Résolution 34/169 de l´assemblée générale, 17 décembre 1979.
2 *Ibid.*, Commentaire de l´Art. 1, (d).
3 Voir le chapitre deux (la perspective d´ensemble).

Lors de la collecte des informations pour l´étude, plus de la moitié des pays signala qu´entre 50 et 100 % des actes de cybercriminalité enregistrés par la police incluaient un élément international.[4] En même temps les pays répondants indiquèrent la police prenait connaissance de la majorité des actes de cybercriminalité par le biais de rapports présentés par les personnes qui en étaient les victimes. Les infractions de cybercriminalité sont donc commises au niveau international mais sont signalées au niveau local. Le rapport peut être présenté par le biais d´une ligne d´assistance nationale pour les cyberdélits ou auprès d´une unité de police spécialisée, mais également auprès d´un poste de police municipal ou rural plus habitué à traiter des cas « classiques » de cambriolage, vol qualifié, vol ou homicide. Cependant, comme c´est le cas pour les délits « classiques », les « cyber » victimes et les « cyber » délinquants sont des individus réels avec des localisations géographiques réelles– et qui relèvent donc de la juridiction de la police locale.

Les postes de police locale transmettent souvent les cas de cybercriminalité à des services spécialisés au niveau national. Toutefois, l´implication croissante des preuves électroniques dans tous types de délits va probablement révolutionner les techniques policières, au niveau central *et* local dans les années à venir. Dans certains pays les postes de police locale sont systématiquement équipés avec une technologie de bureau permettant d´extraire les données des téléphones mobiles des suspects.[5] Les réponses fournies par les pays au questionnaire de l´étude mettent en évidence des variations considérables quant à la capacité des forces de police, entre et au sein des pays, pour enquêter sur des cyberdélits. Comme le commentait un pays : « les corps de police des régions sont très différents quand il s´agit de cybercriminalité. *Certains disposent d´unités contre la cybercriminalitébien organisées alors que d´autres ont à peine quelques officiers entraînés* ».[6]

Une réponse aux incidents de cybercriminalité doit toutefois être accompagnée d´enquêtes tactiques à long et moyen terme qui se concentrent sur les marchés criminels et les architectes du système criminel. La prévention de toutes les formes de criminalité requiert une approche proactive qui cible les problèmes, et que la police travaille de concert avec d´autres partenaires pluridisciplinaires [7] pour atteindre l´objectif général visant à maintenir l´ordre social et la sécurité publique.[8]

Les notions relatives à la « sécurité publique » et l´engagement « communautaire » de la police exigent une certaine adaptation lorsqu´elles sont transposées du monde « hors ligne » vers le monde « en ligne ». Néanmoins, les réponses fournies par les pays au questionnaire de l´étude suggèrent que ce principe, ainsi que de nombreux autres éléments des bonnes pratiques policières relatives à la prévention de la criminalité « classique », est applicable à la cybercriminalité. Ceci inclut notamment la nécessité que les services répressifs travaillent avec des partenaires du secteur privé et de la société civile, d´utiliser des activités de police fondées sur le renseignement pour anticiper et éviter les cyberdélits et d´utiliser des approches de résolution de problèmes basées sur des informations solides et le dépistage. Comme le soulignait un des pays répondants : « *les attaques sont devenues de plus en plus sophistiquées, il est de plus en plus difficile de les détecter et en même temps les techniques trouvent rapidement leur chemin vers une audience plus vaste* ».[9]

---

4 Questionnaire de l´étude sur la cybercriminalité. Q83. Certains pays qui n´ont pas fournir les chiffres exacts estimaient que le pourcentage était très élevé.

5 Voir http ://www.bbc.co.uk/news/technology-18102793

6 Questionnaire de l´étude sur la cybercriminalité.Q113.

7 ONUDC.2010.*Guide sur les principes directeurs en matière de prévention du crime : les faire fonctionner*

8 Bowling, B., et Foster, J., 2002. La Police et le maintien de l´ordre. *Dans* : Maguire, M., Morgan, R., Reiner, R. (eds.). *manuel de criminologie de Oxford.* 3ieme edn. Oxford : Oxford University Press.

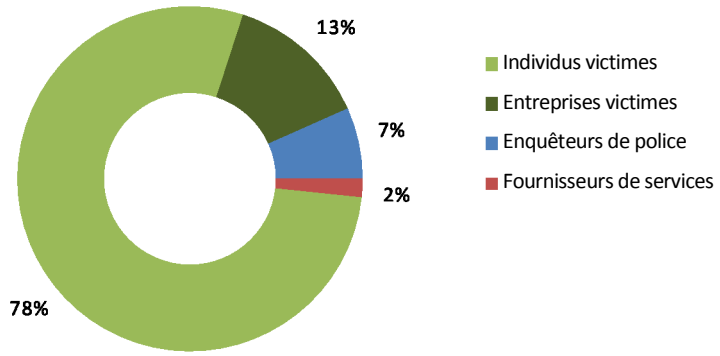
9 Questionnaire de l´étude sur la cybercriminalité. Q85

Comme le mentionne ce chapitre, les éléments essentiels d´une réponse congruente des services répressifs aux actes de cybercriminalité signalés incluent donc : (i) un cadre juridique efficace pour les mesures d´enquête qui offre un équilibre approprié entre le respect de la vie privée et les pouvoirs d´enquête ; (ii) l »accès aux outils et aux techniques d´enquête dans la pratique, y compris les moyens d´obtenir des preuves électroniques de tierces parties telles que les fournisseurs de services internet et (iii) la formation et les compétences techniques suffisantes pour les officiers spécialisés et non spécialisés.

A quoi la police est-elle confrontée ?

Lors de la collecte des informations pour l´étude les pays répondants déclarèrent que la police prenait connaissance de plus de 90 % des actes par le biais de rapports présentés par des personnes ou des entreprises qui en sont victimes.[10] les actes restants sont détectés directement par les enquêteurs de police ou obtenu par le biais de rapports des fournisseurs de services.

Figure 5.1 : sources des rapports sur des cyberdélits présentés à la police



Source : questionnaire de l´étude sur la cybercriminalité Q78. (n=61)

Le panorama de la cybercriminalité envisagé du point de vu des services répressifs est, comme dans le cas de tous les délits, nécessairement incomplet – car il est bâti à partir d´un mélange de cas particuliers qui ont fait l´objet d´une enquête et de renseignements criminels. Le caractère international de la cybercriminalité exacerbe les difficultés, car les pistes d´enquêtes arrivent sur des adresses IP ou des serveurs étrangers, et cela crée des retards pour ce qui concerne les mécanismes de coopération formels ou informels.

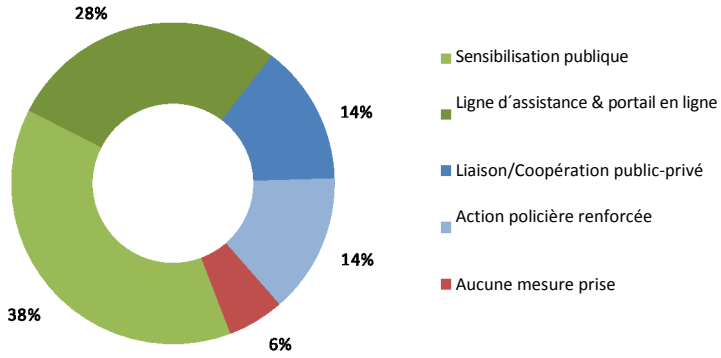
Comme le signale un pays répondant d´Afrique « *la plupart des délits, y compris ceux qui ne sont pas signalés incluent des dimensions internationales. Les cibles se trouvent le plus souvent hors des frontières nationales* ».[11] Un autre pays, qui se trouve également en Afrique, signale que « *la plupart des infractions signalées est entreprise hors du pays. La plupart du temps nous agissons en tant qu´intermédiaires,* » et un pays d´Europe soulignait que « *toutes les enquêtes sur la cybercriminalité menées lors de ces cinq dernières années comprenaient une dimension internationale. Des exemples de ceci sont des infractions liées à l´utilisation de comptes de courrier électronique, de médias sociaux et de serveurs proxy* ».[12]

Outre les éléments transnationaux, une sous déclaration importante des actes de cybercriminalité peut contribuer à présenter une perspective limitée du phénomène sous-jacent. La police prend connaissance de 90 % des actes de cybercriminalité par le biais de rapports présentés par des victimes et les pays estiment que la proportion actuelle de la victimisation de la cybercriminalité signalée à la police dépasse 1 %.[13]Une enquête menée par une organisation du secteur privé suggère que 80 % des personnes qui sont victimes des principaux délits de cybercriminalité ne signalent pas le délit à la police.[14]

10 Questionnaire de l´étude sur la cybercriminalité Q78.
11 Questionnaire de l´étude sur la cybercriminalité. Q83.
12 *Ibid.*
13 Questionnaire de l´étude sur la cybercriminalité. Q82.
14 Symantec. 2012. *Rapport Norton sur la cybercriminalité 2012.*
15 Questionnaire de l´étude sur la cybercriminalité. Q82.
16 *Ibid.*

Les pays qui ont répondu au questionnaire de l´étude sur la cybercriminalité attribue la sous déclaration à plusieurs facteurs, y compris à un manque de confiance de la population quant à la capacité de la police pour traiter les cyberdélits, à un manque de sensibilisation en matière de victimisation et de mécanismes de signalement, à la honte et l´embarras ressentis par la victime, et aux risques perçus pour leur réputation dans le cas des entreprises. Un pays a, par exemple, déclaré que : « *il est très difficile de faire une estimation. Les entreprises et les banques ne tiennent pas à signaler les cyberdélits en raison des risques pour leur réputation* ».[15]un autre pays soulignait que « *la plupart des victimes ne se rende pas compte qu´elles ont été prises pour cibles ou les dommages causés sont insignifiants et elles les ignorent* ».[16] Lorsque des cas sont signalés à la police, les enquêtes ultérieures peuvent révéler une base beaucoup plus large de victimes et de délinquants que ceux identifiés au début d´une affaire. Comme le signalait un des pays répondants : « *certains de ces délits pourraient être beaucoup plus communs [que ceux qui sont signalés]* ».[17]

Figure 5.2 : mesures prises pour augmenter le signalement des cyberdélits à la police



Source : questionnaire de l´étude sur la cybercriminalité Q79. (n=57, r=107)

Plusieurs pays répondants ont mentionné des stratégies et des approches utilisées pour augmenter le signalement des actes de cybercriminalité. Comme le montre la Figure 5.2 ceci inclut des campagnes publiques de sensibilisation, la création de systèmes d´assistance en ligne et téléphonique pour le signalement, la liaison avec les organisations du secteur privé, et l´amélioration de la communication et du partage d´informations de la police. Parmi environ 60 pays qui ont répondu au questionnaire moins de 10 % ont déclaré n´avoir pris aucune mesure visant à augmenter le signalement des actes de cybercriminalité.[18]

Les réponses des pays ont également montré qu´il était nécessaire que les services répressifs collaborent étroitement avec d´autres intervenants, du secteur privé, par exemple – pour augmenter le signalement et à des fins de renseignements. Un pays a, par exemple, déclaré qu´il était important de « *établir une connectivité de 24 heures sur 24 entre les administrateurs des sites web importants, les fournisseurs de services internet, la police et un centre de coordination pour les incidents de sécurité* ». Un autre pays en Amérique signalait que « *la police fédérale cherche à conclure des accords avec des entreprises publiques et privées afin que la police fédérale soit notifiée par voie électronique des délits commis contre ces entreprises et leurs clients* ».[19]Toutefois, la proportion relativement faible d´actes de criminalité signalés par les entreprises qui en sont victimes ou les fournisseurs de services internet, suggère que des mesures supplémentaires de vulgarisation et le développement d´un partenariat public-privé pourraient être nécessaires afin de renforcer le signalement des actes de cybercriminalité. Le développement d´un partenariat public-privé et la responsabilité des fournisseurs de services est traitée au chapitre huit (prévention). Les interactions entre les services répressifs et les fournisseurs de services tiers durant les enquêtes policières sont abordées ci-après dans le chapitre.

17 Questionnaire de l´étude sur la cyberciminalité. Q80.
18 Questionnaire de l´étude sur la cyberciminalité. Q79.
19 Questionnaire de l´étude sur la cyberciminalité. Q79.
20 Questionnaire de l´étude sur la cyberciminalité. Q78.

Une caractéristique notable de la figure 5.1 est la faible proportion d´actes de cybercriminalité détectés par les enquêteurs des services répressifs en l´absence de rapports de victimes. Par conséquent les pays répondants ne font pas référence, en général, dans les réponses écrites du questionnaire, aux enquêtes proactives. Un pays a toutefois signalé que « *dans certains cas la police prend connaissance des actes de cybercriminalité lorsqu´elle effectue ses activités opérationnelles* ».[20] Un autre pays d´Europe signalait aussi que « *dans le cas des infractions relatives à la pornographie infantile les enquêtes sont généralement lancées sur la base d´informations provenant d´autres forces de polices et de sources ouvertes*, » en faisant allusion au travail de renseignement de la police sous-jacent. La répartition de la source des actes de cybercriminalité identifiés illustre les difficultés d´aborder les objectifs *stratégiques*et*tactiques*de la police. Les objectifs stratégiques de la police sont « guidés par la menace » et liés à des objectifs répressifs à plus long terme, et se concentrent sur les causes profondes et les circonstances des délits graves. Les objectifs tactiques de la police sont axés sur les incidents et assujettis des contraintes de temps, et l´accent est mis sur la conservation des preuves et le suivi des pistes d´enquêtes. Dans le cas de la cybercriminalité, les ressources et le temps requis de la police pour traiter des cas individuels sont significatifs. Comme cela est analysé ci-après dans le chapitre, plusieurs pays ont mentionné les grandes quantités de preuves associées aux enquêtes sur des cyberdélits et le temps exigé par les enquêtes sur les cas signalés. Un pays d´Amérique a, par exemple, déclaré que « *la complexité des infractions de cybercriminalité et les éléments liés à la cybercriminalité des infractions traditionnelles ont beaucoup augmenté, et cela entraîne des demandes supplémentaires de formation et la maintenance d´enquêteurs hautement qualifiés et d´experts techniques, cela accroit également la quantité de temps requis pour traiter les cas individuels* ».[21] dans plusieurs pays la capacité des services répressifs est totalement occupée par les affaires de routine. Dans les réponses relatives à la capacité des services répressifs en matière d´enquêtes criminalistiques, par exemple, un pays d´Afrique signala que « *quelques examinateurs/enquêteurs criminalistiques sont disponibles au niveau fédéral, mais ils ne sont pas assez nombreux pour tout le pays. Un seul laboratoire est fonctionnel* ».[22] Un autre pays en Amérique soulignait que « *la difficulté ne réside pas dans l´expertise, mais dans la quantité de données qui doivent être analysées* ».[23] Le caractère des enquêtes criminalistiques et la capacité des services répressifs dans ce domaine, sont analysés de manière détaillée au chapitre Six (preuves électroniques et justice pénale).

Outre les difficultés en matière de capacité et de ressources, la mesure dans laquelle les services répressifs peuvent mener des enquêtes proactives sur la cybercriminalité peut se voir affectée par les différences sous-jacentes entre les systèmes de droit civil et de droit commun pour ce qui concerne la surveillance judiciaire et des poursuites au cours des étapes initiales d´une enquête,[24] ainsi que la mesure dans laquelle des mesures d´enquête intrusive peuvent être autorisées dans des enquêtes prospectives ou basées sur le renseignement. Comme cela est mentionné dans ce chapitre, les enquêtes sur la cybercriminalité utilisent souvent des outils, y compris l´interception de communications et la surveillance électronique, qui peuvent potentiellement violer les droits à la vie privée. Les pays qui doivent se conformer à des engagements relatifs aux lois internationales sur les droits de l´homme devront trouver un équilibre entre la protection de la vie privée et la violation de ce droit, motivée par des objectifs légitimes de contrôle et de prévention de la criminalité. La section relative aux enquêtes et à la vie privée examine cette question de manière plus approfondie.

Toutefois, les services répressifs des pays développés, et également de certains pays en développement, mènent des enquêtes stratégiques à long et moyen terme. Ceci met souvent en scène des unités d´infiltration qui visent des délinquants sur les sites de réseaux sociaux, les salles de discussion, les services P2P et de messagerie instantanée. Les exemples incluent l´infiltration ou l´établissement de forums en ligne de piratage de cartes bancaires,[25] l´examen criminalistique des forums utilisés par des auteurs d´infractions de pornographie infantile,[26] l´utilisation d´officiers des services répressifs posant en ligne comme des mineurs,[27] et l´examen des serveurs de contrôle et de commande des logiciels malveillants.[28]

Plusieurs de ces enquêtes impliquent de multiples organismes d´application de la loi et une vaste gamme de mesures d´enquêtes, y compris les mesures mises en œuvre conformément à l´autorité judiciaire, comme les ordonnances de perquisition ou d´ interception. En effet, les enquêtes stratégiques et tactiques requièrent l´accès à un éventail de pouvoirs d´enquête, qui – conformément aux principes de l´état de droit– doivent être solidement fondés sur une autorité juridique. La prochaine section de ce chapitre examine les pouvoirs d´enquêtes typiques en matière de cybercriminalité inclus dans les instruments régionaux et internationaux et les lois nationales.

21 Questionnaire de l´enquête sur la cybercriminalité Q84.
22 Questionnaire de l´enquête sur la cybercriminalité. Q110.
23 *Ibid.*
24 Voir, par exemple, INPROL. 2012. *Guide du juriste : traditions de la Common Law et de la loi civile.*
25 Voir http ://www.fbi.gov/news/stories/2008/october/darkmarket_102008 and http ://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown
26 Voir https ://www.europol.europa.eu/sites/default/files/publications/2csefactsheet2012_0.pdf
27 Voir http ://cdrc.jhpolice.gov.in/cyber-crime/
28 Voir http ://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin,%20Nikita%20Complaint.pdf

5.2 Aperçu des pouvoirs d´enquêtes

PRINCIPAUX RÉSULTATS :

- plusieurs pays à l´extérieur de l´Europe considèrent que leur cadre juridique national est insuffisant pour mener des enquêtes en matière de cybercriminalité ;
- de plus les approches nationales en matière de pouvoirs d´enquêtes sur la cybercriminalité ont une base commune moindre qu´en matière de d´incrimination de nombreux actes de cybercriminalité ;
- bien que les approches juridiques varient, les pouvoirs d´enquête essentiels requis incluent la perquisition et la saisie, les ordonnances concernant les données informatiques, comme la collecte des données en temps réel et la conservation des données ;
- parmi dix mesures d´enquête, les pays mentionnent généralement l´existence de pouvoirs généraux (non spécifiques en matière de cybercriminalité). Certains pays signalent également une cyberlégislation spécifique, notamment pour garantir une conservation rapide des données informatiques et pour obtenir les données enregistrées des abonnés ;
- plusieurs pays ont signalé l´absence de pouvoirs légaux pour les mesures d´enquête de pointe, comme la criminalistique informatique à distance.

Pouvoirs d´enquête généraux et spécifiques en matière de cybercriminalité

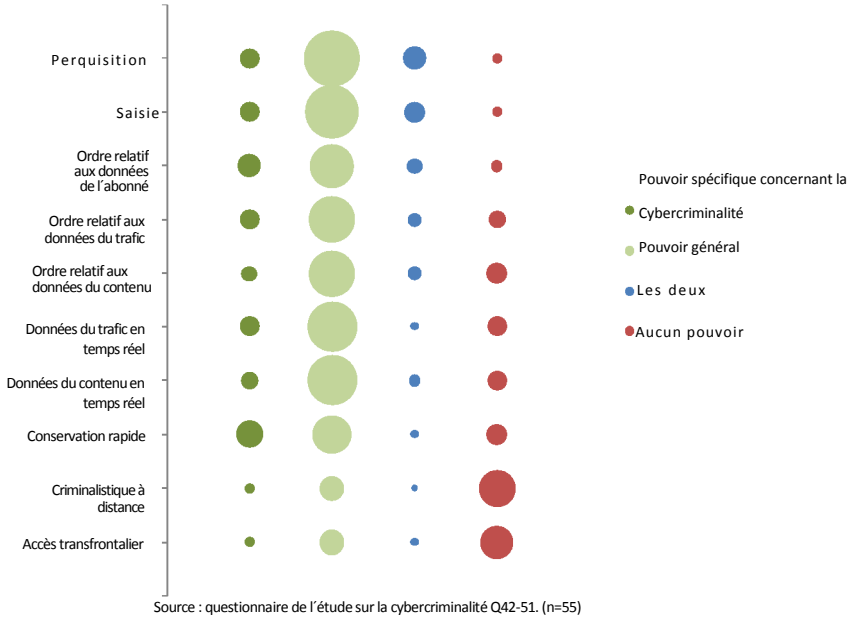
Les preuves des actes de cybercriminalité sont presque toujours sous une forme électronique ou numérique. Ces données peuvent être stockées ou transitoires et peuvent exister sous la forme de fichiers informatiques, de transmissions, de journal, de métadonnées ou de données en réseau. Obtenir ces preuves demande l´utilisation conjointe des nouvelles techniques policières et des traditionnelles. Les services répressifs peuvent utiliser le travail policier « traditionnel » (l´entretien avec les victimes ou la surveillance visuelle secrète des suspects) à certaines étapes de l´enquête, mais requièrent des approches spécifiques en matière de cybercriminalité à d´autres étapes. Ceci peut comprendre le visionnage, la saisie ou la reproduction de données informatiques de dispositifs appartement aux suspects ; l´obtention de données informatiques des tierces parties telles que les fournisseurs de services internet, et–si cela est nécessaire– l´interception des communications électroniques.Alors que certaines de ces mesures d´enquête peuvent être mises en œuvre avec les pouvoirs traditionnels, de nombreuses dispositions de procédure ne se transposent pas aisément d´une approche spatiale et orientée objet à une approche impliquant le stockage de données électroniques et le flux de données en temps réel. Dans certains pays les données informatiques sont couvertes par les dispositions traditionnelles relatives à la perquisition et le terme « toute chose » pour ce qui concerne la saisie est considéré pertinent pour une infraction. Les lois existantes relatives aux « écoutes » ou à « l´interception des communications » peuvent aussi couvrir certainsaspectsdes enquêtes sur la cybercriminalité

29 Voir, par exemple, Feigenbaum *et al*., 2007. Un modèle de routage en oignon avec un anonymat garanti. *Notes sur la sécurité des données et la cryptographie financières en science informatique*, 4886 :57-71 ; et Schwerha, J.J., 2010. *Difficultés des services répressifs pour transborder les preuves électroniques des fournisseurs de services hébergés,* Document de discussion du Conseil de l´Europe, pp.9-10 ; Walden, I., 2013. *Accéder à des données dans le nuage : le bras long des agents des services répressifs. Sécurité et confidentialité du nuage informatique. Réseaux communications informatiques 2013 pages 45-71*

Toutefois, dans d´autres pays les lois procédurales traditionnelles ne pourront être interprétées de manière à inclure les données intangibles ou les communications IP. De plus les pouvoirs d´enquêtes doivent pouvoir traiter des difficultés comme le caractère volatile des preuves électroniques, et les techniques d´obfuscation utilisées par les délinquants– comme l´utilisation de l´encodage, les proxy, les services informatiques hébergés, les systèmes informatiques « innocents » infectés par un logiciel malveillant, et les routages multiples (en oignon) des connexions internet.[29] Ces aspects présentent des difficultés particulières pour les pouvoirs traditionnels. Plusieurs pays répondants ont déclaré que les pouvoirs d´enquête sont fréquemment « *déphasés par rapport aux nouvelles technologies émergentes* » et souvent « *la législation est conçue pour la fouille physique, et par conséquent les instructions prévues par la loi...ne satisfont pas les besoins, les intérêts et les procédures constitutionnelles pertinents pour les enquêtes sur la cybercriminalité* ».[30]

Les cadres juridiques pour les enquêtes en matière de cybercriminalité – que les lois soient surtout générales ou spécifiques en matière de cybercriminalité –requièrent : (i) un champ d´application clair du pouvoir, afin de garantir une certitude juridique lors de son utilisation ; et (ii) une autorité juridique suffisante pour des mesures telles que la conservation des données informatiques et la collecte des données stockées et des données en temps réel. A cet égard les cadres procéduraux spécialisés offrent la possibilité de définir clairement les concepts pertinents – comme les « données informatiques » en premier lieu, ainsi que les données au repos et les données en transit.[31] Ils permettent également de différencier les types de données, comme les données « de l´abonné » (les détails de base de l´enregistrement des usagers des services informatiques, comme le nom et l´adresse), les données de « trafic » (les données indiquant l´origine, la destination, la route, le temps, la date, la taille, la durée ou le type de communications effectuées par le biais d´un système informatique), et les données du « contenu » (le contenu réel d´une communication).[32] Durant la collecte des informations pour l´étude, on interrogea les pays sur l´existence de pouvoirs juridiques généraux ou spécifiques en matière de cybercriminalité pour 10 différentes mesures pertinentes pour les enquêtes menées par les services répressifs en matière de cybercriminalité (et pour d´autres délits impliquant des preuves électroniques). Les mesures d´enquête sur lesquelles portaient les questions étaient : (i) la fouille des données ou du matériel informatique ; (ii) la saisie des données ou du matériel informatique

Figure 5.3 : approches nationales concernant les mesures d´enquête en matière de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité Q42-51. (n=55)

30 Questionnaire de l´étude sur la cybercriminalité Q53.

31 Walden, I., 2003. Traiter le problème des données. *Rapport technique sur la sécurité de l´information*, 8(2) ; Nieman, A., 2009. Criminalistique des cyberdélits : tendre un pont sur la division droit/technologie. *JILT,* 2009(1).

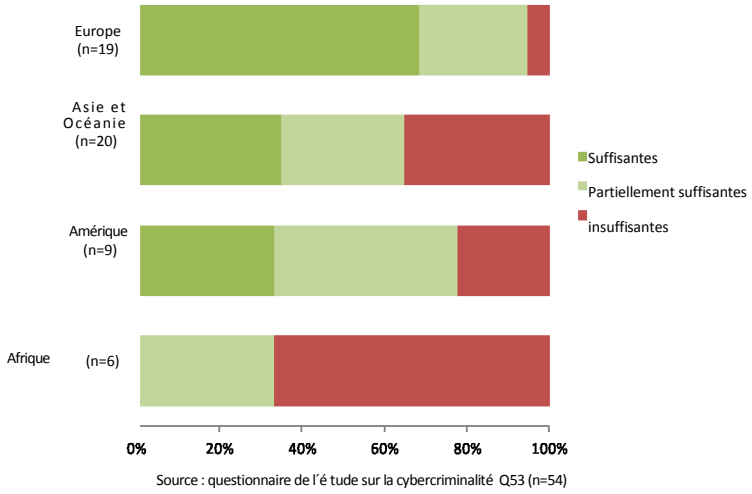
32 Sieber, U., 2008. Maitrise de la complexité dans le cyberespace global : l´harmonisation du droit pénal informatique. *In* : Delmas-Marty, M., Pieth, M., Sieber, U. (eds.). *Les chemins de l´»Harmonisation Pénale/Harmoniser le droit pénal.* Collection de L´»UMR de Droit Comparé de Paris. Paris : Société de législation comparée.

33 Voir le questionnaire de l´étude sur la cybercriminalité. Q42-51.

iii) ordonner à une personne de transmettre aux services répressifs les informations concernant un abonné ; (iv) ordonner à une personne de fournir les données de trafic stockées ; (v) ordonner à une personne de fournir les données du contenu stockées ; (vi) collecter les données de trafic en temps réel ; (vii) collecter les données du contenu en temps réel ; (viii) ordonner à une personne de préserver et maintenir l´intégrité des données informatiques qui sont sous son contrôle durant une période déterminée (« conservation rapide des données) ; (ix) utilisation d´outils informatiques criminalistiques à distance et(x) accès direct des services répressifs aux données informatiques extraterritoriales (accès « transfrontalier » aux données informatiques).[33]

La figure 5.3 fournit un aperçu des dispositions juridiques existantes qui couvrent les dix mesures d´enquête, mentionnées par les réponses de plus de 50 pays au questionnaire de l´étude. Les réponses démontrent que la majorité des pays dépendent de pouvoirs juridiques généraux lors des enquêtes en matière de cybercriminalité. C´est le cas pour une gamme de mesures d´enquête qui comprennent la perquisition, la saisie, les ordres relatifs aux données adressés à des tierces parties, la collecte des données en temps réel et les ordres concernant la conservation des données. Quand il s´agit de mesures d´enquête plus complexes et plus intrusives comme la criminalistique informatique à distance, presque la moitié des pays répondants a déclaré que ces mesures ne sont pas autorisées par la loi. Environ 20 % des pays ont signalé qu´il n´existait aucun pouvoir juridique relatif à la collecte des données informatiques en temps réel ou permettant d´émettre un ordre de conservation rapide des données informatiques. 10 % des pays ont signalé qu´il n´existait aucun pouvoir juridique même quand il s´agit d´une mesure basique de perquisition ou de saisie de données ou de matériel informatique.

Figure 5.4 : perception que les lois nationales en matière d´enquêtes sur la cybercriminalité sont suffisantes



Source : questionnaire de l´é tude sur la cybercriminalité Q53 (n=54)

Les pays qui ont mentionné l´existence de pouvoirs spécifiques en matière de cyberdélits présentent une vaste répartition géographique et se localisent en Europe, en Amérique du nord et du sud, dans les Caraïbes, en Asie de l´ouest et du sud est, en Afrique du nord et de l´ouest. Les mesures d´enquête les plus souvent couvertes par des dispositions spécifiques en matière de cybercriminalité étaient les ordres relatifs aux données de l´abonné adressés et à la conservation rapide des données – et environ 25 à 30 % des pays répondants signalaient l´existence de dispositions spécifiques dans ces domaines. Les mesures de perquisition et de saisie des données ou du matériel informatique sont le plus souvent couvertes par des dispositions générales et des dispositions spécifiques en matière de cybercriminalité – une situation mentionnée par environ 20 % des pays répondants.

Des pouvoirs d´enquête considérés suffisants en matière de cybercriminalité

En ce qui concerne la perception de suffisance des pouvoirs d´enquête, les réponses fournies par les pays au questionnaire de l´étude montre un patron similaire au patron concernant les lois sur l´incrimination. Environ 70 % des pays répondants

d´Europe considéraient que les pouvoirs d´enquête étaient suffisants. Les pays restants considéraient que les pouvoirs d´enquête étaient partiellement suffisants et un seul pays indiqua que les pouvoirs étaient insuffisants. Dans d´autres régions du monde 20 et 65 % des pays jugeaient que les pouvoirs d´enquête étaient insuffisants.

Lorsqu´on leur demanda quelles étaient les principales lacunes des pouvoirs d´enquête, plusieurs pays mentionnèrent une absence de pouvoirs permettant « d´entrer » sur des réseaux électroniques pour chercher des preuves, ainsi qu´une absence de pouvoirs concernant la conservation des données informatiques. Des pays d´Océanie et d´Europe déclarèrent qu´il existait la nécessité d´un « *mécanisme permettant de conserver rapidement les données informatiques pour appuyer les pouvoirs existants en matière de perquisition*, » et un pays d´Amérique du sud souligna qu´il y avait une « *absence de régulationde l´accès aux données et aux journaux de connexion ainsi qu´une absence de régulation des possibilités de perquisition virtuelle* ».[34]

34 *Ibid.*

Par ailleurs, si plusieurs pays ont signalé un manque total de cadres juridiques spécifiques en matière de cybercriminalité, quelques pays ont mentionné une extension réussie des pouvoirs généraux. Un pays d´Afrique australe signala, par exemple, que « *la loi de procédure pénale permet à l´état de saisir toute chose... [même si] la loi ne prévoit pas spécifiquement de cyberdélits* ».[35]

Certains pays ont également signalé que « *étendre à tous les délits et pas seulement aux délits traditionnels liés à l´informatique* » les pouvoirs d´enquête concernant les ordinateurs et autres dispositifs constituait une bonne pratique et que les lois procédurales pertinentes devraient être « *exhaustives* » et « *précises* »[36]

Pouvoirs d´enquête complets en matière de cybercriminalité : exemple national d´un pays de l´Europe du sud

Saisie de données informatiques
La saisie des données informatiques, en fonction de ce qui est considéré comme étant le plus approprié et proportionné, et en tenant compte des intérêts de l´affaire, peut prendre les formes suivantes :

a) saisir le matériel de support du système informatique ou le support de stockage des données informatiques, ainsi que les dispositifs requis pour lire les données ;
b) faire une copie de ces données informatiques, sur un support autonome, qui sera attachée au fichier ;
c) maintenir par des moyens technologiques l´intégrité des données, sans les copier ou les éliminer ; ou
d) éliminer les données informatiques ou bloquer l´accès aux données.

En général trois approches principales apparaissaient dans les réponses fournies par les pays au questionnaire de l´étude : certains pays n´avaient pas de lois spécifiques concernant les enquêtes sur les cyberdélits et appliquaient dans la mesure du possible une large interprétation des pouvoirs procéduraux traditionnels. D´autres pays avaient modifié les pouvoirs d´enquête généraux dans le cas de questions spécifiques et, en utilisant des dispositions générales et des pouvoirs spécifiques relatifs à la cybercriminalité, pouvaient appliquer des mesures telles que des ordonnances concernant les données, de perquisition et de saisie des données, et de conservation des données. Enfin, certains pays avaient introduit une gamme complète de nouveaux pouvoirs d´enquête spécialement conçus pour obtenir des preuves électroniques. Les dispositions législatives d´un pays du sud de l´Europe spécifiaient, par exemple, quatre manières différentes avec lesquelles les données pouvaient être considérées comme « s*aisies* » – (i) en saisissant le support même ; (ii) en faisant une copie ; (iii) en maintenant l´intégrité des données sans les éliminer ni les reproduire ; et (iv) éliminer les données ou bloquer l´accès aux données. Ces dispositions aident à éliminer l´incertitude juridique inhérente à l´application des pouvoirs d´enquête « traditionnels ».

L´examen des relations entre l´existence de pouvoirs législatifs spécialisés et la perception de la suffisance des mesures d´enquête en matière de cybercriminalité, révèle une certaine concordance entre les pays qui ont répondu au questionnaire. Dans le cas des pays qui ont déclaré que les mesures d´enquête étaient suffisantes ou partiellement suffisantes, environ 40 % des mesures d´enquête sur lesquelles portaient les questions étaient couvertes par des pouvoirs spécifiques en matière de cybercriminalité. Par contre, dans le cas des pays qui ont déclaré que les mesures d´enquête étaient insuffisantes, seulement 20 % de toutes les mesures d´enquête étaient couvertes par des pouvoirs spécifiques en matière de cybercriminalité.[37] Ces résultats soulignent l´importance du développer des pouvoirs d´enquête spécialisés– au minimum, dans le cas des mesures pour lesquelles l´extension des pouvoirs traditionnels est mise en doute. Le chapitre sept (coopération internationale) de cette étude souligne que le caractère global des cyberdélits implique que le manque de pouvoirs d´enquête dans un pays peut avoir un impact sur d´autres pays qui présentent des demandes de coopérationinternationale pour la collecte de preuves extraterritoriales.

35 *Ibid.*
36 *Ibid.*
37 Questionnaire de l´étude sur la cybercriminalité Q42-51 et Q53.
38 Voir le chapitre trois (cadres et législation), Section 3.1 Introduction –le rôle de la loi, les catégories pertinentes du droit.

Comme l´indique le chapitre trois (cadres et législation), de nombreux instruments régionaux et internationaux prévoient des pouvoirs d´enquête complets.[38] Le tableau de l´Annexe trois résume les pouvoirs, par article, dans ces cadres. La prochaine section du présent chapitre continue à examiner, de manière détaillée, la nature des dispositions sur les pouvoirs d´enquête incluses dans des instruments multilatéraux et compilées à l´échelle nationale par le questionnaire de l´étude. Sont ainsi examinés les pouvoirs de : (i) perquisition et saisie ; (ii) conservation des données informatiques ;(iii) ordonnances relatives aux données informatiques ; (iv) collecte de données informatiques en temps réel ; (v) utilisation d´outils criminalistiques à distance ; et (vi) accès direct des services répressifs aux données extraterritoriales.

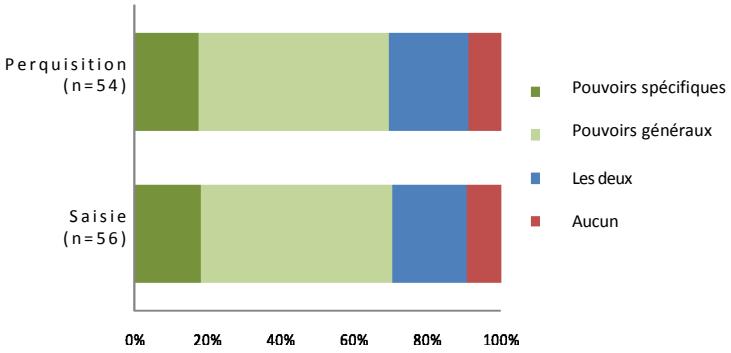
Mandat de perquisition et de saisie : exemple national d´un pays d´Amérique

(2) Un mandat émis en vertu de la présente section peut autoriser un officier de police à :
(a) saisir tout ordinateur, donnée, programme, information, document ou chose s´il a des motifs raisonnables de croire qu´il s´agit de la preuve d´une infraction qui a été, ou est sur le point d´être commise ,conformément à la présente loi ;
(b) inspecter et vérifier l´exploitation de tout ordinateur mentionné au paragraphe *(a)* ;
(c) utiliser ou faire en sorte que soit utilisé un ordinateur mentionné au paragraphe *(a)* afin de chercher des données ou un programme contenus ou accessibles à l´ordinateur ;
(d) avoir accès à toute information, code ou technologie capable de transformer ou de convertir un programme encodé ou des données contenues ou accessibles à l´ordinateur, en un texte ou un format lisible et compréhensible, afin de mener une enquête sur une infraction conformément à la présente loi ;
(e) convertir un programme encodé ou des données contenus dans un autre système informatique sur le lieu spécifié par le mandat, s´il a des motifs raisonnables de croire que les données informatiques liées au fait de commettre l´infraction pourraient être stockées sur un autre système informatique ;
(f) faire et conserver une copie des programmes et des données contenus dans l´ordinateur mentionné au paragraphe *(a)* ou *(e)* et de tout autre donnée ou programme contenu dans les ordinateurs.

Perquisition et saisie

Comme mentionné précédemment, les pays peuvent faire face à diverses difficultés quand il s´agit d´étendre les pouvoirs « traditionnels » de perquisition et de saisie aux données intangibles.[39] Pour cette raison sept instruments internationaux ou régionaux sur la Cybercriminalité[40]contiennent des dispositions sur des pouvoirs spécifiques relatifs à la perquisition,ou l´accès à des systèmes informatiques ou des supports de stockage des données informatiques. Six de ces instruments prévoient aussi l´extension de la perquisition à un autre système informatique sur le territoire du pays, s´il s´avère que l´information recherchée n´est pas sur le système original ou le support faisant l´objet de la perquisition.[41]De nombreux instruments multilatéraux précisent aussi les manières dont les données peuvent être saisies. La loi type du Commonwealth, par exemple, déclare que le terme « saisie » inclut « *faire une impression de la sortie de données* ».Au niveau national les réponses du questionnaire de l´étude montrent que la perquisition et la saisie des données ou du matériel informatique sont autorisées par les lois générales de procédure pénale dans la majorité des pays (environ 50 %) davantage que par le biais de pouvoirs spécifiques en matière de cybercriminalité.[42]

Figure 5.5 : instruments de perquisition et saisie utilisés dans les enquêtes sur la cybercriminalité



39 Voir, par exemple, Brenner, S. W., Frederiksen, B.A., 2002. Perquisitions et saisies informatiques : quelques problèmes non résolus. *Mich. Telecomm. Tech. L. Rev.* 39(8) ; Kerr, O.S., 2005. Mandat de perquisition à l´ère des preuves numériques *Mississippi Law Journal*, 75 :85.

40 Projet de convention de l´Union africaine, Arts. 3-50, 3-51 ; projet de loi type du COMESA, Arts. 37, 33 ; loi type du Commonwealth, Arts.12, 14 ; Convention du Conseil de l´Europe sur la cybercriminalité, Art. 19 ; projet de directive de la CEDEAO, Art. 33 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 20 ; Convention de la Ligue des états arabes, Arts. 26, 27.

41 Projet de convention de l´Union africaine ; projet de loi type du COMESA ; loi type du Commonwealth ; Convention du Conseil de l´Europe sur la cybercriminalité ; textes législatifs types de l´UIT//CARICOM/CTU ; Convention de la Ligue des états arabes.

42 Questionnaire de l´étude sur la cybercriminalité. Q42 et Q43.

Pour ce qui concerne l´application des pouvoirs généraux relatifs à la perquisition, un pays d´Asie de l´est précisa que les dispositions traditionnelles sur la perquisition pouvaient s´appliquer à la « *perquisition informatique* », mais que les dispositions autorisaient seulement la perquisition du matériel informatiques mais non des données.[43]Moins de 20 % des pays répondants mentionnèrent l´existence de pouvoirs spécifiques pour la saisie ou la perquisition en matière de cybercriminalité.

Moins de 10 % des pays déclarèrent ne disposer d´aucun pouvoir relatif à la saisie ou la perquisition– du moins pour les données informatiques. Un pays d´Asie de l´ouest déclara que « *pour ce qui concerne l´accès au matériel et à l´équipement informatiques, le code de procédure pénale traite le cas de l´accès physique des membres de la police judiciaire aux domiciles, mais n´aborde pas les cas de cyberdélits…Ces textes ne permettent pas aux membres de la police judiciaire d´accéder aux courriels et aux réseaux électroniques au motif d´une suspicion de commettre une infraction* ».[44]Le même pays signalait que la réforme des lois était nécessaire afin d´établir ces pouvoirs et actuellement « *si cela avait lieu en l´absence d´une disposition juridique cela violerait les dispositions prévues par la loi et la Constitution* ».

Conservation des données informatiques

Stocker des données informatiques requiert de l´argent et des ressources. Par conséquent les données informatiques sont stockées seulement le temps nécessaire à leur traitement. Dans le cas, par exemple, du clavardage et du service voix sur IP le contenu passe par des fournisseurs de services durant le temps nécessaire à des fins opérationnelles, telles que l´identification des défauts du système, oula facturation de l´abonné. Ceci peut aller de quelques secondes, à des heures, ou à quelques jours ou semaines. Outre les implications pragmatiques relatives au coût du stockage, plusieurs pays ont également des mesures de protection de données qui spécifient que les données ne doivent pas être conservées pour une durée supérieure à celle requise pour leur traitement.[45] Les exigences de procédures légales régulières ou– dans les cas internationaux– les demandes de coopération internationales, peuvent facilement exiger une période de tems supérieure à la durée de vie des données, avant que le mandat pertinent de perquisition ou l´ordonnance de produire les données stockées ne puisse être obtenu.[46]

Conservation rapide de données : exemple national d´un pays d´Afrique australe

Ordonnance de conservation

(1) Toute autorité chargée d´enquête peut solliciter au juge en chambre une ordonnance pour la conservation rapide des données qui ont été stockées ou traitées au moyen d´un système informatique ou de toute autre technologie de l´information et de la communication, lorsqu´il existe des motifs raisonnables de croire que ces données sont vulnérables à la perte ou la modification.

(2) Aux fins de l´alinéa (1), le terme données comprend les données de trafic et les informations concernant l´abonné.

(3) Une ordonnance émise en conformité avec l´alinéa (1) restera en vigueur :

(a) durant le temps que peut raisonnablement requérir l´enquête sur une infraction ;

(b) si des poursuites ont été engagées, jusqu´à ce que soit prononcée la décision définitive ; ou

(c) durant le temps que le juge en chambre considère approprié.

Par conséquent sept instruments régionaux et internationaux sur la cybercriminalité contiennent des dispositions visant à éviter la suppression des données informatiques importantes pour les enquêtes de cybercriminalité provisions.[47] Un ordre adressé à la personne qui contrôle les données informatiques de préserver et de maintenir l´intégrité des données durant une période déterminée ou des procédures accélérées pour sécuriser les données, comme un mandat de perquisition ou de saisie, permettent de donner effet à ces dispositions.

43 *Ibid*

44 Questionnaire de l´étude sur la cybercriminalité Q53.

45 Voir le chapitre huit (prévention), Section 8.3 la prévention de la cybercriminalité, le secteur privé et le milieu universitaire, la prévention de la cybercriminalité par les fournisseurs de services internet et les fournisseurs d´hébergement .

46 James Tetteh, A.-N., Williams, P., 2008. Le système juridique et la criminalistique numérique *: un dilemme de notre temps*.disponible sur : http ://ro.ecu.edu.au/adf/41/

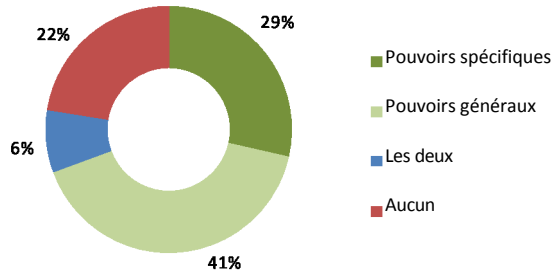
47 Projet de convention de l´Union africaine, Art. 3-53 ; projet de loi type du COMESA, Arts. 33-35 ; loi type du Commonwealth Art.17 ; Convention sur la cybercriminalité du Conseil de l´Europe, Art. 16 ; projet de directive de la CEDEAO, Art. 33 ; textes législatifs types de l´UIT/CARICOM/CTU, Art.23 ; Convention de la Ligue des états arabes, Art. 23.

Les dispositions typiques sur la conservation rapide des données peuvent inclure l´application d´une gamme de conditions et de garanties plus limitée que dans le cas de la divulgation des données, en raison du caractère probablement moins préjudiciable de la mesure sur la conservation(avant l´émission d´une ordonnance de divulgation).Toutefois, à cet égard il faut signaler que les mécanismes internationaux sur les droits de l´homme ont conclu que le seul fait de stocker des informations concernant un individu équivaut à une ingérence avec les droits à la vie privée.[48] Il est donc nécessaire d´évaluer la proportionnalité de la mesure pour émettre une ordonnance de conservation– en particulier si la conformité avec l´ordonnance exigeait que des données spécifiques soient conservées pour une durée supérieure à celle prévue par la législation sur la protection des données.

La conservation des données représente néanmoins une mesure importante permettant de conserver des preuves essentielles avant l´émission d´une ordonnance de divulgation– en particulier dans le contexte des enquêtes transnationales. En effet, la séparation des deux obligations, « préservation » et « divulgation » est un élément clé de la mesure.[49]

Au niveau national– en raison peut être de l´influence des instruments régionaux et internationaux sur la cybercriminalité– la conservation rapide des données est la mesure qui est signalée comme couverte par un pouvoir spécifique sur la cybercriminalité par la proportion la plus élevée de pays. Cependant, les réponses des pays indiquent aussi que cette mesure pourrait être couverte par des dispositions générales de diverses manières. Un pas d´Asie de l´ouest a, par exemple, déclaré que les dispositions sur la perquisition et la saisie étaient interprétées dans le sen où elles prévoyaient une conservation rapide des données. Un autre pays d´Afrique australe expliquait que les données informatiques pouvaient être conservées conformément à sa législation en saisissant l´ordinateur, et un pays d´Europe de l´ouest signalait qu´il utilisait des dispositions générales sur la saisie de la correspondance et d´autres informations.[50] Cependant, plus de 20 % des pays répondants indiquèrent que leurs lois nationales ne prévoyaient aucun pouvoir permettant la conservation rapide des données. L´absence d´autorité juridique pour un outil d´enquête fondamental représente une importante difficulté – non seulement pour ces pays en particulier mais également pour tout autre pays qui souhaite solliciter une assistance en matière d´enquête.

Figure 5.6 : conservation rapide des données informatiques



Source : questionnaire de l´étude sur la cybercriminalité Q49. (n=49)

Ordonnances concernant les données informatiques

Comme le mentionne le chapitre premier (connectivité et cybercriminalité), une grande partie des infrastructures et des systèmes informatiques utilisés pour les communications par internet est détenue et opérée par le secteur privé. Les fournisseurs de services internet ainsi que les fournisseurs de communications électroniques et les fournisseurs de services web, acheminent, stockent et contrôlent une quantité importante de données informatiques liées au contenu, aux opérations et aux connexions internet.

48 Voir, par exemple, ECtHR. demande n°. 9248/81.

49 Voir Brown, I., 2010. Rétention de données de communications dans un internet en évolution. *Journal international de droit et de technologie de l´information*, 19(2) :107.

50 Questionnaire de l´étude sur la cybercriminalité Q42-51.

L´utilisation de mesures coercitives, comme la perquisition et la saisie, de la part des services répressifs pour obtenir ces données est irréalisable dans la plupart des cas – en raison du volume des cas individuels faisant l´objet d´une enquête et de la perturbation causée à des activités commerciales légales. Les ordonnances adressées à ces tierces parties pour enquêter sur des données informatiques fournissent donc un processus juridique approprié pour obtenir des preuves électroniques. Dans plusieurs pays ces ordonnances peuvent être émises en vertu des pouvoirs d´enquête existants, tels que les ordonnances générales de production ou de divulgation de documents. Des difficultés en matière procédurale peuvent toutefois surgir quant aux exigences traditionnelles relatives aux *données d´identification* d´un suspect avant d´émettre des ordonnances pour les preuves. Dans les enquêtes en matière de cybercriminalité, lors d´une demande adressée à un fournisseur de services internet service provider, la seule information connue peut être une adresse IP ou des informations analogues relatives à la connexion. Par conséquent cinq instruments régionaux ou internationaux sur la cybercriminalité contiennent des dispositions spécifiques concernant les ordonnances permettant d´obtenir des données stockées.[51] Ce faisant, les instruments se réfèrent généralement à la distinction mentionnée précédemment dans ce chapitre –entre les données de « l´abonné », du « trafic », et du « contenu ». Ces dispositions concernent généralement les informations qui se trouvent « *en la possession ou sous le contrôle* » d´une personne ou d´un fournisseur de services. L´ordonnance est donc applicable dans la mesure où ces données existent au moment de l´émission de l´ordonnance, et où elles peuvent être récupérées par la personne qui fait l´objet de l´ordonnance. L´existence en soi de ces pouvoirs d´enquête n´oblige pas les fournisseurs de service à collecter ou à conserver des informations qui ne seraient pas traitées ainsi normalement. Pour ce qui concerne les données du *trafic*, certains instruments[52] multilatéraux incluent aussi un mécanisme de divulgation rapide « partielle » de suffisamment de données de trafic pour permettre aux services répressifs d´identifier les fournisseurs de service et du chemin par lequel la communication a été transmise.

Ordonnance concernant des données informatiques : exemple national d´un pays d´Amérique

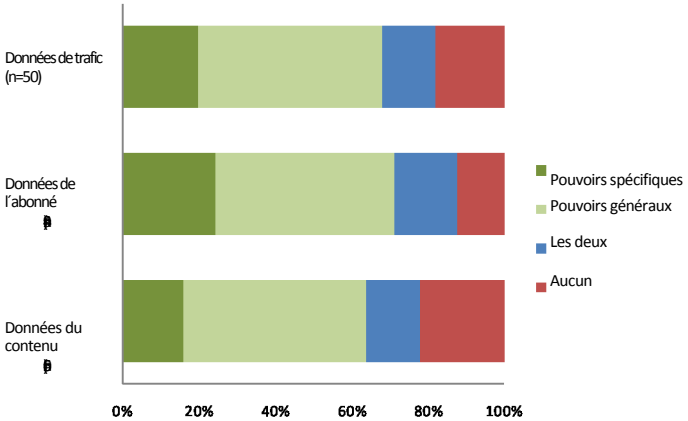
Lorsqu´un magistrat est satisfait sur la base d´une demande faite par un officier de police que des données informatiques spécifiques, une impression ou d´autres informations, font l´objet d´une demande raisonnable pour les besoins d´une enquête criminelle ou de poursuites judiciaires, le magistrat peut ordonner :

(a) qu´une personne sur le territoire du <pays>qui contrôle un système informatique produise à partir de données informatiques spécifiées ou d´une impression ou d´autres sorties intelligibles de ces données ;

(b) qu´un fournisseur de service Internet du <pays> produise des informations sur des personnes qui sont abonnées ou qui utilisent le service ; ou

(c) qu´une personne sur le territoire du<pays>qui a accès à un processus informatique spécifié compile les données informatiques spécifiées et les donne à une personne spécifiée.

Figure 5.7 : ordonnance concernant les données stockées de trafic, de l´abonné et du contenu



Source : questionnaire de l´étude sur la cybercriminalité. Q44, Q45, and Q46. (n=50, 49, 50)

51 Projet de loi type du COMESA, Art. 36(a) ; loi type du Commonwealth, Art.15 ; Convention sur la cybercriminalité du Conseil de l´Europe, Art 18(1)(a) ; textes législatifs types de l´UIT/CARICOM/CTU, Art.22(a) ; Convention de la Ligue des états arabes, Art. 25(1).52projet de loi type du COMESA, Art. 34(a)(ii) ; loi type du Commonwealth, Art.16 ;Convention sur la cybercriminalité du Conseil de l´Europe, Art. 17(1)(b) ; textes législatifs types de l´UIT/CARICOM/CTU, Art.24 ;Convention de la Ligue des états arabes, Art. 24.53 Questionnaire de l´étude sur la cybercriminalité. Q45-47.

Ceci peut être important quand de multiples fournisseurs de services sont impliqués dans le traitement des communications électroniques ou des données informatiques.La figure 5.7 montre qu´au niveau national, les pouvoirs généraux prédominent dans les pays, pour ce qui concerne l´autorisation des ordonnances relatives aux données du contenu, du trafic et de l´abonné.[53] La proportion des pays qui emploient des ordonnances spécifiques en matière de cybercriminalité pour obtenir les données de l´abonné est légèrement plus élevée que pour les deux autres catégories de données. Outre l´influence exercée par les instruments régionaux et internationaux sur la cybercriminalité, ceci peut aussi refléter une nécessité commune de ce type de données, et l´exigence exprimée par les fournisseurs de services de procédures et des pouvoirs juridiques clairs au moment de solliciter ces informations.

Ordonnance concernant les données de trafic : exemple national d´un pays d´Océanie

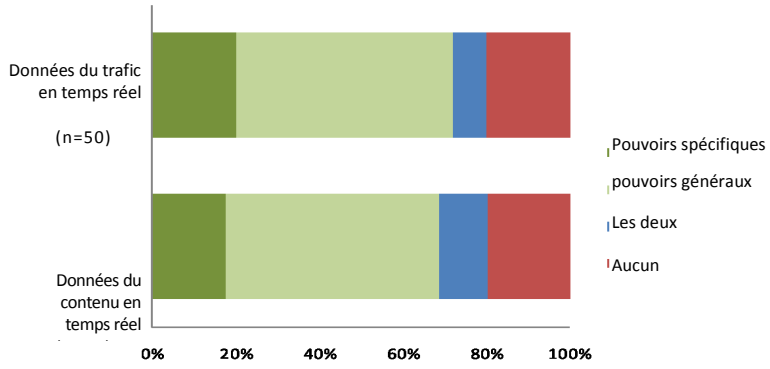
Divulgation des données de trafic

Lorsqu´un magistrat est satisfait sur la base d´une demande faite par un officier de police que des données informatiques spécifiques stockées dans un système informatique font l´objet d´une demande raisonnable pour les besoins d´une enquête criminelle ou de poursuites judiciaires, le magistrat peut ordonner à une personne qui contrôle le système informatique de divulguer les données de trafic suffisantes relatives à une communication spécifiée afin d´identifier :

(a) les fournisseurs de services ; et
(b) la voie par laquelle la communication a été transmise.

Ceci est corroboré par les commentaires des pays répondants. Un pays d´Amérique a, par exemple, déclaré que, bien que les fournisseurs de services coopèrent souvent de manière volontaire avec les services répressifs, l´application des dispositions procédurales générales existantes aux ordonnances de production des données était trop onéreuse et peu pratique. Le pays avait donc commencé le processus d´adoption de dispositions spécifiques en matière de cybercriminalité pour les ordonnances relatives aux données des abonnés.[54] par ailleurs, quelques pays signalèrent une utilisation réussie des dispositions générales. Un pays d´Asie du sud-est signala, par exemple, la possibilité d´étendre un pouvoir d´enquête général pour ordonner de produire « *tout document ou toute autre chose* ». Un pays d´Amérique du sud mentionna aussi que le pouvoir d´un juge d´ « *examinerla correspondance scellée* » avait été appliqué aux données stockées.[55]

Figure 5.8 : ordonnance concernant les données du contenu et les données du trafic en temps réel



Source : questionnaire de l´étude sur la cybercriminalité. Q47 et Q48. (n=50, 51).

Au-delà de la forme juridique des pouvoirs d´enquête, les interactions entre les services répressifs et les fournisseurs de service d´internet pour l´obtention de preuves électroniques peuvent être particulièrement complexes.Les dernières sections de ce chapitre examinent l´utilisation des pouvoirs *dans la pratique*, les bonnes pratiques utilisées par les services répressifsainsi que les difficultés auxquelles ils font face pour obtenir les données détenues par les fournisseurs de service.

54 Questionnaire de l´étude sur la cybercriminalité. Q42-51.
55 Questionnaire de l´étude sur la cybercriminalité. Q42-51.
56 Projet de loi type du COMESA, Art. 38 ; loi type du Commonwealth, Art. 19 ; Convention du Conseil de l´Europe sur la cybercriminalité, Art. 20 ; textes législatifs types de l´UIT/CARICOM/CTU, Art. 25 ; Convention de la Ligue des états arabes, Art. 28.
57 Projet de convention de l´Union africaine, Art. 3-55 ; projet de loi type du COMESA, Art. 39 ; loi type du Commonwealth Art. 18 ; Convention du Conseil de l´Europe sur la cybercriminalité, Art. 21 ; textes législatifs types de l´UIT/CARICOM/CTU, Art.26 ; convention de la Ligue des états arabes, Art. 29.

Collecte de données en temps réel

Les ordonnances relatives aux données représentent une mesure d´enquête permettant d´obtenir des données informatiques *stockées*. Des preuves électroniques essentielles peuvent toutefois ne pas être stockées (et exister seulement dans les communications transitoires), ou requérir une collecte en « temps réel »motivée par le caractère urgent, délicat ou complexe d´une enquête. Six instruments régionaux ou internationaux sur la cybercriminalité incluent donc des dispositions relatives à la collecte de données informatique en temps réel. A cet égard, les instruments font généralement unedistinction entre la collecte des données du trafic[56] et des données du contenu[57]en temps réel. Cette distinction se réfère aux différencesrelatives au degré d »intrusion dans la vie privée des personnes qui font l´objet de ces mesures.[58] La section sur les enquêtes et la vie privée examine de manière plus détaillée les éventuelles garanties qui peuvent être requises par les lois internationales sur les droits de l´homme. A cet égard, un instrument international, la Convention du Conseil de l´Europe sur la cybercriminalité mentionne explicitement l´interception des données du contenu dans le contexte « *d´une gamme d´infractions graves à définir dans le droit interne* ».[59] D´un point de vue pratique, les instruments multilatéraux stipulent souvent que la collecte des données en temps réel peut être effectuée directement par les services répressifs en utilisant leurs propres moyens techniques, ou en obligeant un fournisseur de service, dans le cadre de ses capacités techniques existantes, à collecter ou à enregistrer des données informatiques ou à coopérer et à aider les autorités à le faire .

Collecte de données en temps réel: exemple national d´un pays d´Asie de l´ouest

Collecte en temps réel de données du trafic

1. S´il est probable qu´une personne commette un délit au moyen d´un système informatique, un procureur est habilité à présenter une requête auprès d´un tribunal qui a juridiction sur le lieu de l´enquête, pour émettre une ordonnance qui exige la collecte des données du trafic en temps réel, obligeant par là même un fournisseur de service à coopérer et à aider l´organisme chargé de l´enquête à collecter en temps réel ou à enregistrer les données du trafic associées à des communications spécifiées faites et transmises au moyen d´un système informatique sur le territoire ...
2. Les requêtes prévues par le paragraphe 1 du présent Article devront tenir compte de la capacité technique du fournisseur de service en matière de collecte en temps réel et d´enregistrement des données du trafic. La durée de la collecte en temps réel et de l´enregistrement des données du trafic n´excèdera pas la durée nécessaire pour collecter des preuves dans une affaire pénale.
3. Les requêtes prévues par les paragraphes 1 et 2 du présent Article, seront prises en compte par le tribunal en conformité avec la procédure établie par l´Article <...>du présent Code.

Au niveau national, environ 40 % des pays répondants ont déclaré qu´un pouvoir d´enquête général état utilisé pour autoriser l´interception en temps réel des données du trafic et des données du contenu. De nombreux pays mentionnèrent, par exemple, l´application des lois générales sur l´interception des télécommunications ou des lois sur les écoutes, à la collecte des données informatiques en temps réel.[60] Dans l´ensemble, plus de 60 % des pays répondants signalèrent l´existence d´un pouvoir juridique relatif à la collecte des données informatiques en temps réel – que ce soit un pouvoir général ou un pouvoir spécifique en matière de cybercriminalité. Certains pays signalèrent que des garanties étaient appliquées à ces pouvoirs, comme le fait de limiter seulement aux délits graves la collecte des données informatiques en temps réel.[61] Pour ce qui concerne les aspects pratiques de l´interception des données, une distinction est souvent faite entre les fournisseurs de services privés et publics. La législation nationale d´un pays d´Europe de l´ouest spécifie, par exemple, que l´interception de données informatiques acheminées par des fournisseurs publics sera réalisée avec la coopération du prestataire de service à moins que cette coopération ne soit pas possible ou soit contraire aux intérêts de l´enquête. Dans le cas des fournisseurs de services privés, la législation nationale stipule que l´opportunité de collaborer dans l´interception sera « *offerte* » au prestataire de services à moins que cette coopération soit impossible ou indésirable.[62]

58 Voir Walden, I. *traiter le problème des données* : *le cadre juridique qui régit la criminalistique dans un environnement en ligne. Seconde Conférence internationale itrust 2004*, Procédures. Oxford, 29 mars-1 avril 2004.
59 Convention du Conseil de l´Europe sur la cybercriminalité, Art. 20.
60 Questionnaire de l´étude sur la cybercriminalité. Q47 et Q48.
61 *Ibid.*
62 Koops, B-J. 2010. Législation en matière de cybercriminalité. *Journal électronique de droit comparé*, 14(3).

Outils criminalistiques à distance

Logiciel criminalistique à distance : exemple national d´un pays d´Océanie

Accès à distance autorisé par un mandat pour rechercher une chose

Toute personne qui exécute un mandat de perquisition autorisant un accès à distance peut :

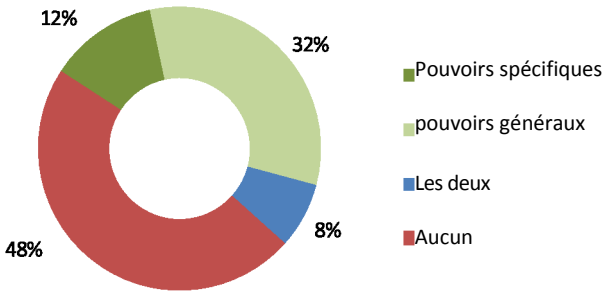
(a) utiliser des mesures raisonnables pour avoir accès à la chose recherchée ; et

(b) si un matériel intangible de cette chose fait l´objet de la perquisition ou peut être légalement saisi, reproduire ce matériel (y compris au moyen de la prévisualisation, la duplication ou toute autre méthode criminalistique).

Plusieurs outils technologiques offrent la possibilité aux organismes d´application de la loi de collecter directement à distance des preuves de systèmes informatiques, et de collecter des informations ou des informations liées à l´enquêtede manière plus générale. Les outils tels que les enregistreurs de frappe et les logiciels d´administration à distance, placés sur le dispositif d´un suspect, peuvent fournir des informations à distance sur l´activité du clavier et les données qui sont stockées, transmises ou reçues par le dispositif.[63] En raison des multiples informations personnelles stockées sur les dispositifs informatiques, l´utilisation de ces outils représente une intrusion significative dans la vie privée des personnes qui font l´objet d´une enquête. Des difficultés peuvent surgir lorsque les preuves sont obtenues en utilisant des outils à distance en direct sur des systèmes informatiques. Il peut, par exemple, être nécessaire de démontrer que les opérations effectuées par l´examinateur n´altèrent pas l´état du système qui fait l´objet d´une enquête.[64]

Un seul instrument régional ou international (non contraignant) mentionne l´utilisation d´outils criminalistiques à distance en tant que mesure d´enquête. Les textes législatifs types de l´UIT/CARICOM/CTU (Art. 27) stipulent qu´un juge peut autoriser un officier de police à utiliser « *un logiciel criminalistique à distance* » pour une tâche spécifique requise par une enquête. De manière plus générale, la Convention du Conseil de l´Europe relative à la protection des enfants (Art 30(5)) mentionne également l´obligation de prendre les mesures législatives et autres nécessaires permettant, le cas échéant, de mener des « *opérations clandestines* ».

Figure 5.9 : utilisation d´outils criminalistiques à distance



Source : questionnaire de l´étude sur la cybercriminalité. Q50. (n=40)

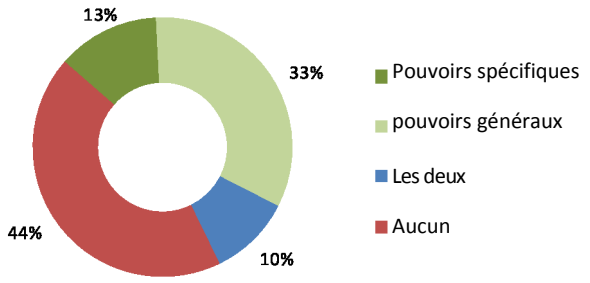
Plus d´un tiers des pays qui ont répondu au questionnaire de l´étude n´ont pas fourni de réponses relatives à l´existence d´une législation autorisant l´utilisation d´outils criminalistiques à distance lors des enquêtes menées par les services répressifs. Parmi les pays qui ont fourni une réponse, presque la moitié a signalé que ces pouvoirs n´existaient pas. Dans le cas des pays restants qui avaient indiqué que ces pouvoirs étaient inclus dans la législation, la majorité mentionnait des pouvoirs généraux plutôt que des pouvoirs spécifiques en matière de cybercriminalité. Certains pays ont explicitement déclaré que « *il n´y a aucune disposition législative pour... l´utilisation des outils criminalistiques à distance* », alors que d´autres ont confirmé que la législation nationale *« permet l´installation d´un dispositif de surveillance des données* ».[65] D´autres pays ont commenté de manière plus générale que les cadres procéduraux prévoient dans certaines circonstances d´utiliser « *une expertise technique ou scientifique* » afin d´obtenir les informations requises durant une enquête.[66]

63 Voir, par exemple, Gartner. 2012. Rapport sur la criminalistique à distance *2012*.
64 Hay, B., Nance, K., Bishop, M. 2009. Analyse directe : progrès et défis. *IEEE Sécurité et vie privée* 7(2) :32.
65 Questionnaire de l´étude sur la cybercriminalité. Q42-51.
66 *Ibid.*

Accès direct des services répressifs aux données extraterritoriales

Avec la connectivité globale, les données informatiques pertinentes pour les enquêtes menées par les organismes d´application de la loi – en matière de criminalité classique et de cybercriminalité– sont de plus fréquemment extraterritoriales hors de la juridiction d´enquête. Comme le mentionne le chapitre sept (coopération internationale), les moyens formels traditionnels de coopération internationale risquent de ne pas être suffisamment rapides pour garantir l´accès aux données extraterritoriales volatiles. Tenant compte de ces difficultés, trois instruments régionaux ou internationaux contiennent des dispositions sur l´accès « transfrontalier » aux données informatiques.[67]ces dispositions prévoient généralement que les services répressifs puissent avoir accès ou recevoir, au moyen d´un système informatique sur le territoire national, des données informatiques stockées dans un autre pays, avec le consentement légal et volontaire de la personne légalement autorisée à divulguer ces données.[68]

Figure 5.10 : accès transfrontalier à un système ou des données informatiques



Source : questionnaire de l´étude sur la cybercriminalité. Q51. (n=39)

Comme dans le cas des outils criminalistiques à distance, plus d´un tiers des pays n´a pas de fourni de réponse à la question de l´étude concernant l´existence de pouvoirs relatifs à l´accès transfrontalier. Parmi les pays qui ont répondu à cette question un peu plus de la moitié a indiqué que ce pouvoir existait. Les pays ont toutefois interprété le terme d´une manière large et ont inclus les cas où la mesure est autorisée par les autorités du pays dans lequel la mesure est mise en œuvre. Un pays a, par exemple, déclaré que la législation permet l´émission d´un mandat permettant l´installation de dispositifs de surveillance dans « *des objets/installations se trouvant à l´étranger* ». Toutefois, ceci peut être fait seulement si un « *juge... en délivrant le mandat est convaincu que la surveillance a été autorisée par le* « *consentement officiel approprié* » *du pays étranger* ».[69] Certains pays qui ont indiqué que des pouvoirs relatifs à l´accès transfrontalier étaient inclus dans la législation nationale, ont mentionné dans les commentaires écrits l´utilisation d´instruments d´entraide judiciaire. La proportion générale des pays qui ont mentionné un pouvoir législatif concernant l´accès transfrontalier dans le questionnaire de l´étude, est supérieure à la proportion des pays disposant du pouvoir d´autoriser l´accès transfrontalier au sens strict (c´est à dire sans l´autorisation des autorités nationales) prévu par certains instruments régionaux ou internationaux.

Le chapitre sept (coopération internationale) examine la question de l´accès direct des services répressifs aux données extraterritoriales de manière plus approfondie – en incluant l´utilisation policière de ces mesures dans la pratique.

---

67 Voir le projet de loi type du COMESA, Art. 49b ; Convention du Conseil de l´Europe sur la cybercriminalité, Art. 32b ; la Convention de la Ligue des états arabes, Art. 40(2).

68 « Les dispositions relatives à l´accès transfrontalier font généralement une distinction entre l´accès au matériel accessible au public (source ouverte) et les autres matériels.
L´accès au matériel accessible au public à des fins de justice pénale est devenu une pratique généralement acceptée (voir le Conseil de l´Europe. 2012. *L´accès transfrontalier et la juridiction : quelles sont les options ? Rapport du groupe transfrontalier adopté par le T-CY le 6 décembre 2012*). L´utilisation du terme « accès transfrontalier » dans cette étude concerne l´accès au matériel non accessible au public.

69 Questionnaire de l´étude sur la cybercriminalité. Q42-51.

Discussion

L´examen de la base juridique des pouvoirs d´enquête utilisés en matière de cybercriminalité (et pour tous les délits impliquant des preuves électroniques) révèle une grande diversité d´approches au niveau national. Elles vont de l´interprétation donnée aux pouvoirs « traditionnels » pour les appliquer aux données non-tangibles à l´existence des pouvoir juridiques relatifs aux mesures particulièrement intrusives, telles que les enquêtes criminalistiques à distance. Les approches nationales des pouvoirs d´enquête en matière de cybercriminalité ont une base commune moindre qu´en matière de d´incrimination de nombreux actes de cybercriminalité. Néanmoins, bien que les pouvoirs juridiques varient, il existe un consensus important quant aux *types* de mesures d´enquête qui *devraient* être disponibles. Ce sont des mesures relativement simples et correspondent à celles qui sont incluses dans de nombreux instruments multilatéraux– (i) les pouvoirs de perquisition et de saisie ; (ii) les pouvoirs permettant d´obtenir des données informatiques stockées ; (iii) les pouvoirs concernant la collecte des données en temps réel ; et (iv) les pouvoirs concernant la rapide conservation des données.

Outre la base juridique de ces pouvoirs, deux autres questions doivent être examinées – (a) les limites et les garanties qui devraient être appliquées à ces pouvoirs ; et (b) l´utilisation des mesures d´enquête dans la pratique. La prochaine section de ce chapitre examine les limites et les garanties dans l´optique des normes internationales des droits de l´homme sur la vie privée. Les sections suivantes du chapitre examinent l´utilisation des mesures d´enquête dans la pratique.

5.3 Vie privée et mesures d´enquête

PRINCIPAUX RÉSULTATS :

- presque tous les pays répondants signalent que les protections relatives à la vie privée sont applicables aux données informatiques et aux communications électroniques ;
- les pays signalent l´existence d´une vaste gamme de garanties pour la protection de la vie privée lors des enquêtes menées par les services répressifs, y compris la restriction des données auxquelles on peut accéder, les limites de temps, les exigences relatives àla cause probable, la surveillance des poursuites et la surveillance judiciaire ;
- les lois internationales sur les droits de l´homme établissent des protections claires pour les droits relatifs à la vie privée des personnes qui font l´objet d´une enquête. Parmi les principes essentiels il est établi que pouvoirs d´enquête doivent indiquer clairement les conditions et les circonstances dans lesquelles les mesures peuvent être utilisées, et des garanties efficaces contre les abus ;
- le développement de l´informatique en nuage introduit un haut niveau d´incertitude pour les usagers concernant le régime de protection de la vie privée qui s´appliquera à leurs données, et les circonstances dans lesquelles la vie privée pourrait etre légalement violée par les services répressifs à des fins d´enquête ou de surveillance de sécurité.

70 La Commission des stupéfiants des Nations Unies et la Commission pour la prévention du crime et la justice pénale. 2010. *Le contrôle des drogues, la prévention du crime et la justice pénale : depuis la perspective des droits de l´homme*. Note du directeur exécutif. E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1., 3 mars 2010.

71 Colvin, M., et Cooper, J. (eds.) 2009. *Les droits de l´homme dans l´enquête et la poursuite des crimes*. Oxford : Oxford University Press.

72 ICCPR, Arts. 9 et 14.

73 ICCPR, Art. 17 ; ECHR, Art. 8 ; ACHR, Art. 11.

74 Voir, par exemple, le Comité des droits de l´homme des Nations Unies. 1988. *Commentaire généralNo. 16 : le droit au respect de la vie privée, de la famille, du domicile et de la correspondance et la protection de l´honneur et de la réputation*, 8 avril 1998.

75 Voir, par exemple, le Comité des droits de l´homme des Nations Unies. *Communication CCPR/C/82/D/903/1999* ; IACtHR *Tristán Donoso.*
Jugement du 27 janvier 2009 ; et ECtHR demande n° 35394/97 et 13710/88.

Les droits de l´homme et les enquêtes des organismes d´application de la loi

Les lois internationales sur les droits de l´homme se préoccupent spécifiquement de la manière dont l´état atteint ses objectifs en matière de justice pénale et de prévention de la criminalité.[70] Tous les aspects de l´enquête et de la poursuite d´un crime peuvent mettre en cause les normes concernant les droits de l´homme, et les pratiques et les lois de procédure pénale font donc l´objet d´une attention spéciale des lois internationales sur les droits de l´homme. [71] Plusieurs droits sont potentiellement applicables lors des enquêtes menées par les services répressifs – dont les droits à la liberté et à la sécurité des personnes, et les droits à un procès équitable.[72] Cependant, les difficultés dans ce domaine proviennent souvent des protections sur la vie privée des lois nationales et internationales. L´ICCPR, l´ECHR et l´ACHR contiennent des interdictions relatives à l »ingérence arbitraire avec la vie privée, la famille, le domicile et la correspondance.[73] La portée du terme « vie privée » est vaste[74] conformément aux lois internationales et la jurisprudence montre clairement que le caractère intrusif des enquêtes pénales met en cause les droits sur la vie privée[75] – y compris lorsqu´un suspect ignore que des informations sont collectées,[76] et la seule existence d´une législation qui prévoit des mesures d´enquête entraîne ce risque.[77]

Comme c´est le cas pour de nombreux autres droits, les droits relatifs à la vie privée des lois internationales ne sont pas absolus et sont soumis à des limitations – y compris dans le cas de la ECHR pour ce qui concerne « *la prévention des troubles et de la criminalité* ».[78] A cet égard, les garanties des lois de procédure pénale telles que la définition des conditions et des circonstances dans lesquelles les pouvoirs d´enquête peuvent être utilisés ; l´identité des fonctionnaires qui les autorisent ; la modalité d´autorisation et la durée d´application des mesures d´enquête, sont essentielles pour une évaluation des droits de l´homme afin de vérifier si les enquêtes pénales qui portent atteinte à la vie privée sont licites et nécessaires.[79]

Quand il s´agit d´enquêtes en matière de cybercriminalité, chaque mesure d´enquête doit être évaluée dans son propre contexte juridique et pratique, afin de déterminer si son ingérence avec la vie privée, la famille, le domicile ou la correspondance d´une personne est justifiée. Bien que le caractère souvent clandestin et/ou électronique de la surveillance des techniques d´enquête en matière de cybercriminalité peuvent donner lieu à des difficultés relatives à vie privée,[80] il est important de rappeler que les exigences de proportionnalité des droits sur la vie privée s´appliquent également aux « simples » mesures de perquisition et de saisie.[81] les garanties et es limites des lois procédurales doivent donc refléter le degré variable d´intrusion des mesures d´enquête – en veillant à ce que chaque mesure soit utilisée seulement quand cela est nécessaire dans une société démocratique.

Existence de protections sur la vie privée et de garanties procédurales

Lors de la collecte d´informations pour l´étude, les pays répondirent aux questions concernant la protection juridique de la vie privée dans le contexte des données informatiques ou des communications électroniques et la mesure dans laquelle les droits sur la vie privée fonctionnaient comme des garanties lors des enquêtes menées par les services répressifs. On demanda également aux pays de préciser les circonstances dans lesquelles les droits sur la vie privée pouvaient être limités à des fins de détection et d´enquête sur la cybercriminalité, et les éléments du droit sur la vie privée liés à la coopération internationale et extra-juridictionnelle

76 Voir la ECtHR demande n°. 8691/79.

77 Voir la ECtHR demande n°. 54934/00.

78 Voir, par exemple, l´Article 8(2) de la EHCR qui prévoit que « *Il ne peut y avoir ingérence d »une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu »elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l »ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés « d'autrui* ».

79 L´approche générale adoptée par le Comité des droits de l´homme des Nations Unies est d´évaluer si une ingérence dans la vie privée est prévue par la loi, est en conformité avec les dispositions, les finalités et les objectifs de la convention et est raisonnable dans les circonstances d´un cas particulier (voir le Comité des droits de l´homme des Nations Unies. *Communication CCPR/C/82/D/903/1999* et le Comité des droits de l´homme. *Commentaire général n°. 16.*) l´approche de la ECtHR dans les cas d´enquêtes menées par les organismes d´application de la loi est de demander (i) lorsqu´il y a eu une ingérence avec les droits sur la vie privée protégés par l´Article 8 de la ECHR ; (ii) si l´ingérence était en conformité avec la loi – non seulement en se basant sur le droit interne mais aussi sur la « qualité » de la loi en termes d´accessibilité, de prévisibilité et de compatibilité avec l´état de droit ; et (iii) si l´ingérence était nécessaire dans une société démocratique (voir ECtHR demande n°. 62540/00).

80 Voir, par exemple, ONUDC. 2009. *Pratiques actuelles de surveillance électronique lors des enquêtes sur des délits graves et la criminalité organisée.*

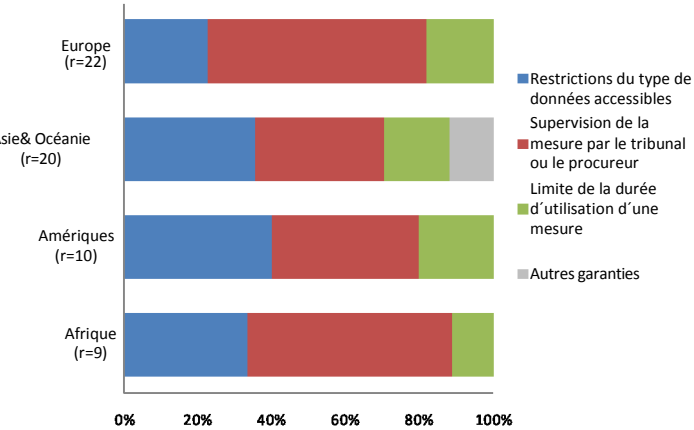
81 Voir, par exemple, ECtHR demande n°. 13710/88.

82 Questionnaire de l´étude sur la cybercriminalité. Q21.

Presque tous les pays répondantsont déclaré que les droits relatifs à la vie privée s´appliquent aux données informatiques et aux communications électroniques. Toutefois, la manière dont ces protections sont inscrites dans la loi, présente des différences considérables. Plusieurs pays ont mentionné des droits constitutionnels généraux sur la vie privée qui sont aussi appliqués aux données informatiques. Quelques pays soulignent même l´approche « technologiquement neutre » des droits sur la vie privée dans leur législation nationale. D´autres citent des législations spécifiques, qui incluent des lois sur « la vie privée » ; des lois sur « la protection de la vie privée » ; des lois sur « la réglementation des télécommunications » ; des lois sur « la protection de la vie privée dans les communications électroniques » ; les infractions « du code pénal » relatives à l´invasion de la vie privée ; des lois sur « la perquisition et la surveillance » ; des lois sur « la confidentialité de la correspondance » ; et des lois sur « le secret des communications ».[82] Certains pays ont mentionné des instruments internationaux, telle que la ECHR, comme étant des sources de protections nationales de la vie privée. Quelques nt déclaré explicitement n´avoir aucune loi générale sur la vie privée. Néanmoins, les données informatiques et les communications électroniques bénéficient dans ces pays de protections telles que les lois sur le privilège du secret professionnel et de la confidentialité.[83]

De nombreux pays ont confirmé que les protections relatives à la vie privée étaient applicables dans le contexte des enquêtes menées par les services répressifs, mais ont souligné le fait qu´il devait y avoir un équilibre entre les droits sur la vie privée et la nécessité de prévenir et d´enquêter sur les délits. Bien que certains pays aient décrit la manière dont cet équilibre a été atteint, la majorité des pays a seulement mentionné les exigences relatives aux mandats, au pouvoir de poursuivre ou au pouvoir judiciaire permettant la perquisition ou la surveillance intrusive. Un pays a précisé que la législation nationale précisait que « *une diligence raisonnable sera exercée [durant la perquisition et la saisie] afin d´éviter la divulgation de circonstances privées qui ne sont liées aux procédures pénales* ».[84] Un autre pays a signalé que l´écoute des communications doit être utilisé seulement comme un moyen « *supplémentaire* » de faciliter une enquête pénale. Certains pays ont notamment déclaré que les lois sur la protection des données (qui jouent un rôle important pour la protection de la vie privée pour ce qui concerne les données personnelles contrôlées et traitées par des tierces parties) contiennent des exceptions qui permettent, par exemple, aux tierces parties de transmettre des informations à un organisme d´application de la loi si cela est « raisonnablement nécessaire » pour l´application du droit pénal.[85]

Figure 5.11 : limites et garanties des enquêtes



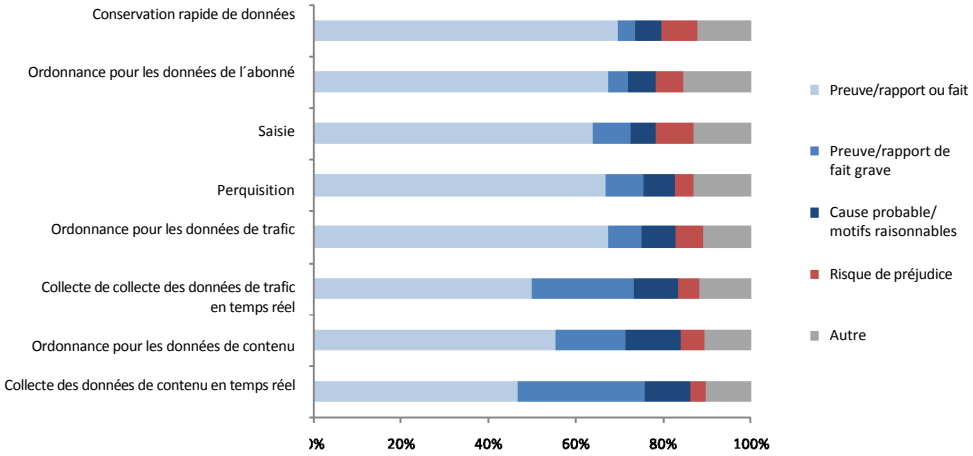
Source : questionnaire de l´étude sur la cybercriminalité Q100. (n=45, r=61)

Le questionnaire de l´étude sollicitait des détails supplémentaires relatifs à la nature des garanties procédurales aidant à assurer le respect des droits de l´homme et du droit à la vie privée lors du processus d´enquête des officiers des services répressifs.

83 *Ibid.*
84 *Ibid.*
85 *Ibid.*
86 Questionnaire de l´étude sur la cybercriminalité. Q100.
87 *Ibid.*
88 *Ibid.* Il faut noter que les pays de l´Union Européenne Union sont soumis à la Décision cadre du Conseil2008/977/JHA du 27 novembre 2008 sur la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale, qui règlemente le traitement des données personnelles réalisé par ces autorités.

La majorité des états (85 %) répondit à cette question en spécifiant qu´il existait des garanties et des limites nationales pour les mesures d´enquêtes en matière de cybercriminalité utilisées par les services répressifs.[86] Étonnamment, quelques pays déclarèrent que ces garanties *n´existaient pas* – et cette situation pourrait causer une incompatibilité avec les lois internationales sur les droits de l´homme. Les garanties mentionnées incluent des restrictions relatives au type de données personnelles auxquelles les services répressifs peuvent avoir accès, et à la supervision des mesures d´enquête par le tribunal ou le procureur. Certains états mentionnent aussi le délai d´utilisation fixé des mesures d´enquête.[87] D´autres pays citent des régimes de protection qui incluent des limitations d´accès aux données informatiques après avoir été obtenues par les services répressifs, des limitations quant à leur utilisation, des exigences relatives à leur destruction, et des mécanismes internes et indépendants de surveillance.[88] Un pays déclara que « *une ample variété de limitations et de garanties est applicable, et divers régimes de limitations et de garanties sont effectivement appliqués à chaque pouvoir d´accès (données de télécommunications, contenu stocké et contenu en direct). Ces régimes incluent des exigences qui doivent être remplies avant que l´accès ne soit accordé, ainsi que des limitations sur l´accès accordé, des limitations sur l´utilisation du matériel obtenu, des exigences relatives à la destruction, des régimes de surveillance interne et indépendante, et des exigences des exigences en matière de rapports publics* ».[89]

Figure 5.12 : exigences légales relatives à l´utilisation des mesures d´enquête

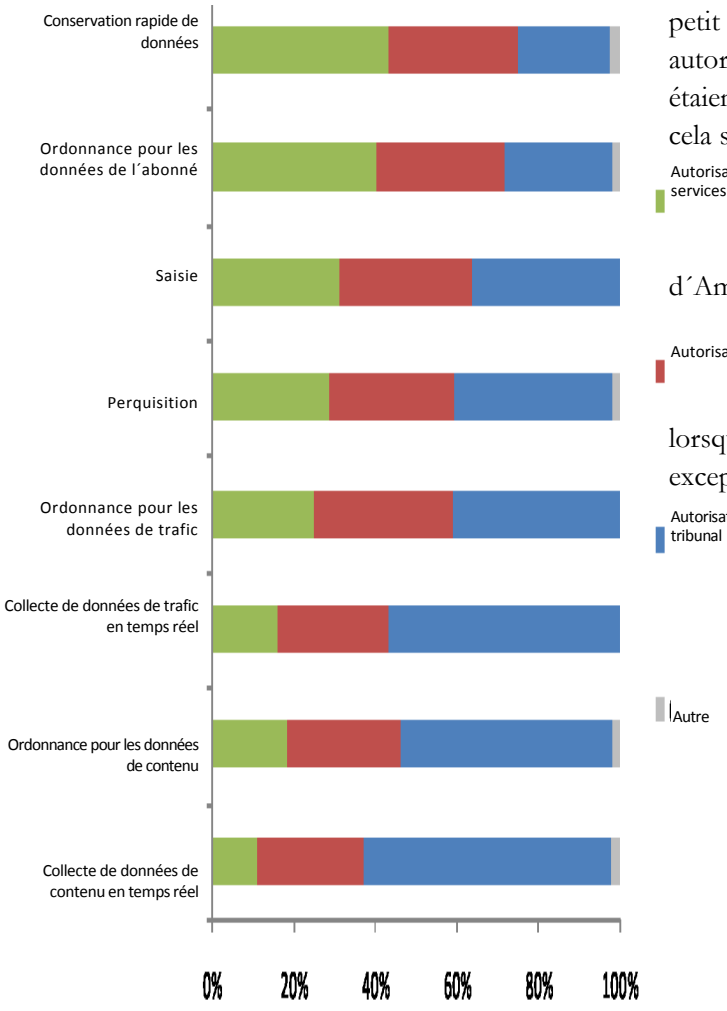


Source : questionnaire de l´étude sur la cybercriminalité. Q87-96. (n=51)

La majorité des pays (environ 75 %), déclarèrent que les garanties étaient prévues dans la législation primaire et les pays restants signalèrent que les garanties découlaient de législations secondaires, de décrets exécutifs, de décisions du tribunal ou de politiques du parquet ou des services répressifs.[90] Bien que les garanties puissent légitimement provenir de sources autres que la législation primaire, elles doivent toutefois– comme cela est mentionné ci-après– être établies par des lois qui fournissent des garanties appropriées et efficaces contre les abus des propres mesures d´enquête .On demanda également aux pays de fournir des détails sur des garanties procédurales spécifiques. Ceci incluait la nature des exigences légales à satisfaire avant qu´une mesure d´enquête ne puisse être utilisée, ainsi que l´identité de l´autorité qui les autorisait. Pour ce qui concerne les exigences procédurales, la majorité des pays signala que de nombreuses mesures d´enquête pourraient être mises en œuvre sur la base de « *preuve ou d´un rapport sur un acte de cybercriminalité* ».[91] Pour ce qui concerne les mesures dont le degré d´intrusion est plus élevé, comme la collecte des données en temps réel ou la collecte des données du contenu, les pays exigent généralement des preuves ou un rapport sur un cyber délit « *grave* », ou des exigences procédurales comme la démonstration d´un « *cause probable* » ou de « *motifs raisonnables* » pour soupçonner qu´une infraction a été commise.[92]

Un patron similaire a été observé pour ce qui concerne l´identité des autorités qui autorisent les différentes mesures d´enquête. Les pays ont fréquemment signalé que des mesures relativement moins intrusives, comme, par exemple, la conservation rapide des données ou les ordonnances concernant les données des abonnés, pouvaient être ordonnées par les autorités chargées de l´application de la loi, par rapport à des mesures plus intrusives.[93] Plus de 80 % des pays répondants ont, par exemple, déclaré que les mesures intrusives telles que les ordonnances relatives aux données du contenu ou la collecte de données en temps réels requéraient l´autorisation du parquet ou du tribunal, et non directement par le biais des agents des services répressifs. Toutefois, un petit nombre de pays a signalé que les autorités chargées de l´application de la loi étaient habilités à autoriser ces enquêtes– et cela soulève des préoccupations potentielles sur la présence de garanties suffisantes pour ces mesures. Un pays d´Amérique a, par exemple, signalé qu´un article de son droit procédural, qui prévoyait l´interception sans mandat lorsqu´il existait des circonstances exceptionnelles, avait été déclaré anticonstitutionnel par la Cour suprême.[94]

Figure 5.13 : autorisation des mesures d´enquête



Source : questionnaire de l´étude sur la cybercriminalité. Q87-96. (n=51)

89 Questionnaire de l´étude sur la cybercriminalité.Q100.
90 *Ibid.*

91 Questionnaire de l´étude sur la cybercriminalité. Q87-96.

92 *Ibid.*

Évaluer les garanties sous l´angle des droits de l´homme

La jurisprudence des cours et des tribunaux internationaux des droits de l´homme met l´accent sur le fait que les protections en matière de procédures sont essentielles pour respecter la vie privée dans le cadre des enquêtes menées par les services répressifs. Le tableau présente les principales dispositions internationales sur les droits relatifs à la vie privée, ainsi que les décisions en matière de droits de l´homme liées à des questions telles que l´absence d´une législation autorisant des mesures d´enquête ; les garanties législatives et l´utilisation des mesures d´enquête dans la pratique. Jusqu´à présent, peu de décisions internationales sur les droits de l´homme ont directement abordé les enquêtes des services répressifs sur la cybercriminalité .[95]

Un important jugement prononcé par la ECtHR a toutefois pris en compte l´équilibre entre le droit à la vie privée et les enquêtes des services répressifs. Dans ce contexte d´une infraction liée au contenu en ligne et qui impliquait un mineur, les organismes chargés de l´application de la loi ne purent obtenir les données de l´abonné d´un fournisseur de services en raison des protections de la confidentialité contenues dans la loi sur les télécommunications. La Cour considéra que cela empêcha que des mesures efficaces soient prises pour identifier et poursuivre le délinquant.[96]

Bien que la liberté d'expression et la confidentialité des communications soient des considérations primordiales, et que les utilisateurs de télécommunications et de services sur internet doivent avoir la garantie que leur intimité et leur liberté d'expression sont respectées, cette garantie ne peut être absolue et doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions….. Il incombe au législateur de fournir un cadre qui concilie les différentes revendications qui concourent à la protection dans ce contexte.

ECtHR demande No. 2872/02

Dispositions des lois internationales sur les droits de l´homme
ICCPR, Article 17, ECHR Article 8, ACHR Article 11 [Nul ne sera l´objet d´immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance (ICCPR)] [toue personne a droit au respect de a vie privée et familiale, de son domicile et de sa correspondance (ECHR)] [Nul ne peut être l´objet d´ingérences arbitraires ou abusives dans sa vie privée, dans la vie de sa famille, dans son domicile ou sa correspondance (ACHR)]
Absence de législationautorisant les mesures d´enquête
ECtHR demande n°. 8691/79 En l´absence de règles juridiques, le fait pour un fournisseur de services de télécommunications de transmettre volontairement à la police, sur sa demande, les registres des numéros de téléphone composés et de la durée des appels quand cela « est fondamental pour les enquêtes policières et est lié à un délit grave » a été jugéincompatible avec le droit à la vie privée. La cour souligna l´absence de règles juridiques relatives à l´étendue et les modalités d´exercice du pouvoir d´appréciation.
ECtHR demande n°. 47114/99 L´interception de messages de téléavertisseurs par les services répressifs qui utilisèrent un « clone » du téléavertisseur d´un suspect en l´absence de lois régulant l´interception des messages de téléavertisseurs, fut jugée incompatible avec le droit à la vie privée. La cour signala que le droit interne doit prévoir la protection contre les ingérences arbitraires avec le droit à la vie privée.

93 *Ibid.*
94 *Ibid.*
95 Bien que la ECtHR ait, par exemple, considéré la surveillance des courriels et de l´usage d´internet dans un contexte professionnel. Voir la demande n°. 62617/00 de la ECtHR. Dans ce cas, la cour a appliqué des tests pour déterminer une éventuelle ingérence dans la vie privée et (si c´est le cas), pour déterminer si l´ingérence était en conformité avec la loi.
96 ECtHR demande n°. 2872/02.

De nombreuses autres décisions sont particulièrement importantes dans le contexte des enquêtes sur la cybercriminalité. Dans le système européen, le fait pour un fournisseur de services de télécommunications de transmettre volontairement à la police des registres téléphoniques a été jugé incompatible avec le droit à la vie privée, en l´absence de règles juridiques spécifiques.[97] De même, en Amérique, l´enregistrement des conversations téléphoniques autorisé par une simple annotation judiciaire et n´étant pas en rapport avec une enquête établie a été jugé comme une violation au droit à la vie privée.[98]

Garanties législatives pour les mesures d´enquête
UN-HRC Communication CCPR/C/82/D/903/1999 L´interception et l´enregistrement des données du trafic sur l´autorisation écrite d´un juge d´instruction, dans le cadre de l´enquête judiciaire préliminaire sur l´implication d´un individu dans une organisation criminelle, ne furent pas considérés comme une violation du droit à la vie privée. Le Comité souligna que la législation habilitante précisait les circonstances exactes dans lesquelles l´ingérence pouvait être permise et que l´ingérence était proportionnée et nécessaire pour atteindre l´objectif légitime de lutte contre la criminalité.
ECtHR demande No. 2872/02 Le manque d´une enquête pénale efficace en raison de l´absence d´une disposition juridique explicite autorisant la divulgation des données de télécommunications dans le cas d´une infraction liée au contenu en ligne fut jugé incompatible avec les obligations positives du droit à la vie privée. La Cour souligna que la victime n´avait pas bénéficié d´une protection efficace.
ECtHR demande No. 62540/00 Les dispositions d´une loi nationale régulant les mesures de surveillance secrète furent jugées incompatibles avec le droit à la vie privée. La Cour souligna que la loi ne prévoyait pas qu´un organisme officiel ou externe examine la mise en œuvre des mesures; qu´elle n´établissait pas de procédures pour préserver l´intégrité et la confidentialité de la preuve obtenue, ni de procédures pour sa destruction; et que le contrôle général de la surveillance reposait sur un membre de l´exécutif au lieu d´un organisme indépendant.
Mesures d´enquête dans la pratique
IACtHR *Escher* Jugement du 6 juillet 2009 L´enregistrement de conversations téléphoniques réalisé par l´état et leur diffusion postérieure sans respecter pleinement les exigences légales furent jugés incompatibles avec le droit à la vie privée. La Cour souligna que la demande de surveillance n´était pas liée à une enquête de police établie ni à des procédures pénales. La Cour souligna aussi que l´interception était autorisée par une simple annotation judiciaire qui ne précisait pas la durée d´application de la mesure ou les exigences procédurales.
ECtHR demande No. 13710/88 Une perquisition, empiétant sur le secret professionnel d´un cabinet d´avocat, réalisée conformément à un mandat large autorisant la perquisition et la saisie de 'documents' fut jugée incompatible avec le droit à la vie privée. La Cour estima que la mesure n´était pas proportionnée à l´objectif poursuivi.

Il est probable que les principes existants de ces cas soient appliqués à de futurs cas en matière de cybercriminalité. La perquisition d´un système informatique pour rechercher des fichiers, ou la surveillance secrète des courriels ou du trafic IP, par exemple, montre des similitudes avec la perquisition et l´écoute classiques. Le fait pour un fournisseur de services internet de fournir des données aux autorités chargées de l´application de la loi (conformément à un accord informel de coopération, ou à un mandat, une injonction de produire ou toute autre ordonnance légale) est équivalent pour les fournisseurs de services de télécommunications. En particulier, l´accès potentiel à une vaste gamme d´informations personnelles lors des enquêtes sur un cyberdélit –y compris des courriels, des appels VOIP, les historiques de navigation sur internet et des photographies– présente un degré d´intrusion très élevé. Dans plusieurs cas, lorsque les registres sont sollicités à un fournisseur de services internet ou lorsque la collecte de données en temps réel est autorisée, la personne faisant l´objet de l´enquête ignorera probablement l´existence d´une enquête ainsi que la nature et l´étendue des données collectées, et cela met implique la jurisprudence en matière de droits de l´homme dans le cadre de la surveillance secrète.[99]

97 ECtHR demande n°. 8691/79
98 IACtHR *Escher* Jugement du 6 juillet 2009.
99 Outre les cas présentés dans le tableau, voir aussi la demande n°. 54934/00 de la ECtHR.

Dans ces circonstances– causées par la vulnérabilité résultant d´un usage abusif – les tribunaux régionaux des droits de l´homme ont recommandé une grande prudence.[100] Les approches en matière de garanties et de vie privée mentionnées par les pays dans le questionnaire de l´étude –et, la variété de situations présentées auprès des tribunaux internationaux des droits de l´homme – montre une grande diversité dans la protection de la vie privée durant les enquêtes menées par les services répressifs. L´examen des décisions *nationales* pertinentes sur la vie privée souligne ce point. Les décisions nationales sur la procédure concernant l´accès des services répressifs aux données des abonnées détenues par les fournisseurs de services internet, par exemple, vont du fait de considérer que la demande adressée par la police à un fournisseur de services internet pour obtenir les données de l´abonné *sans* autorisation judiciaire est *compatible* avec les attentes en matière de protection de la vie privée des usagers, au fait de juger qu´un processus judicaire approprié est *requis* par les droits relatifs à la vie privée. [101]

Comme dans le cas d´une évaluation des droits de l´homme en matière d´incrimination, les lois internationales sur les droits de l´homme international sont à même, dans une certaine mesure, d´adapter ces différences par le biais de la doctrine comme pour la marge d´appréciation.[102] Toutefois, il est clair que les approches nationales divergentes sur la vie privée représenteront un problème croissant dans le contexte des enquêtes transnationales des services répressifs et des avancées telles que l´informatique en nuage.

La vie privée, la juridiction et l´informatique en nuage

Le traitement des données en nuage met en jeu de multiples centres de données, répartis parmi diverses juridictions nationales, et avec divers responsables privés du contrôle et du traitement des données.[103] Dans les conditions actuelles, bien qu´il soit techniquement possible de connaître la localisation des données, les usagers de l´informatique en nuage ne savent pas toujours exactement « où » se trouvent leurs données. Ainsi les approches juridictionnelles relatives au régime de *protection des données* qui régit les données détenues par les fournisseurs de services informatiques en nuage, et *la loi de procédure pénale* qui régit les enquêtes nationales menées par les services répressifs sont complexes.[104]

Ceci introduit une grande incertitude juridique pour les usagers, quant au régime concernant la vie privée qui sera appliqué à leurs données et aux circonstances dans lesquelles le respect de la vie privée peut être violé à des fins d´enquêtes des services répressifs ou de surveillance de sécurité. La législation de certains pays contient, par exemple de vastes pouvoirs relatifs à la surveillance applicables, sans autorisation judiciaire, aux données de non ressortissants hébergées sur des serveurs dans les nuages dans leur juridiction nationale.[105]Si les garanties nationales sur la vie privée font des distinctions entre ressortissants et non ressortissants,[106] les usagers peuvent (i) ne pas avoir connaissance de ces actions ; et (ii) n´avoir aucun recours juridique, conformément au droit du pays qui applique ces mesures d´enquête ou– selon l´application juridictionnelle des lois de leurs pays (et la structure de constitution juridique du fournisseurs d´informatique en nuage) – ni dans leurs propres pays.

100 La ECtHR considère, par exemple, que « *les pouvoirs concernant la surveillance secrète exercée sur les citoyens, caractérisant un état policier, n´est tolérable d´après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* ». ECtHR demande n°. 28341/95.

101 Voir, par exemple, *R v Ward*, 2012 ONCA 660 et*l´état contre. Reid*, 194 N.J. 376 (2008).

102 Legg, A., 2012. *La marge d´appréciation des lois internationales sur les droits de l´homme*. Oxford : Oxford Monographies de droit international.

103 Pour les concepts des responsable du « contrôle » et du « traitement » des données, voir la Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 sur la protection des individus concernant le traitement des données personnelles et le libre mouvement de ces données (telle qu´amendée par la Régulation (EC) n°. 1882/2003 du Parlement européen et du Conseil du 29 septembre 2003).

104 Voir, par exemple, la Direction générale des politiques internes du Parlement européen, Droits des citoyens et affaires constitutionnelles. 2012. *Lutter contre la cybercriminalité et protéger la vie privée dans le nuage.*

105 *Ibid.*

106 Voir, par exemple, *Verdugo-Urquidex* 494 U.S. 259 (1990) et USFISCR n°. 08-01.

Les divergences dans la juridiction des lois sur la vie privée sont suggérées par les réponses fournies au questionnaire de l´étude. Les pays répondants ont signalé de multiples positions juridiques concernant l´application extraterritoriale des protections nationales de la vie privée. Quelques pays ont commenté que les protections relatives à la vie privée avaient un effet extraterritorial, y compris dans des conditions où l´acte ou la pratique commis hors du territoire avait toutefois un « *lien organisationnel* » avec le pays. D´autres pays signalèrent que les lois nationales sur la vie privée n´étaient pas applicables aux données informatiques ou aux communications électroniques en temps réel ou stockées hors du territoire. Un pays déclara que ceci était une « *question ouverte quant à savoir si le matériel informatique localisé à l´étranger bénéficie de la même protection à la vie privée que le matériel informatique localisé sur un serveur [sur le territoire]* ».[107] La majorité des pays répondants coïncidaient néanmoins sur le fait que les protections nationales sur la vie privée étaient applicables aux mesures d´enquêtes menées sur le territoire à la demande de services répressifs étrangers. Un pays signala, par exemple, que « *lorsqu´une demande d´entraide judiciaire d´un pays étranger interfère avec les lois nationales qui protègent la vie privée, cette demande peut être rejetée* ».[108]

Un travail récent effectué par le Parlement européen conclut que « *dans le domaine de la cybercriminalité, les défis en matière de protection de la vie privée dans le contexte de l´informatique dans les nuages sont sous-estimés, si ce n´est ignorés* ».[109] Bien que les pays aient développé diverses garanties relatives à la vie privée concernant les mesures mises en œuvre par les services répressifs dans le contexte nationale, ces garanties sont variées et peuvent ne pas être facilement conciliables dans des cas d´enquêtes transnationales sur la cybercriminalité – et pourraient éventuellement entraîner des conflits juridiques ou des lacunes juridictionnelles. Étant donné que les pays s´efforcent de promulguer des lois qui tiennent compte de l´équilibre délicat entre la vie privée des individus et la prévention et le contrôle de la criminalité, il est fondamental que les lois nationales reflètent un état de droit commun et les principes des droits de l´homme pour les mesures d´enquête des services répressifs.

Un point de départ important se trouve dans la jurisprudence des droits de l´homme mentionnée précédemment et résumée dans l´encadré– qui établit des règles claires du principes du droit pour les lois relatives à la surveillance. Cependant, même ces principes doivent encore faire face aux difficiles questions des transferts de données extraterritoriaux. À cet égard, bien que l´harmonisation des normes sur la vie privée aide à augmenter la prévisibilité de l´accès des services répressifs, y compris des autorités étrangères, aux données des usagers, les pays devront également s´occuper de plus en plus de la portée juridictionnelle des protections nationales de la vie privée. Ceci exige de s´assurer que : (i) l´appui donné aux enquêtes des services répressifs étrangers est soumis aux normes nationales sur la vie privée ; et (ii) ces causes d´action sont disponibles pour les personnes hors des juridictions nationales qui sont affectées par les actions des autorités répressives de ce pays.

Règle des principes du droit pour les lois sur la surveillance

- La loi doit être suffisamment claire et indiquer de manière appropriée les conditions et les circonstances dans lesquelles les autorités sont habilitées à utiliser des mesures d´enquête, ainsi que :
    - la nature des infractions qui peuvent donner lieu à l´utilisation de la mesure ;
    - une définition des catégories de personnes susceptibles de faire l´objet de cette mesure
    - une limite de la durée de la mesure ;
    - la procédure à suivre pour examiner, utiliser et stocker les données obtenues ;
    - les précautions à prendre lorsque les données sont communiquées à d´autres parties ;
    - les circonstances dans lesquelles les données obtenues peuvent ou doivent être effacées ou détruites.
- Des garanties adéquates et efficaces contre l´abus doivent exister, et tenir compte de :
    - la nature, la portée et la durée des éventuelles mesures ;
    - les motifs requis pour les ordonner ;
    - les autorités compétentes qui les autorisent, les appliquent et les supervisent ;
    - les recours prévus par la législation nationale.
- Les lois devraient prévoir l´examen ou la surveillance de la mise en œuvre des mesures, par un organisme ou un fonctionnaire externe aux services qui appliquent la mesure ou dont les qualifications assurent l´indépendance.
- Les lois devraient prévoir, qu´aussitôt qu´une notification peut être faite sans compromettre l´objectif poursuivi par la mesure, les informations devraient etre fournies aux personnes concernées.

ECtHR demande n°. 62540/00

107 Questionnaire de l´étude sur la cybercriminalité. Q21.
108 *Ibid.*
109 Direction générale des politiques internes du Parlement européen, Droits des citoyens et affaires constitutionnelles. 2012. *Lutter contre la cybercriminalité et protéger la vie privée dans le nuage*

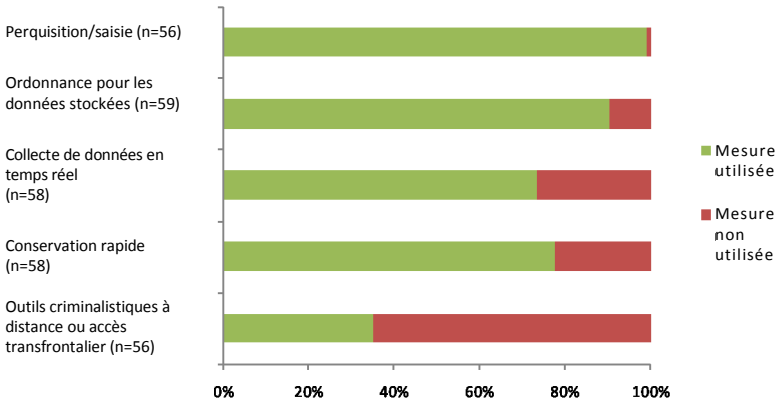
5.4 Utilisation des mesures d´enquête dans la pratique

PRINCIPAUX RÉSULTATS :

- indépendamment de la forme juridique des pouvoirs d´enquêtes, toutes les autorités qui ont répondu au questionnaire utilisent la perquisition et la saisie pour l´appropriation physique du matériel informatique et la capture des données informatiques ;
- la majorité des pays utilisent également des ordonnances pour que les fournisseurs de services internet leur transmettent les données informatiques stockées, pour la collecte de données en temps réel e la conservation rapide des données ;
- les autorités chargées de l´application de la loi font face à de nombreuse difficultés dans la pratique, parmi lesquelles se trouvent les techniques employées par les délinquants pour cacher ou éliminer les données informatiques liées à une infraction.

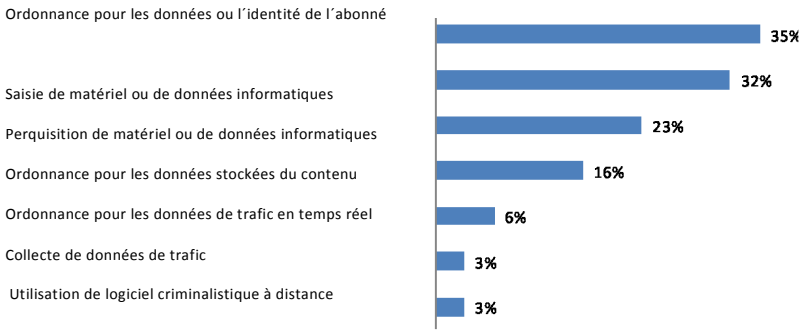
Indépendamment de la forme juridique des pouvoirs, les organismes d´application de la loi qui ont répondu au questionnaire de l´étude ont indiqué qu´un éventail de mesures d´enquête– de la perquisition et la saisie, à la conservation rapide des données– sont amplement utilisées dans la pratique. Presque tous les pays ont, par exemple, mentionné la perquisition et la saisie pour l´appropriation physique du matériel informatique et la capture des données informatiques. Les réponses fournies par des agents des services répressifs suggèrent aussi que plus de 90 % des pays utilisent des ordonnances pour obtenir des données informatiques stockées. Environ 80 % des pays répondants ont mentionné avoir utilisé des mesures de conservation rapide des données.[110] Coïncidant avec la faible proportion des pays qui ont signalé des pouvoirs juridiques pertinents, moins de 40 % des pays ont utilisé un accès à distance.[111]

Figure 5.14 : Utilisation des mesures d´enquête des services répressifs



Source : questionnaire de l´étude sur la cybercriminalité. Q87-97. (n= 56, 59, 58)

Figure 5.15 : mesures d´enquête plus fréquemment utilisées



Source : questionnaire de l´étude sur la cybercriminalité. Q98. (n=31, r=37)

110 Questionnaire de l´étude sur la cybercriminalité. Q87-96.
111 Questionnaire de l´étude sur la cybercriminalité. Q87-96.
112 Voir la Section 5.2 aperçu des pouvoirs d´enquête.

Ces réponses coïncident avec l´existence signalée de pouvoirs juridiques, les pays ont mentionné l´utilisation de la conservation rapide des données *dans la pratique* un peu plus fréquemment que les réponses sur l´existence des *pouvoirs juridiques* ne le laissait entendre.[112] Ceci peut indiquer que dans la pratique la conservation rapide des données a lieu par le biais de relations *informelles* entre les organismes d´application de la loi et les fournisseurs de services.

Les réponses des pays concernant les pouvoirs d´enquête les *plus utilisés*soulignèrent aussi l´importance de la perquisition et de la saisie, ainsi que l´utilisation d´ordonnances pour obtenir les données de l´abonné des fournisseurs de services. Étant donné que de plus en plus de dispositifs sont connectés à l´internet, les données informatiques qui étaient antérieurement stockées sur un dispositif informatique local sont de plus en plus fréquemment traitées par des fournisseurs de services du secteur privé, et cela inclut les services d´informatique en nuage. L´importance pour les fonctionnaires des services répressifs que les fournisseurs de services leur transmettent des preuves électroniques, est illustrée par le fait que les ordonnances concernant les données de l´abonné sont les mesures d´enquête les plus fréquemment utilisées. La section relative aux enquêtes et au secteur privé examine de manière détaillée les interactions entre les organismes d´application de la loi et les fournisseurs de services.

Les difficultés et les bonnes pratiques en matière d´enquête

Les pays répondants ont identifié plusieurs difficultés et bonnes pratiques liées à l´utilisation des mesures d´enquête et aux enquêtes sur la cybercriminalité en général. Les bonnes pratiques mentionnées par les pays soulignent fréquemment l´importance de l´organisation minutieuse des enquêtes. Un pays a, par exemple, signalé que « *la conservation des données et la saisie des données informatiques et des données stockées dans des conditions criminalistiques rigoureuses est un point de référence pour des enquêtes sur la cybercriminalité réussies* ».[113] Un autre pays déclara que « *toutes les mesures devraient être enregistrées et laisser une piste vérifiable. La date et l´heure de chaque action URL, adresse e-mail, etc., devraient être notés, et les informations sur les sources et les contacts devraient être enregistrées* ».[114] De plus de nombreux pays ont signalé que le point de départ d´enquêtes réussies était fréquemment des informations telles que des adresse IP. Par conséquent se concentrer sur l´obtention opportune des données de l´abonné était considéré une bonne pratique.[115]

Pour ce qui concerne les difficultés, plusieurs pays répondants soulignèrent, dans les remarques formulées sur les enquêtes des services répressifs sur la cybercriminalité, un niveau croissant de sophistication criminelle, et le besoin, lors des enquêtes menées par les services répressifs, de se « mettre à jour » avec les auteurs des cyber délits. Un pays d´Europe a, par exemple, signalé que « *les attaques sont devenues de plus en plus sophistiquées, il est de plus en plus difficile de les détecter et en même temps les techniques trouvent rapidement leur chemin vers une audience plus vaste... nous voyons aussi que les éléments numériques (c´est à dire, la cible ou la scène du crime) deviennent de plus en plus importants dans n´importe quel délit* ».[116] Un autre pays souligna que *l´augmentation de l´incidence des cyberdélits était causé par les progrès des outils techniques et de programmation disponibles pour les délinquantsgrâce à un marché illicite de commercialisation d´outils permettant de commettre des cyberdélits* ».[117]

Des niveaux croissants de sophistication entraînent des difficultés accrues dans des domaines tels que la localisation de preuves électroniques ; l´utilisation de techniques d´obfuscation des délinquants ; des difficultés causées par les grands volumes de données à analyser ; et des difficultés pour que les fournisseurs de services communiquent des données.

113 Questionnaire de l´étude sur la cybercriminalité. Q99.
114 *Ibid.*
115 *Ibid.*
116 Questionnaire de l´étude sur la cybercriminalité. Q85.
117 Questionnaire de l´étude sur la cybercriminalité. Q84.
118 Questionnaire de l´étude sur la cybercriminalité. Q87-96.

Au niveau de base de l´enquête, par exemple, le stockage numérique et la connectivité sont de plus en plus fréquemment intégrés aux objets personnels et aux articles ménagers courants, tels que des stylos, des caméras, des montres avec un stockage flash et des bijoux avec des unités flash USB. De plus, les dispositifs de stockage sans fil peuvent être dissimulés dans les cavités murales, les espaces du plafond et du sol. Comme le signalait un pays, ces *facilités de dissimulation* physiques et électroniquesdes données informatiques pouvaient entraîner des difficultés pour les enquêtes.[118] Les pays ont également mentionné des problèmes de « *suppression des données des dispositifs de stockage* ». Lorsque les délinquants utilisent les services de communication en ligne, comme les VOIP, les données informatiques peuvent circuler directement d´usager à usager data (et non à travers les serveurs des fournisseurs de services)[119]et cela implique que seules les copies locales de certaines données sont disponibles–et vulnérables à une suppression ultérieure. De plus les auteurs des infractions peuvent utiliser des « boites aux lettres mortes » dans les dossiers brouillon des comptes de courriel (cela permet des communicationssans un courriel « envoyé »), et utiliser aussi des ponts d´accès Wifi publics gratuits, ou des cartes de crédit et des mobiles prépayés. Un pays a, par exemple, souligné les difficultés pouridentifier une localisation à cause de la « *disponibilité de nombreux points d´accès gratuits* ».[120] Plusieurs pays ont également mentionné que les auteurs des infractions utilisent des techniques d´encodage et d´obfuscation. Ces points sont traités de manière détaillée au chapitre Six (preuves électroniques et justice pénale). Enfin plusieurs pays ont mentionné qu´ il était difficile d´obtenir des informations des fournisseurs de services. Un pays d´Amérique a, par exemple, signalé que le fait que des fournisseurs de services communiquent volontairement des informations de l´abonné a entraîné des pratiques incohérentes dans le pays.[121] D´autres pays ont déclaré que les fournisseurs de services ne stockent pas les données informatiques *assez longtemps* et que *le fournisseur communique les données à la police prend trop de temps.*[122]Un pays d´Asie a mentionné le problème des *renseignements d´enregistrement inexact* stockés par les fournisseurs de service[123]. Les interactions-formelles et informelles- entre les services répressifs et les fournisseurs de services sont examinées dans la prochaine section du chapitre.

5.5 Les enquêtes et le secteur privé

PRINCIPAUX RÉSULTATS :

- l´interaction entre les services répressifs et les fournisseurs de services internet est particulièrement complexe. Les fournisseurs de services peuvent détenir les informations de l´abonné, la facturation, certains journaux de connexion, des informations sur la localisation et le contenu des communications ;
- les obligations juridiques nationales, la rétention des données de la part du secteur privé et les politiques de divulgation varient beaucoup en fonction du pays, de l´industrie et du type de données. Certains pays déclarent qu´il est difficile d´obtenir les données des fournisseurs ;
- généralement les fournisseurs de services requièrent une procédure judiciaire appropriée pour divulguer les données de l´abonné. Par conséquent les pays déclarent utiliser généralement des ordonnances du tribunal pour que les fournisseurs de services leur transmettent les preuves électroniques ;
- cependant dans certains cas, les organismes d´application de la loi peuvent obtenir les données directement. Ceci peut être facilité par des partenariats informels entreles organismes d´application de la loi et les fournisseurs de services.

119 Voir, par exemple, http ://blogs.skype.com/en/2012/07/what_does_skypes_architecture_do.html

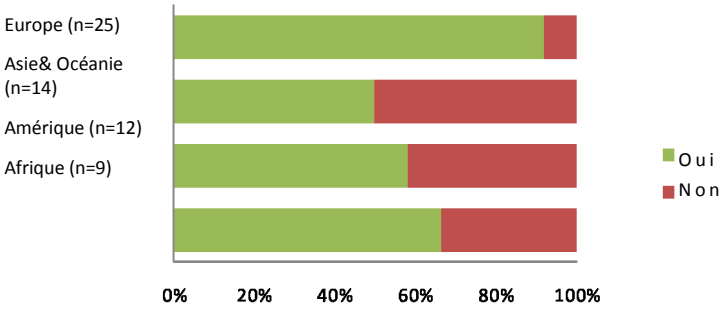
120 Questionnaire de l´étude sur la cybercriminalité. Q87-96
121 *Ibid.*
122 *Ibid.*
123 *Ibid.*

OBTENIR LES DONNÉES DES FOURNISSEURS DE SERVICES

Les réponses fournies par les pays et le secteur privé au questionnaire de l´étude présentent un panorama contrasté et complexe des interactions entre les organismes d´application de la loi et le secteur privé, caractérisé par : (i) les différences entre les pays relatives aux pouvoirs juridiques pour ordonner aux fournisseurs de services de divulguer les données informatiques ; (ii) les difficultés lorsque les fournisseurs de services sont implantés à l´étranger ; et (iii) les différences de politiques du secteur privéet des niveaux de coopération formelle et informelle avec les organismes d´application de la loi. Les fournisseurs de services électroniques détiennent les informations des abonnés, la facturation, certains journaux de connexion, des informations relatives à la localisation (comme les données relatives aux tours de téléphonie cellulaire dans le cas des fournisseurs de téléphonie cellulaire), et le contenu des communications, et toutes ces données peuvent représenter des preuves électroniques essentielles d´une infraction. Toutefois, les fournisseurs de services électroniques ne sont généralement pas tenus de signaler aux services répressifs les activités criminelles réalisées sur leurs réseaux, (bien que dans plusieurs pays, la détection de pornographie infantile implique une obligation de signalement). Par conséquent les pays répondants utilisent les pouvoirs juridiques afin que les fournisseurs de services leur communique les données informatiques requises au cours d´une enquête pénale. Comme cela a été mentionné, la majorité des pays répondants a signalé l´existence de pouvoirs généraux ou de pouvoirs spécifiques en matière de cybercriminalité, pour ordonner à de tierces parties comme les fournisseurs de services de transmettre les données.

Les pays répondants ont, par exemple, déclaré que « *conformément à la loi sur la procédure pénale, une personne qui dirige des procédures autorisées par le procureur... peut solliciter les données conservées nécessaires qui pourraient être liées au délit commis* ».[124] les pays ont aussi déclaré que *« la police peut demander aux personnes et aux entreprises de témoigner, de communiquer des données ou de faire tout ce qui pourrait être utile à l´affaire* ».[125] Néanmoins, les commentaires formulés par les pays répondants indiquent que de nombreux pays n´ont pas les pouvoirs législatifs suffisants, ou font face à des problèmes dans la *pratique*pour obtenir les données.[126] Une question fréquemment mentionnée était que les fournisseurs de services internet ne sont généralement pas tenus de conserver les données informatiques, et lorsque les ordonnances nécessaires ont été délivrées les journaux de connexion ne sont plus disponibles.[127] De nombreux pays ont également mentionné les difficultés pour résoudre les questions relatives à la vie privée, liées à la divulgation des données de la part des fournisseurs de services.[128]

Figure 5.16 : les services répressifs contraignent des personnes non tenues de le faire à fournir des informations



Source : questionnaire de l´étude sur la cybercriminalité. Q101. (n=60)

Ces difficultés ont été plus souvent mentionnées par les pays localisés hors d´Europe. Ce patron est aussi confirmé par les réponses fournies par les services répressifs à une question relative à la capacité de contraindre les personnes qui ne font pas l´objet d´une enquête à fournir des informations. La figure 5.16 montre qu´environ 60 % des pays d´Afrique, d´Asie et d´Océanie, et d´Amérique ont répondu que cela était possible. D´autre part, presque tous les pays d´Europe, mentionnent la capacité de contraindre les tierces parties à produire des informations.

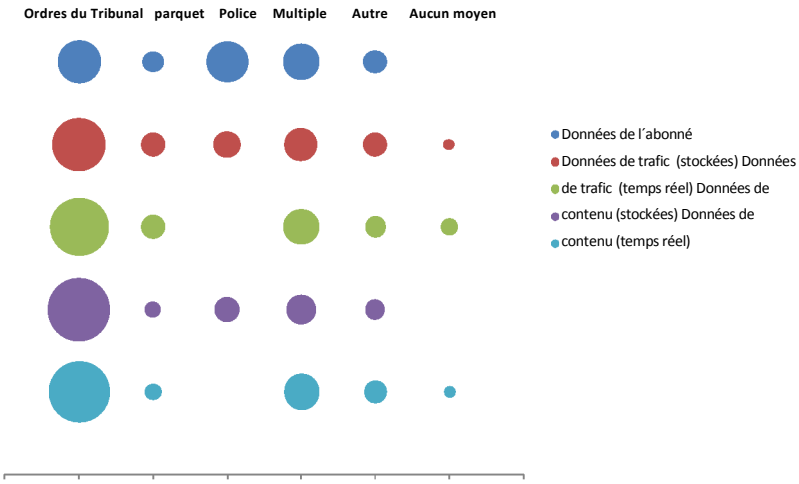
Ces informations représentent le point de vue « pratique » des services répressifs alors que les informations présentées précédemment dans ce chapitre illustrent l´existence des pouvoirs juridiques en principe.

Dans la pratique les agents des services répressifs mentionnent généralement avoir utilisé des ordonnances formelles du tribunal pour que les fournisseurs de services leur transmettent les données informatiques. La figure 5.17 montre la répartition relative des réponses concernant les méthodes utilisées pour obtenir les données de l´abonné, les données stockées du trafic et du contenu, et les données en temps réel du trafic et du contenu. Comme le laisse supposer leur caractère moins intrusif, les méthodes utilisées pour obtenir les données de l´abonné étaient plus variées– et cela incluait toutes les ordonnances émises par les tribunaux, le parquet et la police.

124 Questionnaire de l´étude sur la cybercriminalité Q101.
125 *Ibid.*
126 Questionnaire de l´étude sur la cybercriminalité. Q89-91.
127 *Ibid.*
128 *Ibid.*

De nombreux pays ont signalé que plusieurs moyens d´obtenir des données étaient disponibles, en fonction de divers facteursqui incluaient l´étape à laquelle se trouvaient l´enquête ou les procédures et l´urgence de la demande. Un pays de l´Asie de l´ouest a, par exemple, signalé que les données stockées du contenu pouvaient être obtenues par le biais d´un fournisseur de services « *en se basant sur l´ordonnance émise par un procureur public au cours de l´enquête... ou sur l´ordonnance émise par un tribunal au cours du procès* ».[129] Un autre pays a signalé que les données de l´abonné pouvaient être obtenues avec « *l´ordonnance émise par un procureur ou dans un cas urgent avec une lettre de la police et l´accord formel du procureur* ».[130] D´autres moyens d´obtenir les données furent aussi mentionnés. Un pays signala, par exemple, qu´il existait des moyens simplifiés d´obtenir les données de l´abonné en « *entrant sur la base de données publique des numéros qui est une base de données comprenant les informations des abonnés géréepar un important opérateur conformément à la législation* ».[131] En général, les réponses montraient une grande diversité quant aux moyens employés par les états, et incluaient des demandes de la police, des demandes formelles, des avis juridiques, des mandats, des ordonnances judiciaires et des injonctions de produire.

Figure 5.17 : procédures juridiques et procédures pratiques pour que les fournisseurs de services transmettent les preuves et les informations



Source : questionnaire de l´étude sur la cybercriminalité. Q102. (n=58)

Obtenir des données des fournisseurs de services : exemple national d´un pays d´Amérique

La législation fédérale d´un pays d´Amérique stipule qu´une entité gouvernementale peut exiger qu´un fournisseur de services de communications électroniques divulgue le contenu d´une communication filaire ou électronique stockée dans un système de communication électronique durant cent huit jours ou moins, seulement en vertu d´un mandat. Conformément à cette législation, les services répressifs nationaux peuvent avoir accès à certains types de données par le biais d´une injonction de produire (émise généralement par un procureur), mais requièrent un mandat du tribunal pour obtenir d´autres types de données.

Communication par courriel	**Autorisation procédure**
Stockage distant, ouvert	Injonction de produire
Stockage distant, non ouvert et stocké pour plus de 180 jours	
en transit	Mandat
Stocké sur ordinateur personnel	
Stockage distant, non ouvert et stocké pour 180 jours ou mois	

La législation nationale contient aussi des dispositions qui contraignent un fournisseur de services à divulguer des informations relatives à l´abonné dans des « *circonstances urgentes* ». Plusieurs lois nationales permettent aussi la divulgation du contenu et du non-contenu des communications à une entité gouvernementale, si le fournisseur croit de bonne foi qu´une urgence impliquant un danger de mort ou des atteintes graves à l´intégrité physique d´une personne exige la divulgation sans délai des communications liées à cette urgence. Les agents des services répressifs peuvent aussi envoyer une lettre au fournisseur de services lui ordonnant de conserver les registres et toute autre preuve en sa possession dans l´attente de l´émission de l´ordonnance du tribunal ou de toute autre procédure pour une période allant jusqu´à 90 jours. Le non-respect de cet ordre entraîne généralement des recours civils et des amendes imposées à l´entreprise

129 Questionnaire de l´étude sur la cybercriminalité. Q102.
130 *Ibid.*
131 *Ibid.*

Points de vue du secteur privé

Les informations recueillies pour l´étude incluent aussi les informations provenant des organisations du secteur privé concernant les points de vue et les expériences de coopération avec les autorités chargées de l´application de la loi. Les organisations du secteur privé qui ont répondu au questionnaire de l´étude ont mentionné diverse politiques internes et obligations externes concernant les demandes de données des services répressifs nationaux et étrangers. De plus, plusieurs politiques du secteur privé sont accessibles au public sous la forme de « manuels d´application de la loi » qui fournissent une orientation sur la conservation des données et les cadres pour les demandes des services répressifs.[132]

Dans les réponses fournies au questionnaire de l´étude, plusieurs autorités chargées de l´application de la loi soulignèrent les difficultés relatives à la courte période de conservation des données des organisations du secteur privé et des fournisseurs de services.[133] En vue de fournir des informations sur la pratique de conservation des données, le tableau ci-après présente des informations concernant un échantillon des politiques d´accès des services répressifs et la conservation des données du secteur privé et stockées durant la fourniture des services de communications électroniques et informatiques. Il montre également des politiques divergentes de conservation de données pour ces différents types de données – et donne une indication des difficultés auxquelles font face les services répressifs et les organisations du secteur privé pour identifier et sécuriser les informations appropriées pouvant être utilisées comme preuves. Aucun des fournisseurs de services examinés ne conservait les mêmes données durant la même période de temps. Les périodes de conservation accessibles au public allaient d´un jour à une durée indéfinie. Certaines informations semblaient être conservées seulement durant la période pendant laquelle le compte de l´abonné restait actif. De nombreuses organisations du secteur privé déclarèrent que répondre aux demandes des services répressifs pouvaient exiger du temps et qu´il n´était pas toujours facile de le faire en raison des politiques et des protocoles de stockage et de conservation des registres. Ne pas disposer de personnel en nombre suffisant pour répondre aux demandes pouvait aussi entraver l´observation de ces demandes ou les délais requis. Pour les plus petites organisations, donner suite aux demandes des services répressifs était plus astreignant en termes de dépenses de ressources et de personnes.[134]

Conservation et stockage des données des organisations du secteur privé

Entreprise	Types de données produites	Durée de rétention des données	Demande formelle requise pour la divulgation
Fournisseur de services de communication et d´information #1	Dialogue de salle de discussion Conversations de messagerie instantanée	Aucune	Oui
	Journaux du répertoire des membres Journaux des accès à la connexion/ IP du courriel Journaux du groupe IP Journaux des accès aux connexions internet	60 jours	
	Journaux des connexions TV et téléphone		
Fournisseur de services de communication et d´information	Registres de l´historique des connexions IP	60 jours	Oui
	Données transactionnelles	90 jours (Privé)/60 jours (Groupes)	

132 Voir, par exemple, https ://www.facebook.com/safety/groups/law/guidelines/ ; http ://pages.ebay.com/securitycenter/LawEnforcementCenter.html ; http ://support.twitter.com/articles/41949-guidelines-forlaw-enforcement# ; ethttp ://myspace.desk.com/customer/portal/articles/526170-law-enforcement-support

133 Voir le chapitre (prévention), Section 8.3 prévention de la cybercriminalité, le secteur privé et le milieu universitaire, la prévention de la cybercriminalité par les fournisseurs d´hébergement et de services internet.

134 Entretiens de l´étude de la cybercriminalité (secteur privé).

#2	Enregistrement de comptes e-mail	Aussi longtemps que ces comptes existent		
	Compte de jeu			
	Registres de l´identification de l´appelant			
Services de communication et d´information #3	Informations du compte web de messagerie	Diverses périodes de conservation		
	Fichier journal d´adresse IP	180 jours	Oui	
	Registres des comptes	2 ans minimum		
	Registres détaillés des appels			
Fournisseur de services de communication	Messagerie instantanée	30-90 jours		
	Contenu de message vidéo			
	Boîte vocale			
	Transactions financières	Aussi longtemps que nécessaire	Oui	
	Données d´enregistrement			
	Informations du service et du compte			
Développeur de jeux et fournisseur de réseau	Communications de l´usager	Diverses périodes de conservation (jusqu´à 180 jours)		Oui
	Informations du compte	Indéfiniment		
	Journaux IP			
Fournisseur de services d´information #1	Domaines	Diverses périodes de conservation (1jour à une durée indéfinie)		
	E-mails			
	Journaux de connexion de l´IP des proxy	5-7 jours		
	Journaux de connexion de l´IP des membres	90 jours		Oui
	Journaux de connexion de l´IP de la source			
	Session logs	6 mois		
Fournisseur de services d´information #2	Contenu et journaux de l´activité de l´hébergement web/domaines	Minimum 30 jours après la dissolution du groupe/site web/domaine		
	Contenu et journaux du groupe			
	Journaux de la salle de discussion/messagerie instantanée	45-60 jours		Oui
	E-mails	4 mois ou plus d´inactivité		
	Informations de l´abonné	18 mois d´inactivité		
	Contenu du compte	90 jours après la suppression du compte		
	Profils			
	Adresses IP de la connexion	Jusqu´à un an		
Fournisseur de service de messagerie	Informations de l´abonné	Diverses périodes de conservation		
	Contenu du compte	Jusqu´à 37 jours après la suppression du compte	Oui	
	Liens, témoins de connexion			
	Informations de la localisation			
	Données du journal			
	Données du gadget			
Fournisseur de réseau social#1	Données d´enregistrement (Informations de base de l´abonné)	Jusqu´à 90 jours après la suppression du compte		Oui
	Données transactionnelles (journaux			

Fournisseur de réseau social #2	Communications privées de l´usager	Diverses périodes de conservation	Oui
	Information de base de l´identité de l´usager, registres généraux	Aussi longtemps que ces comptes existent /10 jours après la suppression du compte	
	Journaux des adresses IP	90 jours	

La préoccupation primordiale des entreprises relatives aux demandes des services répressifs est d´avoir la capacité de fournir les données requises mais « *sans enfreindre d´autres exigences législatives ou règlementaires* ».[135] Les organisations du secteur privé ont fréquemment mentionné les conditions d´utilisation des services des clients et le respect de la vie privée. Les organisations du secteur privé ont cependant déclaré qu´elles devaient répondre rapidement et positivement si « *la vie est en danger*, mais ont également précisé que cela « *était très, très rare* ».[136] Les organisations du secteur privé qui ont répondu au questionnaire, ainsi que les fournisseurs de services, établissaient une claire distinction entre les obligations légales de fournir les données et les demandes informelles. Presque toutes les entreprises répondantes ont déclaré qu´elles « *devaient répondre »* et qu´elles « *répondaient* » aux ordonnances formelles des tribunaux nationaux de produire les informations « *en conformité avec les lois applicables* »[137] et « *en conformité avec leurs responsabilités légales* ».[138] Apres la réception d´une demande une organisation du secteur privé a, par exemple, mentionné que la première étape consistait à déterminer « *s´il y a un droit statutaire sous-jacent de demander les informations ou s´il y a une obligation légale de divulguer les informations, et à veiller à ne violer aucune autre loi ni aucune obligation contractuelle de l´entreprise envers les clients ou le droit à la vie privée des clients* ».[139]

La majorité des organisations du secteur privé ont déclaré qu´elles ne considéraient pas avoir l´obligation de fournir des informations en réponse à une requête informelle–comme un appel téléphonique–des services répressifs, toutefois de nombreuses organisations ont précisé qu´elles pouvaient choisirde fournir volontairement des renseignements conformément à leurs propres politiques internes. Une entreprise internationale a, par exemple, signalé qu´elle répondait à ces demandes « *si les données étaient disponibles et si le fait de les fournir était en conformité avec les règlementations juridiques et les èglementations des ressources humaines de l´entreprise* ».[140] La majorité des organisations ont déclaré qu´elles fourniraient des données en réponse à une requête « formelle » des services répressifs – telle qu´une lettre officielle. Néanmoins, presque toutes ont indiqué que cela n´était pas une obligation absolue et que les données pouvaient fournies seulement dans certaines conditions, comme dans le cas où « *il existe une obligation statutaire de fournir les informationset leur divulgation ne viole aucune autre loi ni aucune obligation contractuelle de l´entreprise* ».[141]

Les entreprises internationales et les fournisseurs de services nationaux mentionnent fréquemment que la nomination des points de contact des services répressifs facilite la coopération avec les autorités chargées de l´application de la loi. Ceci inclut l´équipe d´intervention en cas d´incident contre la sécurité informatique (CSIRT), la sécurité informatique, juridique, la gestion des risques ou des services de sécurité. D´autres entreprises ont des équipes multidisciplinaires ou des groupes de travail qui gèrent les relations avec les services répressifs. Certaines organisations du secteur privé ont signalé que les mécanismes visant à renforcer la coopération et les échanges d´informations avec les services répressifs sont encore en cours de développement.[142] Ces mécanismes sont importants en vue du nombre croissant des demandes de données présentées par les services répressifs aux fournisseurs de services. Un opérateur multinational de télécommunications a, par exemple, signalé que le nombre de demandes formelles de données informatiques reçues entre 2008 et 2010 avait été multiplié par 50.[143]

135 Questionnaire de l´étude sur la cybercriminalité (secteur privé) Q24.
136 Questionnaire de l´étude sur la cybercriminalité (secteur privé)Q26.
137 Questionnaire de l´étude sur la cybercriminalité (secteur privé)Q24-27.
138 Questionnaire de l´étude sur la cybercriminalité (secteur privé)Q24.
139 Questionnaire de l´étude sur la cybercriminalité (secteur privé)Q24-27.
140 *Ibid.*
141 *Ibid.*
142 Questionnaire de l´étude sur la cybercriminalité (secteur privé)Q30.
143 Questionnair de l´étude sur la cybercriminalité (secteur privé)Q35.
144 Questionnaire de l´étude sur la cybercriminalité (secteur privé)Q28.

Les organisations du secteur privé ont aussi souligné le fait qu´elles reçoivent souvent des demandes des services répressifs *nationaux* et *étrangers*. Plusieurs entreprises ont déclaré qu´elles tenaient compte des demandes des services répressifs *étrangers* seulement si elles étaient présentées par le biais des voies *formelles nationales*.[144] Certaines entreprises ont déclaré que les services répressifs étrangers doivent obtenir une ordonnance de production des données émise par un tribunal national, par le biais d´une demande d´entraide judiciaire. Les entreprises dont les bureaux se trouvent dans plusieurs pays ont mentionné que les différentes opérations nationales devaient toujours tenir compte les réglementations et les lois locales. Néanmoins, les organisations multinationales du secteur privé déterminent généralement un siégé principal de juridiction pour la réception des demandes globales des services répressifs.[145]

Outre une exigence générale relative à une procédure juridique en bonne et due forme adressé au siège de la juridiction de l´entreprise, de nombreuses organisations du secteur privé signalent que les demandes informelles des services répressifs étrangers peuvent aussi être satisfaites a titre discrétionnaire.[146] Les informations accessibles au public relatives à des fournisseurs de services à l´échelle internationale comme Google, par exemple, déclarent que : « *en utilisant les traités d´entraide judiciaire et d´autres arrangements diplomatiques et de coopération, les organismes [étrangers] peuvent [par le biais des autorités nationales] collecter des preuves à des fins d´enquête légitime,* et que : « *les données de l´abonné peuvent être fournies volontairement en réponse à une procédure juridique valide des organismes* [*étrangers*]*, si ces requêtes sont en conformité avec les normes internationales, les lois [du* « *siège* » *national], les politiques de Google et le droit du pays requérant* ».[147]

Ceci ajoute à l´exigence par défaut qui oblige les services répressifs étrangers à obtenir des injonctions de produire, des mandats ou des ordonnances au siège de la juridiction du fournisseur de services, la possibilité de fournir à leur discrétion des données aux services répressifs dans les limites des lois nationales et des conditions d´utilisation des clients. Ces relations discrétionnaires entre le secteur privé et les services répressifs sont bâties sur la confiance et ne sont pas légalement contraignantes– elles existent généralement dans des zones socio-politiques ou géographiques limitées. Une entreprise d´Amérique centrale a, par exemple, déclaré qu´elle acceptait des obligations dérivées des demandes informelles des services répressifs, mais que cela était limité exclusivement aux demandes émises par les autorité locales.[148] Un pays européen a spécifié qu´il traitait les demandes informelles des services répressifs étrangers de la même manière que les demandes des autorités nationales, mais qu´il ne se considérait pas comme légalement tenu de les satisfaire dans l´un et l´autre cas.[149] Comme l´a publiquement déclaré un des principaux fournisseurs de services en ligne : « *nous agissons de bonne foi avec... autorités, mais nous n´avons pas l´obligation de le faire... si l´on abuse de notre bonne foi, nous devrons reconsidérer soigneusement cette coopération* ».[150] En d´autres termes, dans les limites imposées par les lois sur la protection des données et les termes et conditions d´utilisation des clients, les fournisseurs de services ont une grande marge de manœuvre en matière de divulgation de données, y compris envers les services répressifs étrangers. Ces décisions sont souvent basées sur des relations de travail existantes et sur la confiance. Un fournisseur d´équipement de réseaux à l´échelle mondiale a, par exemple, déclaré que toutes les demandes « *font l´objet d´un examen afin de vérifier leur faisabilité technique et leur conformité avec les régulations spécifiques du pays [...] juridiques et [...] en matière de droits de l´homme* ».[151]

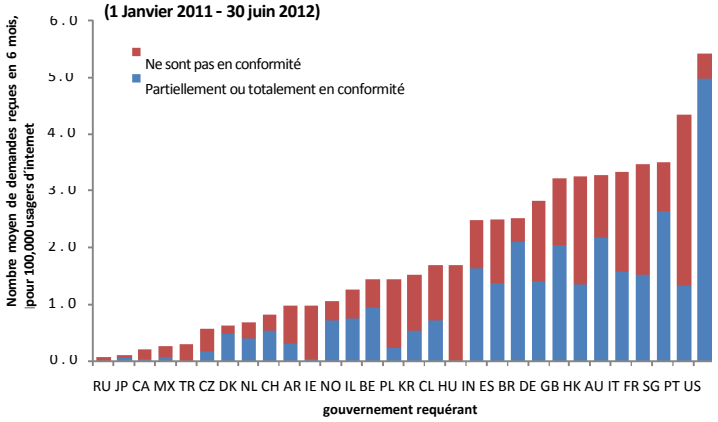
Le mélange de : (i) de la capacité variable des services répressifs étrangers de garantir une procédure juridique en bonne et due forme au siège de la juridiction par le biais d´une demande d´entraide judiciaire ; et (ii) l´existence de réseaux informels basés sur la confiance, entraîne des variations dans le degré de conformité des fournisseurs de services internationaux avec les demandes d´informations des services répressifs étranger. La figure 5.18 montre le nombre de demandes reçues et satisfaites de divers pays (échelonnée par 100,000 usagers d´internet dans les pays requérants) tel qu´indiqué par le rapport de transparence de Google.[152]La proportion la plus élevée de demandes satisfaites est dans le siège de la juridiction. Les demandes d´autres pays

varient entre zéro % de demandes satisfaites à presque 80 %, avec une moyenne d´environ 50 % de demandes satisfaite. Ce patron est probablement causé par de nombreux facteurs qui incluent : le fait que les demandes des services répressifs étrangers soient présentées directement ou de manière informelle plutôt que par le biais de l´entraide judiciaire ; les politiques des entreprises envers les demandes informelles de différents pays ; et la capacité des autorités étrangères relative à la préparation des demandes d´entraide judiciaire.

145 Entretiens de l´étude sur la cybercriminalité (secteur privé). Q28.
146 *Ibid.*
147 Voir, par exemple, http ://www.google.com/transparencyreport/userdatarequests/legalprocess/
148 Questionnaire de l´étude sur la cybercriminalité (secteur privé). Q28.
149 *Ibid.*
150 Chambre des lords et Chambres des communes. *Projet de loi sur les communications de données du comité mixte–premier rapport*. Section 6 (questions juridictionnelles – demandes adressées à l´étranger CSP), 28 novembre 2012.
151 Questionnaire de l´étude sur la cybercriminalité (secteur privé). Q28.
152 voirhttp ://www.google.com/transparencyreport/userdatarequests/

Les relations informelles entre les services répressifs et les organisations du secteur privé peuvent aller au-delà de la fourniture de données informatiques pour les enquêtes. Lors de la collecte des informations pour l´étude, les pays et les organisations du secteur privé ont mentionné une vaste gamme de domaines de coopération. Un pays du nord de l´Europe a, par exemple, signalé que « *les services répressifs ont une relation de travail informelle avec les principaux fournisseurs de services afin de mettre à jour les informations de contact et de développer des procédures pour l´échange formel de données* ».[153] D´autres pays signalent que « *il y a des codes de pratiques qui permettent de volontairement échanger des informations, parallèlement à la législation formelle* ».[154]

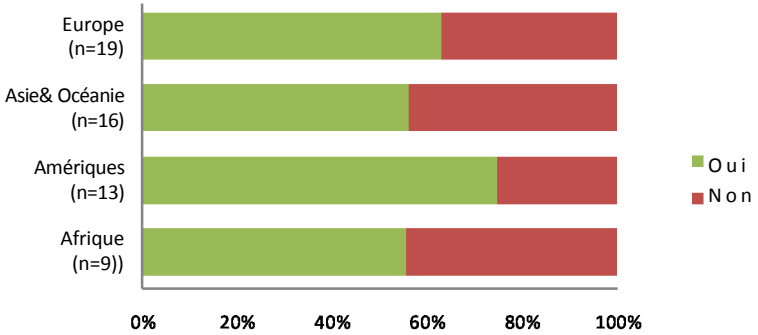
Figure 5.18 : demandes de données d´utilisateurs envoyées par les gouvernements à Google (1 Janvier 2011 - 30 juin 2012)



Source : ONUDC présentation du rapport de transparence de Google.

Plusieurs pays ont notamment mentionné les relations avec les entreprises de télécommunications. Un pays a, par exemple, souligné que : « *les services répressifs maintiennent d´étroites relations avec l´industrie des télécommunications– en particulier avec les participants de l´industrie les plus importants. Ces relations sont essentiellement utilisées pour déterminer des mesures pratiques (comme les meilleures procédures pour notifier un mandat, déployer des capacités et transmettre les informations licitement intercepter), des questions techniques (comme le fonctionnement des réseaux de télécommunications), et des questions relatives aux politiques* ».[155] les informations fournies par les organisations du secteur privé indiquent aussi plusieurs entreprises – et non seulement les fournisseurs de services électroniques– forment des partenariats avec les organismes d´application de la loi. Ceux-ci visent à partager des informations générales sur les tendances et les menaces de la cybercriminalité, et à faciliter le signalement de suspicion de cyberdélits.[156] Les partenariats publics-privés concernant la cybercriminalité sont examinésplus en détail au chapitre huit (prévention).

Figure 5.19 : relations informelles entre les services répressifs et les fournisseurs de services



Source : questionnaire de l´étude sur la cybercriminalitéQ103.

Les réponses fournies par les pays au questionnaire de l´étude suggèrent que les relations informelles entre les services répressifs et les fournisseurs de services sont tout aussi fréquentes dans diverses régions. La figure 5.19 montre qu´entre 50 pour .cent et 60 % des pays de toutes les régions signalent l´existence de ces relations.[157]

153 Questionnaire de l´étude sur la cybercriminalité Q103.
154 *Ibid.*
155 *Ibid.*
156 Questionnaire de l´étude sur la cybercriminalité (secteur privé). Q40-45.
157 Questionnaire de l´étude sur la cybercriminalité Q103.
158 Questionnaire de l´étude sur la cybercriminalité Q103.

De nombreux pays ont pris soin de souligner que les relations informelles entre les services répressifs et les fournisseurs de services concernaient des échanges d´informations qui « *n´impliquaient pas les données privées des usagers* ».[158] Toutefois, d´autres semblaient indiquer que les données privées des usagers pourraient être fournies aux organismes d´application de la loi par le biais de ces arrangements.[159] Bien que les relations durables et efficaces entre les services répressifs et les fournisseurs de services puissent grandement aider les enquêtes sur les cyberdélits, il est essentiel que ces arrangements soient en conformité avec l´état de droits et les normes internationales des droits de l´homme. Comme cela est mentionné dans le chapitre, ceci inclut le fait de clairement définir les conditions et les circonstances dans lesquelles les organismes d´application de la loi sont habilités à obtenir des données informatiques, et de définir des garanties adéquates et efficaces contre les abus.[160] Des arrangements similaires ou les fournisseurs de services donne libre accès aux services répressifs, par exemple, aux données stockées du contenu, du trafic ou de l´abonné peuvent être passées au cribles par les organismes des droits de l´homme.[161]

5.6 Capacités des services répressifs

PRINCIPAUX RÉSULTATS :

- plus de 90 % des pays répondants ont commencé à mettre en place des structures spécialisées pour enquêter sur la cybercriminalité et sur des délits mettant en cause des preuves électroniques ;
- cependant, les pays en développement manquent de ressources et de capacités ;
- Les pays avec de bas niveaux de développement disposent de nettement moins de services de police spécialisée, environ 0,2 pour 100 000 utilisateurs nationaux d´internet. Ce taux est de deux à cinq fois plus élevé dans les pays plus développés ;
- dans les pays moins développés 70 % des officiers spécialisés des services de détection et de répression ont signalé un manque de matériel et d´habilités informatiques.

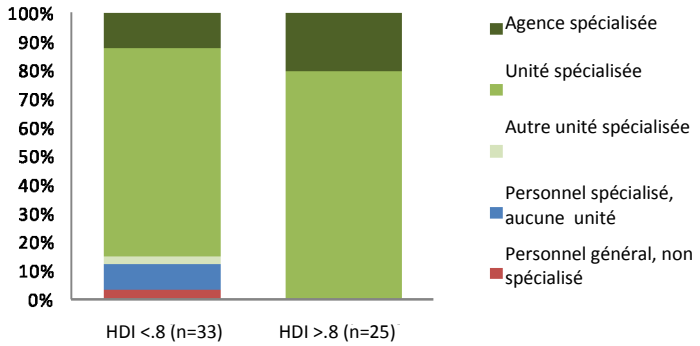
Cette section présente les informations collectées concernant la *capacité* des autorités chargées de l´application de la loi pour prévenir et lutter contre la cybercriminalité. La capacité institutionnelle dans le contexte de la police comporte de nombreux éléments, tels que les capacités stratégiques et opérationnelles, les habilités techniques du personnel, et le fait de disposer de suffisamment d´agents et de ressources. [162] Un autre élément important est le niveau de spécialisation. Les délits qui requièrent une riposte spécialisée sont typiquement ceux qui présentent des difficultés spécifiques relatives aux définitions des infractions, à l´applicabilité des lois, ou à la collecte et à l´analyse des preuves.[163] La cybercriminalité présente toutes ces caractéristiques, et la spécialisation des services répressifs est fondamentale pour une riposte efficace en matière de prévention des délits et de justice pénale. La spécialisation des services répressifs peut être au niveau personnel et au niveau organisationnel – qui souvent coïncident. La spécialisation sera donc probablement toujours requise dans le domaine de la cybercriminalité et des preuves électroniques mais c´est aussi le cas – étant donné que le monde avance vers une hyper connectivité– pour tous les agents des services répressifs qui seront de plus en plus souvent appelés à collecter et à traiter des preuves électroniques de manière routinière.

159 *Ibid.*
160 Voir la Section 5.3vie privée et mesures d´enquête, existence de protections de la vie privée et de garanties procédurales.
161 Voir, par exemple, http ://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention
162 Katz, C.M., Maguire, E.R., Roncek, D.W., 2002. La création d´unités spécialisées de police. *Maintien de l´ordre,* 25(3) :472-506.
163 Mace, R.R., 1999. *Les organisations de poursuites et le contrôle du réseau de cybercriminalité.* (Doctoral dissertation). AAT 9920188.

Spécialisation organisationnelle

La majorité des pays qui ont répondu au questionnaire de l´étude ont mentionné l´existence de structures spécialisées des services répressifs contre la cybercriminalité. Plus de 75 % des pays ont mentionné une unité spécialisée dans les organisations existantes d´application de la loi. Environ 15 % ont mentionné une agence spécialisée en matière de cybercriminalité.[164] Il faut noter qu´aussi bien les pays les plus développés (HDI>0.8) que les pays moins développés (HDI<0.8) ont mentionné des niveaux significatifs de spécialisation. Cependant, les pays les moins développés montrent un large éventail de structures, car certains pays ne disposent pas de personnel spécialisée et d´autres mentionnent l´existence de personnel spécialisé qui n´est pas intégré au sein d´une structure spécialisée. Avec une seule exception (en Afrique), les pays qui ont signalé le manque d´agences ou d´unités spécialisées countries ont fait part de leur intention d´en établir une dans un avenir proche.[165]

Figure 5.20 : structures des services répressifs pour prévenir et lutter contre la cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalitéQ113. (n=58)

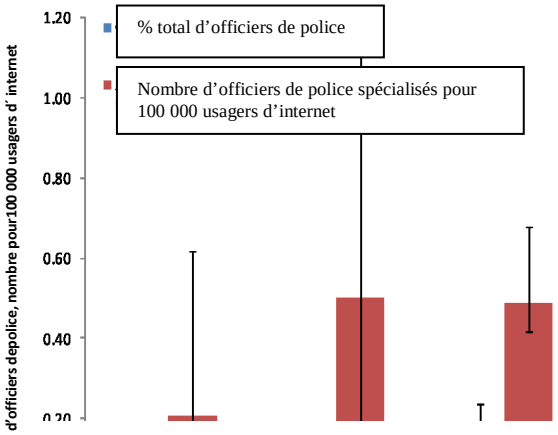
Les pays répondants présentent aussi des variations du niveau d´intégration des unités spécialisées dans les agences et les services des organismes d´application de la loi fédéraux, régionaux, municipaux et étatiques. Dans certains pays, « *tous les organismes fédéraux chargés des enquêtes ont des unités spécialisées en matière de cybercriminalité* ».[166] D´autres mentionnent des unités au niveau fédéral « *avec des accords variables d´application de la loi entre les différentes jurisdictions* ».[167] Il y a eu aussi des variations considérables dans les pays relatives à la couverture géographique et à l´uniformité des unités au sein des organismes d´application de la loi.[168] Plusieurs pays ont mentionné l´établissement d´une unité nationale spécialisée et des projets d´ajouter progressivement des unités et du personnel dans des bureaux locaux. Les pays développés ont fréquemment mentionné « *un vaste éventail de ressources* » ou « *des ressources suffisantes* », bien que certains aient indiqué que *'les ressources sont adéquates pour mener des enquêtes en vue d´élever les capacités à un niveau supérieur* » et que « *toutes les ressources sont suffisantes pour nous permettre d´effectuer le travail. Mais pour obtenir de meilleurs résultats, plus efficaces et rapides nous aurions besoin de nouvelles ressources actualisées en matière de matériel informatique et de logiciels* ».[169] D´autres pays plus développés ont mentionné des besoins spécifiques de développement du personnel qui incluaient le fait de ne pas disposer « *de suffisamment de ressources humaines* et mentionnaient des différences entre les ressources de la police fédérale et de la police d´état « *certains groupes de police d´état disposent de capacités adéquates, d´autres non* ».[170] Des pays en développement d´Afrique et d´Asie ont signalé des besoins en matière « d´*outils criminalistiques* » et ont souligné que « *les ordinateurs criminalistiques et les applications informatiques criminalistiques sont désuets* ».[171]

164 Questionnaire de l´étude sur la cybercriminalité Q113.
165 *Ibid.*
166 Questionnaire de l´étude sur la cybercriminalité Q113.
167 *Ibid.*
168 *Ibid.*
169 Questionnaire de l´étude sur la cybercriminalité Q109.
170 *Ibid.*
171 *Ibid.*

Spécialisation du personnel

Plusieurs pays ont mentionné l´existence d´officiers de police spécialisés en cybercriminalité.[172] Les pays avec de bas niveaux de développement disposent de nettement moins de services de police spécialisée, environ 0.2 pour 100,000 utilisateurs nationaux d´internet. Ce taux est de deux à cinq fois plus élevé dans les pays plus développés. Dans tous les pays la proportion d´officiers de police spécialisés en cybercriminalité est inférieure à un % de l´effectif total de la police.[173] En général environ 40 % des pays répondants ont déclaré que les officiers spécialisés en cybercriminalité possédaient des compétences avancées en TI. Un peu plus de 30 % des pays ont déclaré que les officiers spécialisés possédaient des compétences intermédiaires en TI, 20 % des pays indiquèrent que les officiers spécialisés possédaient des compétences basiques en TI et 6 % des pays dirent que les officiers spécialisés ne possédaient aucune compétence de TI. Ce panorama global masque cependant des différences significatives liées au niveau de développement du pays. Dans les pays les plus développés environ 70 % des officiers spécialisés possèdent des compétences avancées en TI et ont accès à des équipements informatiques sophistiqués et cette proportion s´élevait à environ 20 % dans les pays moins développés. Par ailleurs environ 45 % des pays moins développés déclarèrent que les officiers spécialisés en cybercriminalité possédaient seulement des compétences basiques en TI et avaient accès à des équipements informatiques moyennement sophistiqués.

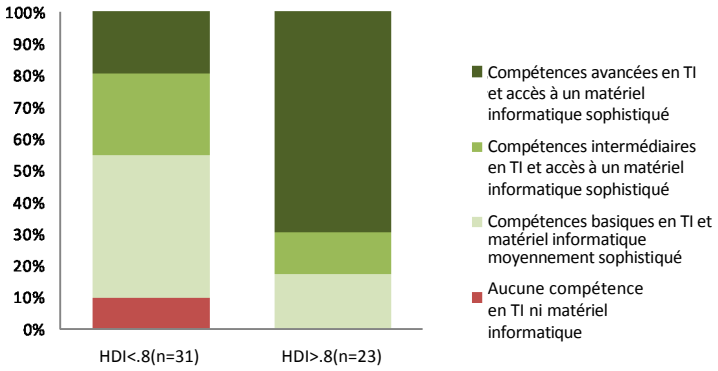
Figure 5.21 : nombre d´officiers de police spécialisés, selon le niveau de développement du pays



Source : questionnaire de l´étude sur la cybercriminalité Q115 et Q61. (n=44)

Cependant, la situation peut aussi varier significativement au sein d´un même pays. Un pays a, par exemple, déclaré *« il est impossible de faire une déclaration générale car toute la gamme est représentée »*.[174] *Certaines unités disposent « d´équipement et de logiciels appropriés mais le niveau de compétences (des employés) est insuffisant pour traiter certaines questions »*. D´autres unités « *ont des officiers hautement spécialisées mais manquent de matériel sophistiqué* » [175]

Figure 5.22 : capacités techniques des services répressifs



Source : questionnaire de l´étude sur la cybercriminalité Q116. (n=54)

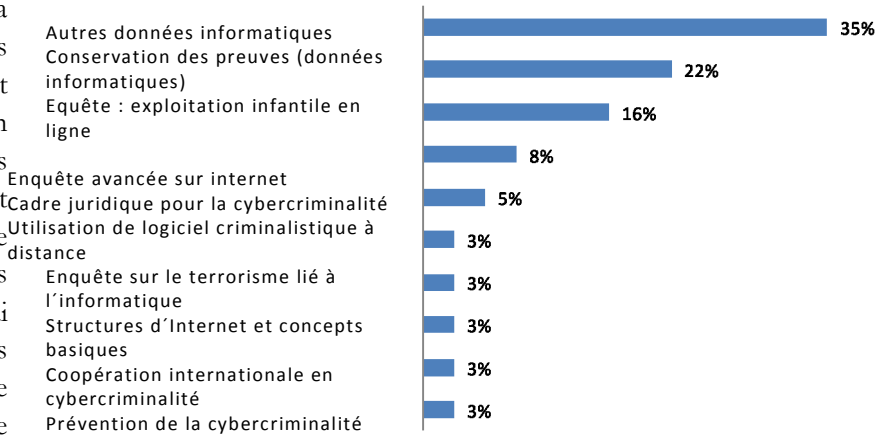
172 Questionnaire de l´étude sur la cybercriminalité Q115.
173 Calculs basés sur le questionnaire de l´étude sur la cybercriminalité. Q115 ; et l´enquête des Nations Unies sur les tendances de la criminalité et le fonctionnement des systèmes de justice pénale, dernier année disponible.
174 Questionnaire de l´étude sur la cybercriminalité. Q116.
175 *Ibid.*

Développement du personnel

La plupart des pays a déclaré qu´ils fournissaient une cyber-formation au personnel spécialisé et non spécialisé des services répressifs. Les officiers spécialisés des services répressifs recevaient une formation qui couvrait une gamme de thèmes, allant des enquêtes basiques et de l´orientation en technologie, jusqu´aux preuves et aux questions criminalistique.

les thèmes multiples de formation (35 %), la conservation des preuves électroniques (environ 20 %) et l´exploitation des mineurs en ligne (environ 15 %) furent les thèmes les plus souvent mentionnés en matière de formation pour les officiers spécialisés. D´autres thèmes qui incluaient les enquêtes avancées sur internet, ´la criminalistique numérique, l´utilisation de logiciels criminalistiques spéciaux et l´analyse des logiciels malveillants.

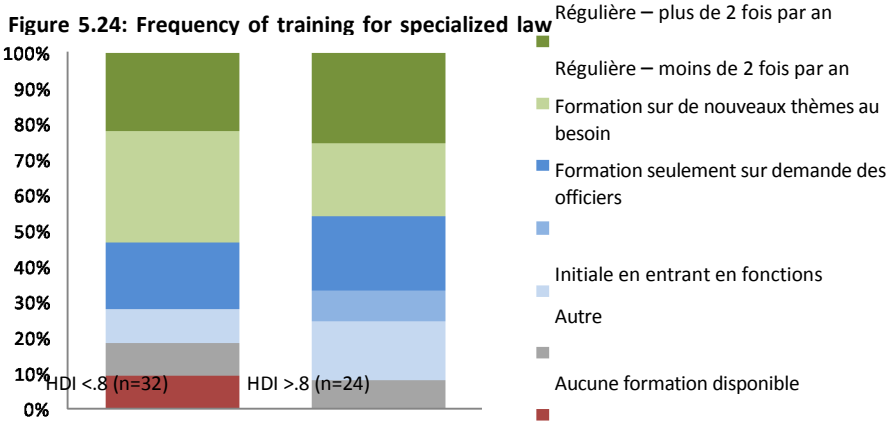
Figure 5.23 : thèmes de formation pour les officiers spécialisés des services répressifs



Source : questionnaire de l´étude sur la cybercriminalité Q117. (n=37)

L´étendue et la portée des programmes de formation fournis aux officiers spécialisés varient beaucoup. Dans certains pays tous les officiers spécialisés reçoivent des formations en cybercriminalité, en personne ou en ligne. Dans d´autres pays la formation était impartie au niveau national aux officiers par unités sélectionnées sur la terminologie basique en matière de cybercriminalité ou sur la méthodologie basique d´enquête. Certains déclarèrent qu´ils fournissaient des formations additionnelles sur des thèmes comme les connaissances basiques en TI, la connaissance des délits commis au moyen de la technologie, la conservation des preuves et les logiciels criminalistiques à distance. Les pays ont signalé que cette formation était intégrée à la formation des officiers spécialisés ou disponibles sur la demande ou en fonction des besoins des officiers. La formation régulière est un élément important de la capacité des services répressifs en permettant aux officiers spécialisés de se tenir informé des techniques et des progrès les plus récents

Figure 5.24 : fréquence de la formation pour les officiers spécialisés

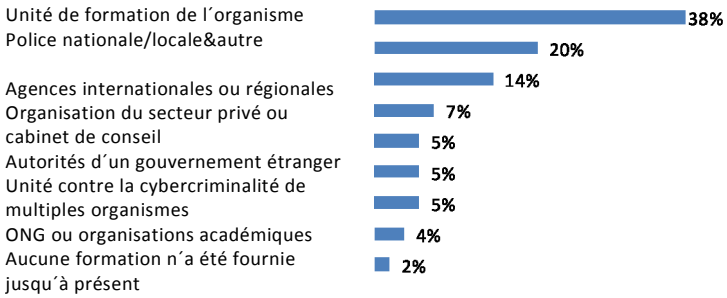


Source : questionnaire de l´étude sur la cybercriminalitéQ118. (n=56)

techniques et des progrès les plus récents. Entre 50 et 60 % des pays les plus développés tout autant que des pays les moins développés ont déclaré fournir une formation régulière (plus d´une fois par an). Certains pays moins développés ont toutefois déclaré qu´impartir une formation était « *rare* » ou qu´aucune formation n´était disponible.[176]

La formation pour les officier spécialisés est le plus souvent directement impartie par une unité de formation de l´organisme chargé de l´application de la loi. Environ 15 % des pays déclarèrent que des organisations régionales ou internationales fournissaient une formation en matière de cybercriminalité aux officiers spécialisés des services répressifs – et indiquèrent que ces organisations jouaient un rôle important en fournissant une assistance technique. Le chapitre six (preuves électroniques et justice pénale) examine les besoins et la fourniture d´assistance technique de manière plus détaillée.

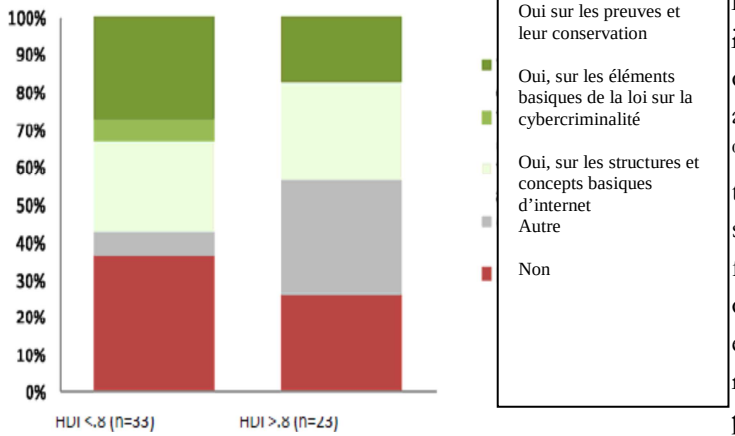
Figure 5.25 : fournisseurs de formation pour les officiers spécialisés des services répressifs



Source : questionnaire de l´étude sur la cybercriminalité Q119 (n=56)

Étant donné que les preuves électroniques sont sont devenues un élément important des enquêtes sur tous types de délits, les officiers non spécialisés des services répressifs devront de plus en plus mener des enquêtes liées à l´informatique. Les réponses du questionnaire de l´étude montrent de nettes différences entre les pays en matière de fourniture de formation sur la cybercriminalité pour les agents non spécialisés des services répressifs. Environ 25 % des pays, parmi les pays les plus développés et les pays en développement, déclarèrent impartir une formation basique sur les concepts et les structures d´internet aux agents non spécialisés. Environ 40 % des pays moins développés ont toutefois déclaré que les officiers non spécialisés ne reçoivent aucune formation en matière de cybercriminalité ou de preuves électroniques. De nombreux pays ont néanmoins mentionné des initiatives pour améliorer la formation sur la cybercriminalité pour les officiers non spécialisés. Un pays a, par exemple déclaré, « entreprendre un programme général pour donner à tous les officiers une compréhension *basique de la cybercriminalité ainsi que la législation et des techniques pertinentes* ».[177]Un autre pays a indiqué que « *les officiers réguliers reçoivent une formation en matière de conservation de preuves électroniques dans le contexte de cours sur les enquêtes générales* ».[178] D´autres pays ont signalé que les thèmes de cybercriminalité sont en cours « *d´intégration dans la formation régulière de la police* »[179] et que la formation pour les officiers est « *disponible avec des cours en ligne sur notre plate-forme de formation technologique* »[180]

Figure 5.26 : formation pour le personnel non spécialisé des services



Source : questionnaire de l'étude sur la cybercriminalité. Q120

176 Questionnaire de l´étude sur la cybercriminalitéQ118.
177 Questionnaire de l´étude sur la cybercriminalité Q120.
178 *Ibid.*
179 *Ibid.*
180 *Ibid.*

CHAPITRE SIX : PREUVES ÉLECTRONIQUESET JUSTICE PÉNALE

Ce chapitre examine le processus de justice pénale dans les cas de cybercriminalité, qui débute avec la nécessité d´identifier, de collecter et d´analyser les preuves électroniques par l´entremise de la criminalistique numérique. Il examine la recevabilité et l´utilisation des preuves électroniques lors d´un procès et montre comment de multiples difficultés en matière de poursuites peuvent avoir une incidence sur la performance du système de justice pénale. Il fait le lien entre les besoins de capacités des services répressifs et de la justice pénale, et des activités d´assistance technique requise et octroyée.

6.1 Introduction aux preuves électroniques et à la criminalistique numérique

Principaux résultats :

- les preuves sont les faits pertinents au moyen desquels la culpabilité ou l´innocence d´une personne est établie lors d´un procès. Les preuves électroniques comprennent toutes les preuves existant en forme digitale ou électronique ;
- la criminalistique numérique se rapporte à la récupération des informations – qui sont souvent volatiles et facilement contaminées – pouvant avoir une valeur probante ;
- les techniques de criminalistique incluent la création de copies « bit à bit » des informations stockées et effacées, le « blocage d´écriture », afin de garantir que les informations originales ne sont pas altérées, et des « hachages » cryptographiques de fichiers, ou des signatures digitales, qui peuvent révéler des changements dans les informations.

Les preuves électroniques dans les procédures pénales

Les preuves sont les faits pertinents au moyen desquels la culpabilité ou l´innocence d´une personne est établie lors d´un procès. Les preuves électroniques comprennent toutes les preuves existant en forme digitale ou électronique. Comme le mentionne le chapitre premier (connectivité globale), les preuves électroniques sont fondamentales, non seulement dans le cadre des poursuites et des enquêtes sur la cybercriminalité, mais de plus en plus pour la criminalité en général. Les cadres juridiques optimisés pour les preuves électroniques, ainsi que la capacité des services répressifs et de la justice pénale d´identifier, de collecter et d´analyser les preuves électroniques, sont donc essentiels pour une riposte efficace contre la criminalité.

Lors de la collecte des informations pour l´étude, on interrogea les pays sur la capacité des autorités chargées de l´application de la loi et des procureurs de collecter et de gérer les preuves électroniques. Des questions furent également posées sur les cadres juridiques pour les preuves électroniques, la recevabilité des preuves électroniques et les lois et les règles de preuve qui s´appliquent aux preuves électroniques. [1] Avant d´examiner les réponses des pays, cette section contient une brève introduction sur la nature des preuves électroniques et les moyens permettant de les collecter, y compris la criminalistique numérique.

1 Questionnaire de l'étude sur la cybercriminalité Q109-112, et Q143-150.

Générer des preuves – l´interaction d´un usager avec des dispositifs électroniques produit de nombreuses traces numériques générées par un système informatique (parfois appelées empreintes numériques ou artefacts). Les données informatiques et les communications électroniques qui sont potentiellement importantes pour un acte criminel peuvent inclure des giga-octets de photographies, de vidéos, de courriels, de journaux, de conversations et de données du système. Localiser les informations pertinentes dans ces données peut exiger beaucoup de temps. La variété de formats de fichiers possibles, de systèmes d´exploitation, de logiciels d´application et d´éléments de hardware peut aussi compliquer le processus d´identification des informations pertinentes.

Les artefacts informatiques peuvent être facilement modifiés, écrasés ou effacés et posent donc des problèmes car les sources d´informations numériques doivent être authentifiées et vérifiées.[2] Les règles de la preuve varient considérablement en fonction de la juridiction, et même entre les pays qui ont des traditions juridiques similaires. Cependant, les systèmes juridiques dans la tradition de Common Law tendent généralement à avoir des règles définies en matière de recevabilité de la preuve. Dans les systèmes juridiques dans la tradition de droit civil, dans lesquels des juges professionnels maintiennent un niveau élevé de contrôle sur les procédures du tribunal, la recevabilité de la preuve peut être flexible, même si la pondération des éléments de preuve (y compris la vérification de leur crédibilité et leur authenticité) peut aussi être soumise à un ensemble de règles.[3]

Dans plusieurs systèmes juridiques, la qualité des procédures appliquées pour maintenir l´intégrité des informations numériques depuis le moment de leur création jusqu´à leur introduction devant le tribunal, doit être démontrée par le proposant de la preuve. L´intégrité et l´authenticité des informations numériques ont une influence directe sur le poids de la preuve, pour ce qui concerne sa crédibilité et sa véracité. La partie qui cherche à présenter une preuve doit généralement démontrer la pérennité de la preuve ou la chaîne de garde, afin de démontrer que les preuves n´ont pas été falsifiées ni altérées. La pérennité de la preuve est généralement une question de fait et le processus de la chaîne de garde est le mécanisme appliqué pour maintenir et documenter l´historique chronologique de la preuve qui a été déplacée d´un lieu à l´autre.[4]

Dans le cas des informations numériques, la pérennité de la preuve doit être maintenue et concerne le *dispositif physique* qui héberge les données (quand il est reçu ou saisi) et les *données stockées* contenues dans le dispositif.[5] Ainsi, la partie qui présente la preuve doit démontrer que : (i) les informations numériques obtenues à partir du dispositif sont une représentation véridique et précise des données originales contenues dans le dispositif (authenticité) ; et que (ii) le dispositif et les données que la partie souhaite présenter comme preuve sont les mêmes que ceux qui ont été initialement découverts et qu´ils ont été postérieurement placés sous surveillance (intégrité). La finalité est de démontrer que le dispositif est ce qu´il est prétendu être et que les informations numériques sont véridiques et n´ont pas été falsifiées ni altérées.[6]

La fiabilité des informations générées et stockés sur un ordinateur a également été contestée en se basant sur les failles de sécurité des programmes et des systèmes d´exploitation qui pourraient menacer l´intégrité des informations numériques.

2 Voir, par exemple, l*es États-Unis contre Whitaker*, 127 F3d 595, 602 (7ieme Cir. 1997).

3 Voir Jackson, J.D., et Summers, S.J., 2012. *L´internationalisation de la preuve criminelle : au-delà de la Common Law et de la tradition de droit civil*.
Cambridge : Cambridge University Press.

4 Casey, E., 2011. *Preuves électroniques et délits informatiques : la criminalistique, les ordinateurs et l´internet*. New York : Elsevier.

5 Département de Justice des U.S, 2007. *Les preuves électroniques dans la salle d´audience : un guide pour es procureurs et les services répressifs*. Institut national deJustice, p.16.

6 Marcella Jr., A.J., Greenfield, R.S., (eds.), 2002. *Cyber criminalistique : un manuel de terrain pour collecter, examiner et préserver les preuves des délits informatiques*, 2nd edn. Boca Raton : CRC Press, p.136.

7 *Re Vee Vinhnee, Débiteur American Express Travel Related Services Company, Inc contre Vee Vinhnee* 336 BR 437 (9ieme Cir. BAP, 16 Décembre2006), p.18.

La vulnérabilité des informations numériques à la manipulation a été tenue en compte par les tribunaux lorsque des preuves électroniques ont été présentées, et ils ont souligné « *la nécessité de démontrer la précision de l´ordinateur pour rechercher et conserver les informations en cause* »[7] La recevabilité des informations générées par ordinateur (comme les registres de fichiers journaux) qui détaillent les activités sur un ordinateur, un réseau ou tout autre dispositif, peut être contestée si le système qui génère les informations n´a pas de solides contrôles de sécurité.[8]

Outre le fait de devoir démontrer l´authenticité et l´intégrité de la preuve, des difficultés relatives à l´utilisation de preuves électroniques surgissent, dans certaines juridictions, avec l´application de *règles de preuves* particulières. Il peut, par exemple, être nécessaire de démontrer que les preuves électroniques tombent sous le coup d´une interdiction générale de preuve par ouïe dire avec des exceptions particulières,[9] ou que, par exemple, l´impression de données informatiques satisfait les exigences de la règle de la meilleure preuve.[10] Les approches nationales relatives à ces problèmes mentionnés sur le questionnaire de l´étude sont abordées dans ce chapitre.

Criminalistique numérique

Plusieurs formes de preuves électroniques peuvent être relativement simples, comme, par exemple, l´impression d´un courriel facilement accessible envoyé par un délinquant, ou les journaux de connexion IP directement signalés par un fournisseur de services internet. D´autres formes de preuves électroniques peuvent néanmoins requérir des techniques sophistiquées pour récupérer les traces d´activités ou les données des ordinateurs et des réseaux qui peuvent fournir des preuves d´une conduire délictueuse. La criminalistique numérique est la branche de la criminalistique qui s´occupe de récupérer et d´enquêter sur le matériel qui se trouve sur des systèmes numériques et informatiques. Pour découvrir ces traces, les experts en criminalistique numérique exploitent la tendance des ordinateurs à stocker et enregistrer les détails de pratiquement chaque action exécutée par les usagers.

Scénario criminalistique : preuve d´une fraude informatique dans un café internet

Scénario : il y a eu une tentative de fraude par courriel. La police obtient la preuve que les courriels en cause peuvent avoir été envoyés d´un ordinateur de bureau d´un café internet local

L´installation d´un café internet typique ressemble à bien des égards à un environnement de réseau domestique. Il contient probablement de multiples ordinateurs portables ou ordinateurs de bureau connectés avec des appareils réseau par câble et sans fil. Pour facturer l´utilisation des ordinateurs, un cybercafé peut exiger l´identification d´un utilisateur ; cela peut être obligatoire dans plusieurs juridictions et cela fournit une piste de vérification qui permet d´associer un individu à un ordinateur spécifique à un moment donné. Il peut aussi être possible d´identifier la personne qui utilise un ordinateurà un moment donné avec l´enregistrement des caméras de sécurité.

Si une enquête est menée assez rapidement, ou s´il y a une connaissance préalable des activités, les enquêteurs criminalistiques peuvent alors être à même d´obtenir un accès physique à l´ordinateur et de mener une enquête standard. Ce processus est compliqué en raison du caractère public du dispositif, qui contient les traces d´activités de nombreux usagers.

Un café internet, qui gère davantage de trafic et d´usagers qu´un réseau résidentiel, a probablement des dispositifs supplémentaires de réseau comme des serveurs proxy servers qui conservent des copies des pages web les plus souvent requises afin d´accélérer le traficet des pare-feu pour la sécurité. Ces dispositifs doivent être analysés pour rechercher des traces d´activités de réseau liées aux activités suspectes de l´usager.

8 Chaikin, D., 2006. Enquêtes de réseau des cyber attaques : les limites des preuves numériques. *Criminalité, droit et changement social*, 46(4-5) :239256, 249.

9 La preuve par ouïe dire est souvent définie comme *« la preuve d´une déclaration faite à une autre occasion, dans le but d´établir la véracité de son contenu »* (*Halbury »s Laws*, Vol. 17). Certains types de preuves électroniques peuvent constituer strictement une preuve par ouïe dire, mais pourraient être admises sous des exceptions telles que des « documents commerciaux ». Voir Thomson, L.L.,

2011. La recevabilité des documents électroniques en tant qu´éléments de preuve dans les tribunaux des U.S. Appendice IX.B.1, *Centre de bibliothèques de recherche, étude des droits de l´homme sur les preuves électronique*

10 Selon le principe général, la meilleure preuve doit être présentée devant les tribunaux courts. Si la règle de la meilleure preuve est appliquée, les copies de l´original peuvent ne pas être recevables comme éléments de preuve à moins qu´il ne soit possible de démontrer que l´original n´est pas disponible car il a été détruit ou en raison d´autres circonstances. L´impression des informations contenues dans un ordinateur ou un autre dispositif de stockage ne devrait pas techniquement être considérée « originale ». Cependant, dans certaines juridiction la règle de la meilleure preuve n´exclut pas les impressions lorsque l´impression reflète avec exactitude les données réelles. Voir, par exemple, *Doe contre les États unis*, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992) ; et *Laughner contre l´État* 769 N.E.2d 1147, 159 (Ind. Ct. App. 2002).

Les informations stockées sur des dispositifs électroniques, y compris les ordinateurs et les téléphones portables, sont volatiles et facilement altérées ou corrompues durant les enquêtes. Par ailleurs ces informations sont facilement reproduites. La première étape fondamentale des enquêtes en matière de criminalistique numérique est donc de créer une *image* criminalistique intacte(ou une copie bit à bit) du dispositif de stockage, contenant une copie du dispositif original aussi détaillée que possible. En opérant sur l´image plutôt que sur le dispositif original, les données peuvent être examinées sans altérer l´original et cela fournit donc une garantie contre les altérations ou les falsifications. Une image criminalistique est généralement créée à l´aide d´un dispositif spécial appelé un *bloqueur d´écriture* qui évite que ne soient altérées les données originales.[11]

Scénario criminalistique : preuve de conspiration pour commettre un délit grave obtenue d´un opérateur mobile

Scénario : une personne fait l´objet d´une enquête car elle est soupçonnée de conspirer pour commettre un homicide. Dans le cadre de l´enquête, la police demande des données à l´opérateur de téléphonie mobile de cette personne.

Les capacités d´un opérateur de téléphonie mobile sont similaires à ceux d´un fournisseur de services internet combinées à ceux d´un fournisseur de téléphonie fixe, avec l´ajout de données de géolocalisation qui révèlent la localisation de l´usager.

Les renseignements du trafic téléphonique, dans la plupart des juridictions, comprennent les numéros de téléphone composés ainsi que l´heure et la durée de l´appel. Les capacités en matière d´écoute sont similaires à celles d´autres fournisseurs de téléphonie. Ces informations peuvent révéler des patrons d´appels à d´autres personnes et établir des corrélations entre des faits du monde réel, comme par exemple lorsqu´un appel téléphonique est réalisé peu après qu´un délit ait été commis.

La différence la plus significative avec les téléphones portables est le dispositif est transporté par son propriétaire à tout moment et est constamment connecté à une station de base locale pour les téléphones mobiles qui relaie les signaux de téléphone. En localisant la station de base à laquelle le téléphone est connecté à un moment donné on peut en déduire la localisation de la personne dans une région déterminée. S´il est activement triangulé en utilisant de multiples stations de base un téléphone peut être localisé dans un rayon de quelques dizaines de mètres.

Selon la juridiction et les politiques de conservation des données, les fournisseurs peuvent stocker les localisations géographiques des téléphones portables lorsqu´ils envoient ou reçoivent des messages ou des appels, comme l´indique la Directive sur la conservation des données de l´Union européenne. D´autres juridictions peuvent ne pas conserver ces données du tout, sauf sur une demande explicite des services répressifs, et la triangulation de la localisation pourrait alors permettre de localiser avec précision une personne par le biais de son téléphone.

Outre la création de copies bit à bit pour les informations stockées, d´autres outils criminalistiques importants incluent l´utilisation de logiciels de récupération de données ou de fichiers qui peuvent récupérer les fichiers supprimés ou altérés des restes de données brutes sur les dispositifs de stockage après que le fichier original ait disparu.[12] De plus, pour comparer rapidement et avec précision les fichiers, les outils d´analyse utilisent le hachage cryptographique qui correspond à une petite et unique « signature » pour un élément de donnée déterminé. Effectuer le plus petit changement sur une donnée causerait un résultat de hachage différent. Divers dispositifs requièrent des techniques criminalistiques et des techniques d´enquête différentes. L´examen de dispositifs mobiles requiert des outils différents de ceux qui sont employés pour examiner un ordinateur de bureau ou un serveur de réseau. Les différents types de matériel informatique, de logiciels et de systèmes d´exploitation présentent chacun des problèmes différents pour récupérer les informations.

La criminalistique informatique s´occupe de l´analyse des ordinateurs portables et de bureaux, des domiciles et des entreprises. Les ordinateurs contiennent généralement des disques durs à haute capacité qui stockent une grande quantité d´informations, de photos et de vidéos, ainsi que les historiques de navigation internet et des informations concernant les courriels et les messages instantanés. Ils utilisent généralement un petit nombre de systèmes d´exploitation bien connus tels que Windows, Mac OS, et Linux.

11 Institut national des standards et des technologies des U.S, 2004. *Spécifications du bloqueur en écriture(HWB) Version 2.0.*

12 Gutmann, P., 1996. Suppression sécurisée de données de mémoire magnétique et transistorisée. *Procédures du 6ieme symposium USENIX sur la sécurité.*

La criminalistique des dispositifs portables examine les dispositifs portables de faible puissance, avec une capacité de stockage inférieure à celle des ordinateurs et dont le logiciel plus simple permet de réaliser des appels téléphoniques et de naviguer sur internet. L´écart entre les téléphones et les ordinateurs tend cependant à devenir moindre, en ce qui concerne le logiciel, la fonctionnalité et la capacité de traitement. La caractéristique des téléphones portables est leur mobilité – ils sont généralement avec leurs propriétaires à tout moment –et leur constante connectivité. Ceci permet de surveiller la localisation géographique avec une précision raisonnable dans les systèmes modernes. Les téléphones mobiles contiennent souvent une liste relativement complète de contacts et de registres d´appels. Toutes les données et les informations sur un réseau mobile ISP permettent aux enquêteurs d´obtenir de nombreuses informations relatives à l´utilisation du téléphone. Les tablettes électroniques sont souvent des versions à plus grande échelle d´un téléphone portable, et, pour cette raison, les outils conçus pour les téléphones portables sont aussi applicables.

Exemple de cas : identifier un extorqueur sur internet (un pays d´Amérique du nord)

Une enquête menée par les services répressifs sur un présumé extorqueur illustre certaines des techniques utilisées pour dépister les délinquants en ligne. L´accusé menaçait de publier des images sexuelles de ses victimes sur leurs propres pages de réseaux sociaux.
Les enquêteurs reçurent des informations du service de sécurité du site de réseau social sur les connexions aux comptes des victimes, toutes provenaient d´une seule adresse IP. Une personne, depuis cette adresse IP, avait accédé à 176 différents comptes en moins de deux mois, en général depuis le même ordinateur. Plusieurs utilisateurs de ces comptes les avaient désactivés après avoir été piratés. La même adresse IP avait été utilisée pour accéder au propre compte du suspect 190 fois, davantage que pour les autres adresses. Elle avait aussi été utilisée 52 fois pour accéder aux comptes de courriels d´une des victimes. Une connexion séparée du compte du suspect provenait d´une adresse IP enregistrée comme une entreprise, inscrite comme l´employeur du suspect sur son profil du réseau social. Sur cette base, une requête fut adressée au fournisseur de services pour obtenir des informations sur l´abonné associé à cette adresse IP. Au bout d´une semaine, il transmit les renseignements relatifs à l´abonné, en incluant une adresse physique qui concordait avec d´autres registres publics. Les enquêteurs exécutèrent un mandat de perquisition dans ses locaux et saisirent des preuves qui furent utilisées pour inculper le suspect au cours du même mois.

Source : http ://www.justice.gov/usao/cac/Pressroom/2013/016.html et http ://arstechnica.com

Les techniques criminalistiques de réseau sont essentielles dans l´actualité car les ordinateurs et les téléphones mobiles, et les actes pour lesquels ils sont utilisés, sont associés aux services en ligne et au stockage en nuage. Ces services stockent des données sur internet plutôt que sur les dispositifs de l´usager et réduisent la quantité d´informations pouvant être collectées sans utiliser l´analyse de réseau. Le trafic de réseau est en grande partie transitoire. Pour obtenir des informations détaillées sur les activités qui ont lieu sur un réseau, le trafic doit être collecté et stocké à des fins d´analyse ultérieure. Ceci peut inclure l´analyse des fichiers journaux des dispositifs de réseau tels que les pare-feu et les systèmes de détection et de prévention des intrusions, ainsi que l´analyse du contenu du trafic de réseau enregistré lorsqu´il est disponible.[13]

Dans les cas où un attaquant peut avoir obtenu l´accès électronique à un système informatique, toutes les données de cet ordinateur peuvent avoir été compromises par l´attaquant. Dans ces cas, les fichiers journaux de l´activité de ce système ne sont probablement pas considérés

comme étant fiables et la criminalistique de réseau peut être le seul moyen pour un analyste d´obtenir des données. La plus grande difficulté d´une enquête criminalistique de réseau est de reconstruire les actions qui ont été exécutées sur le réseau à partir des données disponibles du journal qui sont limitées. Ceci peut être utilisé pour détecter des tentatives de piratage, des accès non autorisés au système et des tentatives de déni de services, ainsi que les données indiquant les ressources auxquelles ont eu accès les personnes à un moment donné.

13 Chappell, L., 2012. *Analyse de réseauWireshark (Seconde édition) : guide officiel d´étude de l´analyse de réseau Wireshark*. Laura Chappell University.

6.2 Capacité en matière de traitement de preuves électroniques et de criminalistique numérique

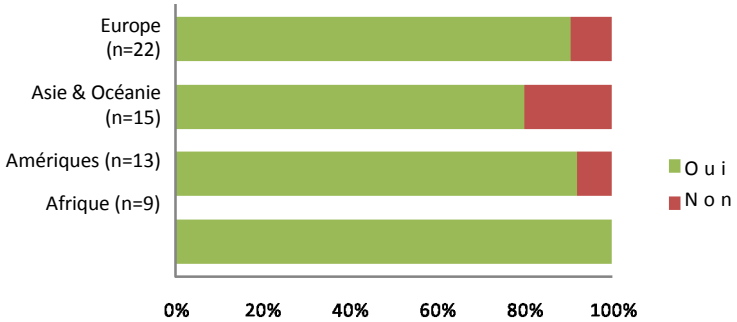
Principaux résultats :

- pratiquement tous les pays ont mentionné des capacités de criminalistique numérique. Cependant, divers pays, de toutes les régions du monde, ont signalé un nombre insuffisant d´experts en criminalistique, des différences entre les capacités existantes au niveau fédéral et au niveau étatique, un manque d´outils criminalistiques et des retards causés par d´immenses quantités de données à analyser ;
- la moitié des pays a signalé que les suspects utilisent le cryptage et cela rend difficile l´accès à ce type de preuves et prend beaucoup de temps sans la clé de décryptage ;
- tous les pays d´Afrique et un tiers des pays d´autres régions du monde ont signalé que les ressources étaient insuffisantes pour les procureurs traitent et analysent les preuves électroniques ;
- les preuves électroniques sont recevables devant les tribunaux pour plus de 85 % des pays répondants. Bien qu´en nombre restreint, des obstacles juridiques tels que l´irrecevabilité de toutes les preuves électroniques ou l´irrecevabilité des preuves électroniques extraterritoriales, représentent de sérieux obstacles pour la poursuite des actes de cybercriminalité.

Capacité criminalistique

La capacité des services répressifs de collecter et d´analyser les preuves électroniques durant les enquêtes peut être cruciale pour l´identification et la poursuite fructueuses des délinquants. Les pays qui ont répondu au questionnaire de l´étude ont indiqué un panel de capacités à cet égard. Plus de 90 % des pays, de toutes les régions du monde, ont mentionné la capacité de mener des enquêtes basées sur la criminalistique numérique.[14]Des informations additionnelles fournies par les pays, relatives à l´accès à des ressources en matière de criminalistique et aux niveaux de capacités, révèlent une situation différente. Moins de la moitié des pays d´Afrique et environ deux tiers des pays d´Amérique déclarèrent que les services répressifs disposaient de suffisamment de ressources (comme l´électricité, du matériel informatique, des logiciels et l'accès à internet) pour mener des enquêtes et analyser des preuves électroniques.[15] Par contre, presque 80 % des pays d´Europe, d´Asie et d´Océanie, déclarèrent disposer de suffisamment de ressources.

Figure 6.1 : capacité des services répressifs en matière de criminalistique électronique



Source : questionnaire de l´étude sur la cybercriminalitéQ110.

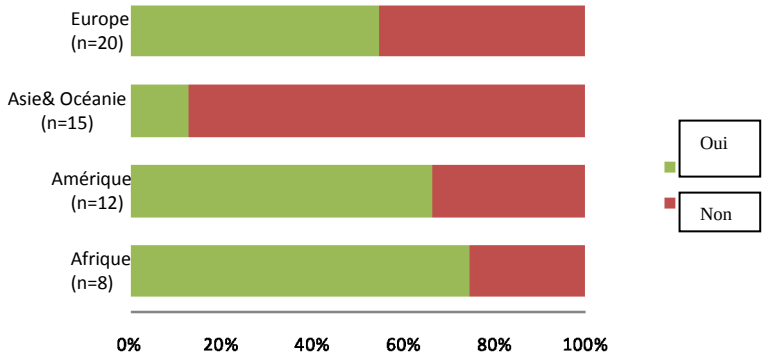
Cependant, plusieurs pays, y compris certains pays développés, mentionnèrent des difficultés associées au traitement de grandes quantités de données et au nombre croissant de dispositifs soumis à une analyse criminalistique.[16]

14 Questionnaire de l´étude sur la cybercriminalitéQ110.
15 Questionnaire de l´étude sur la cybercriminalitéQ109.
16 Questionnairede l´étude sur la cybercriminalitéQ110.

Un pays d´Europe signala, par exemple, que « *au niveau national, la police est hautement qualifiée en matière de criminalistique informatique. Au niveau local et du district, elle peut seulement effectuer un travail basique en matière de criminalistique informatique* ». Le même pays déclara que « *le nombre croissant de preuves électroniques saisies durant les enquêtes sur tous types de délits pose un problème, en particulier pour la police locale qui gère un grand nombre de cas* ». De même, un pays d´Amérique souligna que « *la difficulté ne réside pas dans l´expertise, mais dans la quantité de données qui doivent être analysées* »[17] et un autre pays déclara que « *la quantité des informations et des données saisies cause des problèmes croissants en matière d´analyse et de stockage* ».[18]

Alors que certains pays ont mentionné une capacité fédérale ou centralisée d´un « *laboratoire central [criminalistique] et des périphériques chargés de l´analyse experte des preuves électroniques saisies lors des enquêtes de police* »[19], d´autres mentionnèrent une approche distribuée avec « *des unités criminalistiques réparties dans tout le pays* »[20] « *qui effectuaient des analyses criminalistiques électroniques avec des outils criminalistiques spécialisés...utilisés dans les réseaux, les systèmes informatiques, les téléphones mobiles et les dispositifs de stockage* ».[21] Plusieurs pays, en particulier des pays en développement, mentionnèrent un manque de ressources en matière d´équipement technique criminalistique et des difficultés pour recruter du personnel ayant les compétences suffisantes pour mener des enquêtes et administrer les preuves électroniques. Un pays d´Afrique a, par exemple, déclaré que « *quelques enquêteurs criminalistiques sont disponibles au niveau fédéral, mais ils ne sont pas assez nombreux pour tout le pays. Un seul laboratoire est fonctionnel* ».[22]

Figure 6:2 : preuves électroniques codées par des suspects



Source : questionnaire de l´ étude sur la cybercriminalité Q112. (n=55)

De nombreux pays ont déclaré faire face au cryptage de données lors des enquêtes menées par les services répressifs et de l´analyse des preuves électroniques. Entre 60 et 80 des pays de toutes les régions, à l´exception de l´Asie et de l´Océanie, ont déclaré que les preuves électroniques étaient souvent chiffrées par les suspects.[23] Plusieurs pays ont déclaré que les délinquants utilisent de plus en plus le cryptage. Un pays a observé que « *en fonction du type de délit, le cryptage devient beaucoup plus commun* ».[24] Ce point de vue n´est cependant pas universel. Un pays d´Europe a, par exemple, mentionné que « *les preuves collectées sont très rarement encodées par rapport à l´énorme quantité de données saisies* ».[25] De plus, savoir si la faible proportion de cryptage signalée par les pays d´Asie et d´Océanie est due à des différences dans l´utilisation sous-jacente de l´encodage par les suspects, ou aux capacités de détection et d´analyse du matériel codé des services répressifs n'est pas claire.

17 Questionnaire de l´étude sur la cybercriminalitéQ109.
18 *Ibid.*
19 *Ibid.*
20 *Ibid.*
21 *Ibid.*
22 Questionnaire de l´étude sur la cybercriminalité Q111.
23 Questionnaire de l´étude sur la cybercriminalitéQ112.
24 *Ibid.*
25 *Ibid.*
26 *Ibid.*
27 *Ibid.*

Les pays ont déclaré qu´il n´y avait pas « *de manière simple* » de surmonter le « *défi de taille* que représente l´encryptage car *« cela requiert des capacités et une assistance technique expertes* ».[26] Plusieurs pays ont déclaré ne pas posséder les moyens ou les outils qui permettent de traiter le problème de l´encryptage, sans obtenir ou saisir la clé de décryptage du suspect. Un pays a mentionné que : « *si le suspect est arrêté ou connu, on obtient la clé de décryptage du suspect durant l´enquête* ».[27] Certaines juridictions ont des recours juridiques pour contraindre une personne à coopérer.[28] Si le suspect ne révèle pas la clé de décryptage, les enquêteurs peuvent utiliser divers logiciels, entreprendre une expertise technique, ou transmettre la preuve potentielle aux laboratoires criminalistiques ou au personnel spécialisé pour tenter de la décoder. Un pays a déclaré qu´il utilisait « *des professionnels certifiés et des logiciels certifiés* »[29] dans ses efforts de décryptage. D´autres pays mentionnèrent la possibilité d´arrêter un suspect « *lorsque les machines sont ouvertes et en fonctionnement* »[30] lorsque les données ne sont pas chiffrées.

Outre les difficultés que représente la technologie de cryptage pour la criminalistique numérique, les délinquants peuvent aussi utiliser la « sténographie » (« dissimuler » l´information). Ceci consiste à dissimuler des informations ou des communications dans des fichiers innocents, comme des images graphiques, des documents, des échantillons audio ou des applications. Les fichiers multimédias sont les hôtes idéaux pour la sténographie car ils sont généralement volumineux et ne suscitent pas immédiatement des soupçons. Du point de vue de la criminalistique, l´identification de données cachées peut s´effectuer en comparant des fichiers suspects ou des flux de données avec les originaux connus. De nombreux pays répondants ont mentionné une utilisation accrue des techniques d´obfuscation et de cryptage. Un pays d´Amérique a souligné que « *les organisations criminelles tentent de rendre les enquêtes difficiles en stockant les données liées aux actes criminels dans des serveurs étrangers ou dans des systèmes de stockage en nuage, et utilisent la cryptographie et d´autres techniques d´obfuscation de données ».*[31]

L´utilisation accrue de l´informatique en nuage représente un problème pour la criminalistique informatique. Les informations stockées à distance par les délinquants dans les services d´informatique en nuage peuvent devenir visibles pour les enquêteurs durant une recherche ou une analyse criminalistique – comme lorsque des sessions d´internet en direct sont localisées sur des ordinateurs en fonctionnement, ou au moyen de services à distance disponibles sur les dispositifs mobiles saisis. Outre les considérations juridiques relatives à l´accès direct, des services répressifs aux données extraterritoriales (examinées au chapitre sept (coopération internationale)), le stockage des données en nuage complique le processus criminalistique d´identification, de collecte et d´analyse des informations stockées sous forme informatique.[32] La possibilité qu´un utilisateur de nuage obtienne un accès aux données d´une autre personne introduit la possibilité de problèmes supplémentaires concernant l´authenticité des données.

Face à ces problèmes, les pays répondants ont mentionné une variété de techniques utilisées pour garantir que l´intégrité des preuves électroniques collectées au moyen de la criminalistique numérique soit maintenue. Les pays ont, par exemple, mentionné l´utilisation de l´imagerie criminalistique ; l´utilisation de déclarations sous serment attestant l´authenticité des données ; des valeurs de hachage ; l´utilisation de bloqueurs en écriture ; la capture de données d´internet par capture d´écran ; l´étiquetage systématique, les méthodes de documentation, d´emballage et de transportet le scellement des images enregistrées sur un disque optique.[33] Pour ce qui concerne les normes et les directives des enquêtes criminalistiques quelques pays ont mentionné le Guide de bonnes pratiques en matière de preuves électroniques de l´Association des hauts fonctionnaires de la police.[34]

---

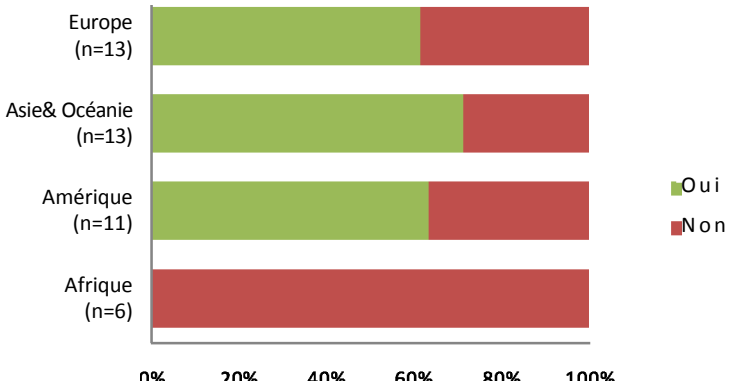
28 La loi de 2000 régissant les pouvoirs d´enquête d´un pays du nord de l´Europe, prévoit le pouvoir d´imposer une obligation de divulgation à un suspect afin qu´il révèle la clé des informations qui sont en sa possession. Le non-respect d´un avis de divulgation peut donner lieu à une peine de prison et /ou une amende s´il est reconnu coupable. De même, la loi de 2001 sur la cybercriminalité d´un pays *d´Océanie* habilite un magistrat à émettre une ordonnance exigeant qu´une personne fournisse des informations ou prête une assistance raisonnable et nécessaire à un officier des services répressifs, afin qu´il ait accès aux données contenues ou accessibles d´un ordinateur.

29 *Ibid.*

30 *Ibid.*
31 Questionnaire de l´étude sur la cybercriminalitéQ85.
32 Reilly, D., Wren, C., and Berry, T., 2011. Informatique en nuage : avantages et inconvénients pour les enquêteurs en criminalistique informatique. *International Journal Multimedia and Image Processing*, 1(1) :26-34, 33.
33 Questionnaire de l´étude sur la cybercriminalité Q111.
34 voir http ://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf

Les pays ont également signalé de nombreuses pratiques pour stocker les preuves électroniques, afin de les protéger contre la détérioration et les dommages. Cela inclut l´utilisation de multiples exemplaires de copies faites à partir d´une seule copie maitresse ; le stockage de données informatiques dans un réseau TI désigné sous accès restreint ; l´utilisation d´installations dont l´humidité, la température et la radiation électromagnétique sont contrôlées ; l´utilisation de coffres-forts, l´utilisation de dispositifs antistatiques ; l´utilisation de casiers de preuves surveillés et l´utilisation de sacs scellés.[35]

Figure 6.3 : ressources suffisantes pour gérer et analyser les preuves électroniques



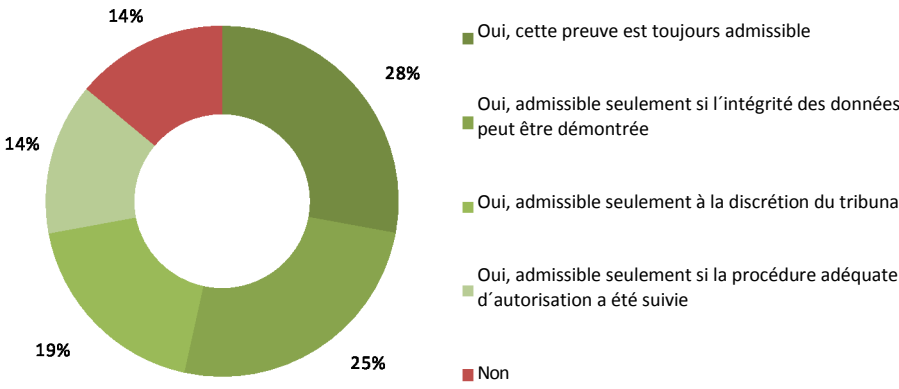
Source : questionnaire de l´étude sur la cybercriminalité Q149. (n=44)

Outre la capacité des services répressifs en matière de criminalistique numérique, il est également important que les procureurs aient des ressources suffisantes pour gérer et analyser les preuves électroniques. Les preuves qui ne sont pas présentées au procès n´ont aucune incidence sur le jugement de l´accusé. Les réponses fournies par les pays montrent que les procureurs disposent de moins de ressources que les services répressifs pour gérer les preuves électroniques.[36] Certains pays ont, par exemple, commenté que les procureurs éprouvent souvent des difficultés pour comprendre les preuves électroniques et requièrent l´assistance d´autres professionnels pour identifier les tendances et la signification des données.[37] Aucun des pays africains qui ont répondu ne considérait suffisantes les ressources pour les preuves électroniques – et cela démontre un besoin urgent en matière de support et d´assistance techniques.

Les preuves électroniques dans les procédures pénales

Plus de 85 % des pays répondants ont déclaré que les preuves électroniques étaient admissibles dans les procédures pénales.[38] Un petit nombre de pays – particulièrement en Afrique et en Asie – ont toutefois déclaré que les preuves électroniques n´étaient pas recevables. Un pays en Afrique considérait, par exemple, que les preuves électroniques « *Ne sont pas définies dans notre législation et sont donc inadmissibles* ».[39]Il existe dans ce cas de sérieux obstacles à une poursuite fructueuse des actes de cybercriminalité et des délits qui impliquent des preuves électroniques.

Figure 6.4 : preuves électroniques admissibles dans les procédures pénales



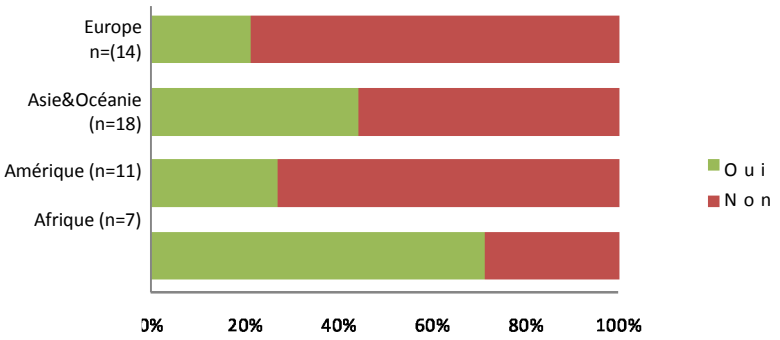
Source : questionnaire de l´étude sur la cybercriminalité Q144. (n=43)

35 Questionnaire de l´étude sur la cybercriminalitéQ111.
36 Questionnaire de l´étude sur la cybercriminalité Q149.
37 Questionnaire. de l´étude sur la cybercriminalitéQ149.

38 Questionnaire de l´étude sur la cybercriminalité Q144.
39 Questionnaire de l´étude sur la cybercriminalitéQ143.

Dans le cas des pays pour lesquels les preuves électroniques sont généralement admissibles lors des procédures pénales, la recevabilité des preuves est soumise à des conditions, comme le fait de démontrer l´intégrité des données, la discrétion du tribunal ou les procédures d´autorisation, dans environ 70 % des pays.[40]

Figure 6.5 : distinction juridique entre les preuves électroniques et les preuves physiques



Source : questionnaire de l´étude sur la cybercriminalitéQ143. (n=50)

Malgré la reconnaissance généralisée des preuves électroniques dans les tribunaux nationaux, un pays déclara ne pas reconnaître les preuves électroniques *de l´extérieur* de sa juridiction.[41] Quand il s´agit de délits transnationaux comme dans le cas des cyberdélits, une telle restriction peut avoir une incidence sur la possibilité d´engager des poursuites fructueuses. De nombreux pays ont déclaré que le problème de la recevabilité des preuves électroniques extraterritoriales dépend souvent du fait que les procédures d´entraide judiciaire aient été correctement suivies. Un pays a, par exemple, souligné que « *les preuves étrangères apportées lors des procédures pénales doivent être sous forme de témoignage et toute pièce à conviction annexée à ce témoignage … ; le témoignage doit être fait sous serment ou affirmation, sous un avertissement qui serait accepté par un tribunal du pays étranger, ou sous l´obligation imposée de dire la vérité, expressément ou indirectement, conformément à une loi du pays étranger, et le témoignage doit prétendre être signé ou certifié par un juge, un magistrat ou un officier* ».[42] Dans plusieurs juridictions, ces exigences évitent fréquemment que les preuves électroniques extraterritoriales obtenues par des voies informelles entre les polices soient utilisables dans des procès pénaux.

La majorité des pays qui admettent les preuves électroniques ont déclaré ne pas établir de différence entre les preuves électroniques et les preuves physiques. Un peu moins de 40 % des pays ont signalé l´existence d´une distinction juridique entre les preuves électroniques et les preuves physiques.[43] Bien que les approches varient, plusieurs pays considèrent ceci comme une bonne pratique car cela garantit une recevabilité équitable de tous les autres types de preuves. Dans le cas des pays qui n´établissent pas de distinction juridique entre les preuves électroniques et les preuves physiques, plusieurs déclarent que les preuves électroniques, ainsi que leur contrepartie traditionnelle, « *doivent être : admissibles ; authentique ; précises, complètes et convaincantes pour les jurys* ».[44] L´admissibilité des preuves électroniques dépend aussi des règles générales qui s´appliquent à toutes les preuves, y compris au fait que les éléments de preuve « *aient été obtenus légalement, en respectant les principes de pertinence et d´abondance* ».[45] Dans quelques pays, le fait de « *décider si une preuve* [*électronique*] *est admissible ou non* est à la discrétion du tribunal ».[46]

Il a été indiqué que les preuves électroniques ont été transmises aux autorités judiciaires ou au parquet et utilisées dans des procès pénaux, de plusieurs façons.

40 *Ibid.*
41 Questionnaire de l´étude sur la cybercriminalité Q145.
42 *Ibid.*
43 Questionnaire de l´étude sur la cybercriminalité Q143.
44 Questionnaire de l´étude sur la cybercriminalité Q143.
45 Questionnaire de l´étude sur la cybercriminalité Q144.
46 *Ibid.*
47 *Ibid.*

Les pays répondants ont tous mentionné : le déplacement physique des ordinateurs saisis au tribunal ; l´utilisation au tribunal de copies des données informatiques stockées sur des disques optiques ; l´utilisation au tribunal d´impressions des données informatiques archivées dans des classeurs et la présentation du témoignage et du rapport analytique d´un expert seulement devant le tribunal (les données informatiques restent en stockage).[47] Quelques pays ont, par exemple, déclaré que les données ou les documents électroniques « *doivent être imprimés afin qu´ils puissent être lus durant l´audience principale* ».[48] Certains pays ont aussi souligné que « *seules les parties pertinentes de la preuve collectée sont transmises aux procureurs – les données et le matériel non pertinents sont stockés par la police* ».[49]

Les pays ont également fourni des détails sur les nombreux moyens et les formes sous lesquelles les preuves électroniques pourraient être présentées au tribunal. Cela va des témoignages rendus par des officiers de police aux témoignages présentés par des professionnels en criminalistique, ainsi que la présentation d´informations numériques sur des projecteurs et des moniteurs à grand écran et des impressions identifiant des objets, des documents, des photographies, des journaux de traces informatiques et des captures d´écran.[50] Un pays d´Asie a mentionné l´utilisation de rapports d´experts en soulignant que « *les rapports écrits sont généralement présentés avec des explications relatives aux données techniques* ». D´autres pays relatent la présentation des preuves électroniques sur des écrans d´ordinateurs : « *dans une affaire de délit informatique sophistiqué, l´utilisation d´un projecteur au tribunal, pour dépouiller les éléments de preuve, s´est révélée un moyen efficace pour que la poursuite transmette des informations au tribunal* ».[51]

D´autres pays mentionnent de multiples moyens de présentation. Un pays d´Europe, par exemple, adéclaré que la présentation de preuves électroniques au tribunal « *Dépend de l´état et de la localisation actuels de la preuve.* [*Les preuves électroniques peuvent être présentées comme*] *des impressions papier, des médias numériques (disques durs, CD, DVD, lecteurs flash), des présentations sur des ordinateurs portables ou de bureau, des présentations à distance et l´accès en direct dans de rares cas* ». Certains pays ont toutefois indiqué que les salles d´audience ne sont généralement pas conçues pour utiliser la technologie lors des procès pénaux. Un pays d´Amérique a, par exemple, signalé que « *les procès électroniques ne sont pas encore communs. Les salles de tribunaux ne sont pas toutes connectées pour ainsi permettre à l´État de présenter les cas de forme électronique Actuellement, l´État doit obtenir le consentement du juge et de l´avocat de la défense pour utiliser la technologie dans la salle d´audience* ».[52]

Très peu de pays ont mentionné l´existence de lois spéciales sur la preuve qui régissent les preuves électroniques. Lorsque c´est le cas, les lois abordent des domaines tels que les présupposés juridiques concernant la propriété ou la paternité des documents et des données électroniques, ainsi que les circonstances dans lesquelles les preuves électroniques peuvent être considérées authentiques.[53] D´autres pays fournissent des informations sur la manière dont les règles sur la preuve traditionnelle peuvent être interprétées dans le contexte des preuves électroniques. Un pays d´Océanie a, par exemple, précisé la manière dont la règle du ouïe dire pouvait s´appliquer aux preuves électroniques dans sa juridiction : « *pour ce qui concerne spécifiquement les preuves électroniques, la règle du ouïe dire n´est pas applicable si les informations contenues dans les preuves électroniques concernent une communication qui a été transmise entre ordinateurs et qui a été admise pour identifier, l´émetteur, le récepteur, la date et l´heure de la transmission* ».[54] Un autre pays signalait aussi qu´il existait la « *présomption générale* » que « *si une preuve a été produite par une machine ou tout autre dispositif, et si ce dispositif produit généralement ce résultat lorsqu´il est correctement utilisé, il est inféré que le dispositif fonctionnait correctement lorsque la preuve a été produite* ».[55]

48 *Ibid.*
49 Questionnaire de l´étude sur la cybercriminalité Q143.
50 Questionnaire de l´étude sur la cybercriminalitéQ150.
51 *Ibid.*
52 *Ibid.*
53 Questionnaire de l´étude sur la cybercriminalitéQ147.
54 Questionnaire de l´étude sur la cybercriminalitéQ146.
55 Questionnaire de l´étude sur la cybercriminalitéQ143.

Enfin, les pays ont mentionné les moyens par lesquels les preuves électroniques pouvaient être utilisées pour établir un lien entre un acte criminel et un délinquant spécifique. La nature de la cybercriminalité implique qu´un dispositif faisant office de médiateur, sous la forme d´un système informatique, est généralement situé entre le délinquant et la victime – ce qui donne lieu à des difficultés pour attribuer des actes à une personne spécifique. Dans les cas où un défendeur est poursuivi, par exemple, pour la possession d´un contenu informatique illégal, il faut établir que le contenu a été sciemment placé sur le dispositif par le défendeur, et non par une autre personne ayant accès au dispositif. À cet égard, un pays a commenté que : « *les preuves circonstancielles sont souvent les seuls moyens d´établir l´identification de la personne qui parle ou se communique. Les méthodes suivantes se sont avérées utiles : prouver la possession du dispositif de communication (saisie après l´arrestation ou exécution d´un mandat), les informations relatives à l´abonné, la surveillance (conformément à une autorisation du tribunal, si elle est requise), l´analyse du contenu de la communication et l´examen criminalistique du dispositif de e communication* ».[56] Un autre pays a observé que *« de multiples séries de preuves électroniques doivent souvent être présentées conjointement pour prouver qu´un suspect utilisait un dispositif électronique à un lieu et un moment particuliers ».*[57]

La plupart des pays a déclaré qu´il n´existe pas de critères ou de mesures spécifiques pour établir ce lien. Les pays ont mentionné une variété de techniques informatiques spécifiques ou de techniques traditionnelles pour « *associer les preuves électroniques à un système informatique sous le contrôle du défendeur ou auquel a accès le défendeur. Les techniques de preuves types incluent la motivation, l´opportunité, les preuves corroboratives non-électroniques, le contrôle des preuves, les preuves relatives à l´état d´esprit et les preuves qui appuient l´exclusion des autres* ».[58] En général, les pays répondants ont mentionné une quantité considérable de connaissances accumulées en matière d´identification, de collecte, d´analyse et de présentation des preuves électroniques. Les bonnes pratiques dans ce domaine furent soulignées non seulement par les pays développés, mais également par de nombreux pays en développement – cela indique des niveaux croissants de dialogue global et la diffusion de normes techniques en matière de preuves électroniques. Cependant, plusieurs institutions des pays en développement – y compris des autorités des services répressifs et du parquet – ont mentionné un manque significatif de ressources et de capacités pour pleinement appliquer ces normes. De plus, dans quelques pays, des obstacles juridiques tels que l´inadmissibilité de toutes les preuves électroniques et l´inadmissibilité des preuves électroniques extraterritoriales, représentent de sérieux obstacles pour la poursuite des actes de cybercriminalité.

6.3 La cybercriminalité et le système de justice pénale dans la pratique

Principaux résultats :

- les procureurs mentionnent une gamme de difficultés pour la poursuite fructueuse des cyberdélits, qui incluent l´insuffisance des cadres juridiques, des difficultés pour attribuer des actes aux individus, des retards dus aux procédures de coopération internationale et des difficultés concernant les preuves ;
- ces difficultés sont illustrées par les statistiques disponibles sur le ratio des suspects et des actes consignés par la police, et par les mesures d´attrition qui comparent le nombre de condamnation au nombre d´actes consignés ;

Cette section élargit les thèmes des preuves criminalistiques et électroniques à la performance du système de justice pénale, dans son ensemble, dans les affaires de cybercriminalité. Elle examine les difficultés et les bonnes pratiques mentionnées par les procureurs et les tribunaux, et identifie leurs éventuelles incidences sur les poursuites et les condamnations des auteurs de cyberdélits.

56 Questionnaire de l´étude sur la cybercriminalitéQ148.
57 *Ibid.*
58 *Ibid.*
56 Questionnaire de l´étude sur la cybercriminalitéQ148.

Difficultés et bonnes pratiques relatives aux poursuites

Les pays répondants ont identifié des difficultés et des bonnes pratiques dans le contexte des procédures de justice pénale, depuis la soumission de l´affaire jusqu´à ce que soit rendue la décision finale. Un pays a, par exemple, proposé un panel complet de bonnes pratiques dans le domaine de la gestion des cas, la divulgation de la preuve et la présentation de la preuve lors du procès l : « *1) collaborer/les transmettre rapidement aux enquêteurs, au personnel de TI, aux parajuristes et aux avocats de la défense ; 2) s´occuper des garanties de contrôle de la qualité, ex, règles commerciales ; 3) enquête de l´inventaire et divulgation de l´indice ; 4) choisir un témoin expert qui puisse témoigner sur les questions de contrôle de qualité telles que l´intégrité de la base de données de la poursuite ; 5) garantir la compatibilité/interopérabilité du système informatique de la police/du gouvernement ; 6) rencontrer et s´entretenir avec l´avocat de la défense dès le début de l´affaire ; 7) éviter de mélanger les médias ; 8) être à même de défendre la divulgation ; 9) tenir compte des métadonnées dès le début de l´affaire et rechercher l´assistance/appui d´experts ; 10) s´assurer que les documents électroniques ont été rédigés de manière appropriée ; 11) choisir l´outil informatique approprié pour le type de preuves qui seront présentées lors du procès (un seul type ne convient pas à toutes les preuves) ; 12) obtenir la permission du juge ; 13) identifier les pièces à conviction à l´avance, essayer l´équipement au bureau /salle du tribunal, avoir un plan de secours et être préparé* ».[59]

Les difficultés mentionnées qui font obstacle à une poursuite fructueuse concernent généralement l´insuffisance des cadres juridiques, l´identification des suspects, la disponibilité et l´interprétation de la preuve et les procédures appropriées pour la gestion des preuves.

Pour ce qui concerne la législation pour les pouvoirs procéduraux (traités au chapitre cinq (application des lois et enquêtes)), les pays répondants ont, par exemple, souligné que le « *manque de cadres juridiques* », « *le manque de législations procédurales*, « *le manque de pouvoirs d´enquête appropriés qui n´enfreignent pas excessivement le droit à la vie privée et à la liberté de parole* » et le manque d´une « *législation spécifique sur la protection de la vie privée* »[60], compliquent et retardent les enquêtes.

Les procureurs ont également mentionné les difficultés citées à la section antérieure de ce chapitre concernant l´attribution d´un acte à un individu. Un pays a, par exemple, déclaré que « *l´attribution d´un acte est en général le point le plus difficile d´une enquête sur un cyberdélit et cela constitue un obstacle pratique pour une poursuite fructueuse* ».[61] Les procureurs des pays répondants ont également mentionné les difficultés liées aux cas qui ont une dimension extraterritoriale, y compris « *la difficulté pour obtenir des preuves qui requièrent la coopération internationale d´autres pays* » et « *les retards lors des poursuites et des enquêtes sur des cyberdélits* », causés par les processus formels de coopération internationale et d´entraide judiciaire.[62]

Les questions liées aux preuves ont été citées comme étant les principaux obstacles à des poursuites fructueuses et cela incluait « *la grande quantité de preuves* », « *la courte période de temps durant laquelle les fournisseurs de services stockent les informations requises à des fins d´enquête,* » « *maintenir l´intégrité des preuves électroniques du moment de la saisie jusqu´à ce que l´affaire soit close* », « *ne pas établir une chaîne de garde des preuves et le manque d´installations de stockage pour maintenir les preuves* ».[63] « *La production de preuves de cyberdélits au tribunal est encore difficile* » et « *le manque d´intégrité de la preuve causé par une gestion inappropriée des services répressifs* »[64] furent aussi mentionnés comme des points particulièrement difficiles par plusieurs pays.

59 Questionnaire de l´étude sur la cybercriminalité Q142.
60 *Ibid.*
61 *Ibid.*
62 *Ibid.*
63 *Ibid.*
64 *Ibid.*
65 Questionnaire de l´étude sur la cybercriminalitéQ142.
66 Questionnaire de l´étude sur la cybercriminalitéQ183.
67 Questionnaire de l´étude sur la cybercriminalitéQ142.
68 *Ibid.*

Les pays ont réitéré l´importance de la collecte et la présentation des preuves. « *Une étroite relation de travail entre les procureurs et les enquêteurs en vue de collecter toutes les preuves pertinentes correctement identifiées* »[65], est fondamentale pour la réussite des poursuites. « *Le matériel informatique, et, s´il y a lieu, le logiciel de l´accusé doivent avoir été saisis aussi rapidement qu´il est légalement possible de le faire... puis une rapide évaluation effectuée par des spécialistes externes ou des membres du personnel hautement qualifiés et spécialement formés* ».[66] « *L´identification et le repérage séparés de tous les documents/images informatiques pertinents,* »[67] une « *chaîne de garde claire des pièces à conviction* »[68] et « *le développement de politiques de présentation des preuves devant le tribunal basées sur des présentations antérieures réussies* »[69], sont des éléments importants des poursuites et des condamnations fructueuses. Enfin, la « *perception d´un manque d´aisance parmi la communauté juridique en matière de concepts, et la manière dont cela influe sur l´administration de la justice* »[70], et « *la compréhension des preuves numériques des officiers judiciaires* »[71], ont été signalées comme des obstacles additionnels pour la poursuite et la condamnation fructueuses des cas de cybercriminalité.

Les problèmes mentionnés incluaient la nécessité de ressources et de formations additionnelles, ainsi qu´une « *meilleure orientation pour les tribunaux à tous les niveaux en résumant (et en diffusant) l´expérience judiciaire permettant d´identifier et d´uniformiser les normes dans les cas de sécurité des systèmes informatiques* ».[72] Un pays a souligné que « *Il est important et décisif, pour la bonne gestion des cas de cybercriminalité, que les tribunaux nationaux aient les moyens financiers adéquats pour acquérir l´équipement technique nécessaire* ».[73] Les partenariats public-privé avec « *les fournisseurs de services internet, les fournisseurs d´hébergement des sites web et d´autres fournisseurs de services* »[74], ainsi qu´avec les sociétés bancaires et de télécommunications, ont également été signalés comme une méthode productive pour renforcer la collecte de preuves.

Les résultats et l´efficacité du système de justice pénale

Les objectifs principaux de la riposte de la justice pénale, à tout type de délit, sont d´obtenir des résultats équitables pour les victimes et pour les délinquants, ainsi que la dissuasion, la réinsertion et la réintégration sociale des délinquants condamnés et un sens général de dissuasion pour les délinquants potentiels.[75] Il est extrêmement difficile d´évaluer dans quelle mesure ces objectifs sont effectivement et efficacement atteints. Ces mesures vont du taux d´attrition qui fournit des informations sur le nombre de personnes suspectes poursuivies et condamnées par le système de justice pénale pour des délits spécifiques, aux mesures de la rapidité du prononcé d´une décision, de la punitive et de la récidive ».[76] Bien que ces mesure soient fréquemment mentionnées, il faut signaler qu´elles ne représentent pas des indicateurs directs de la qualité de la justice et peuvent être fortement influencées par des différences dans les mécanismes du système de justice pénale, comme l´application de règles de dénombrement des suspects, les seuils appliqués lors de l´enregistrement des cas, ou la participation des procureurs lors de l´étape d´enquête initiale.

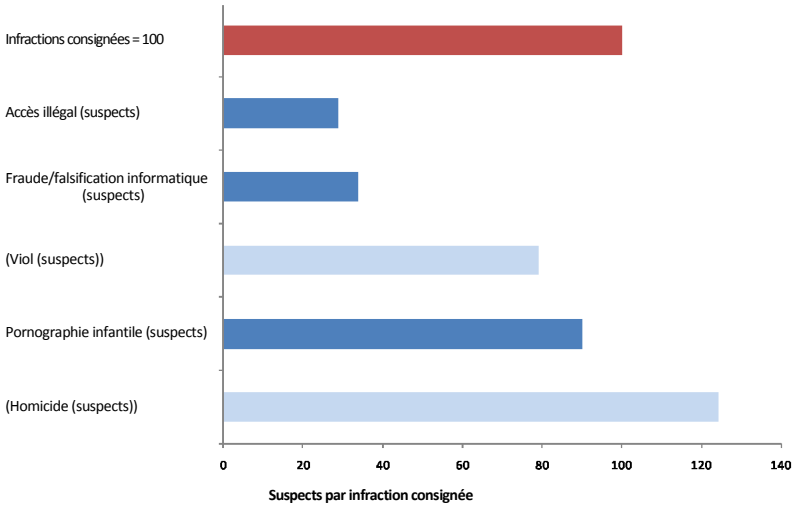
Néanmoins, afin d´obtenir une meilleure compréhension de la riposte du système de justice pénale à la cybercriminalité, le questionnaire de l´étude a demandé aux pays de fournir les statistiques disponibles sur le nombre d´infractions de cybercriminalité enregistrées et le nombre de personnes soupçonnées (ou « présentées officiellement devant la police ») d´avoir commis des infractions de cybercriminalité, ainsi que le nombre de personnes poursuivies et condamnées pour des cyberdélits.[77] Comme le mentionne le chapitre deux (la perspective d´ensemble), les statistiques présentées par la police ne représentent pas une base solide pour une mesure comparative transnationale des tendances de la cybercriminalité.[78] Les statistiques de la justice pénale et des services répressifs au sein de chaque pays, peuvent toutefois permettre de calculer le nombre de cas, de suspects et le taux d´attrition de chaque pays et lorsque le nombre de cas signalés est important, avec des effets d´une année à l´autre (quand les cas sont reportés d´une année sur l´autre), cela peut les justifier

69 *Ibid.*
70 Questionnaire de l´étude sur la cybercriminalitéQ141.
71 *Ibid.*
72 Questionnaire de l´étude sur la cybercriminalitéQ142.

73 Questionnaire de l´étude sur la cybercriminalitéQ183.
74 *Ibid.*
75 Albanese, J.S., 2012. *Justice pénale.* 5ème ed. Upper Saddle River : Prentice Hall.
76 Voir, par exemple, Harrendorf, S., Smit, P., 2010. Attributs des systèmes de justice pénale– ressources, performance et punitivité. *Dans :* Institut européen pour la prévention et la lutte contre la criminalité affilié aux Nations Unies (HEUNI). 2010. *Statistiques internationales sur la justice et la criminalité.* Helsinki.
77 Questionnaire de l´étude sur la cybercriminalitéQ54-70, Q121-137, et Q165-181.
78 voir le chapitre deux (la perspective d´ensemble), la Section 2.1 Mesurer la cybercriminalité, et la Section 2.3 les auteurs de cyberdélits, les profils typiques des délinquants

En général, les pays répondants pouvaient fournir assez peu de statistiques relatives aux tribunaux, à la justice pénale et aux services répressifs. Pour un ensemble de six pays, essentiellement en Europe, il a cependant été possible de calculer le nombre moyens de personnes présentées officiellement devant les services répressifs pour des actes de cybercriminalité, comme l´accès illégal, la falsification et la fraude informatiques, et des délits de pornographie infantile.

Figure 6.6 : personnes présentées officiellement devant la police par infraction consignée (6 pays)

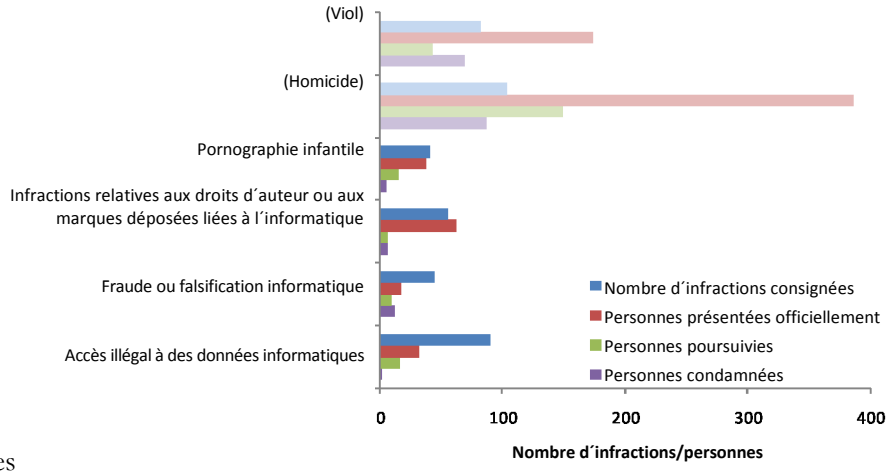


Source : questionnaire de l´étude sur la cybercriminalité Q54-70.

La figure 6.6 montre ces résultats, ainsi que les rapports entre le nombre de suspects et le nombre de délits de viol et d´homicide, dans les mêmes six pays.[79] Il existe une différence significative entre les délits de pornographie infantile et les autres infractions informatiques d´accès illégal et de fraude ou de falsification. Le ratio entre les suspects et les délits de pornographie infantile est similaire à celui des délits « classiques ». Le ratio relatif à l´accès illégal et la falsification ou la fraude informatique est significativement inférieur – il représente environ 25 suspects enregistrés pour 100 infractions.

Ceci pourrait indiquer de nombreux facteurs, y compris des différences des capacités d´enquête de la police pour les différents cyberdélits, des différences dans les axes d´enquête de la police et des variations sur le moment où différents actes de cybercriminalité sont enregistrés comme des infractions à des fins statistiques. Le patron peut néanmoins révéler les véritables différences sous-jacentes des capacités des délinquants, ainsi que des mesures qu´ils ont prises pour dissimuler leurs activitéscriminelles et pour éviter d´être détectés lors des enquêtes menées par les services répressifs.

Figure 6.7 : répartition du système de justice pénale dans les cas de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité Q54-70.

79Questionnaire de l´étude sur la cybercriminalité Q54-70 ; et l´enquête des Nations Unies sur les tendances de la criminalité et le fonctionnement des sy

Bien que les ratios d´infractions et de suspects puissent être calculés comme une moyenne pour de nombreux pays, un seul pays a fourni suffisamment de statistiques pour le questionnaire de l´étude, pour calculer un taux d´attrition des infractions et des condamnations. La figure 6.7 montre le nombre d´infractions enregistrées par la police, les personnes formellement présentées, les personnes poursuivies et les condamnées pour quatre actes de cybercriminalité dans un pays d´Europe de l´est, ainsi que les données équivalentes pour les délits « classiques » de viol et d´homicide. Les données confirment qu´il y a un nombre plus élevé de suspects par infraction enregistrée pour le délit de pornographie infantile que pour d´autres actes de cybercriminalité. Ce patron est similaire pour d´autres infractions liées au contenu – par exemple, pour les infractions relatives aux droits d´auteurs ou aux marques déposées. Cependant, toutes les infractions de cybercriminalité montrent des taux de personnes poursuivies ou condamnées beaucoup moins élevés que dans le cas des délits conventionnels. Dans le cas du pays déclarant, les condamnations pour des cyberdélits représentent en moyenne, 10 % des infractions enregistrées par la police et environ 80 % pour les délits de viol et d´homicide.

Le patron démontre que les nombreuses difficultés en matière de poursuites des cyberdélits mentionnées par les pays répondants sont confirmées par des taux de condamnations plus faibles pour les infractions de cybercriminalité – du moins pour ce pays. Comme le mentionne la prochaine section de ce chapitre, dans plusieurs pays en développement, la poursuite des infractions de cybercriminalité fait face non seulement aux difficultés représentées par la collecte des preuves transnationales et l´obfuscation utilisée par les délinquants, mais aussi aux limitations en matière de spécialisation et de capacités du parquet et dans le domaine judiciaire.

6.4 Capacité de la justice pénale

PRINCIPAUX RÉSULTATS :

- les niveaux de spécialisation des procureurs en matière de cybercriminalité sont inférieurs à ceux des services répressifs. Environ 60 % de tous les pays répondants ont mis en place des structures spécialisées de poursuites pour la cybercriminalité ;
- les procureurs des pays développés ont des niveaux de spécialisations supérieurs à ceux des pays en développement ;
- plus de 60 % des pays les moins développés ont déclaré que les procureurs spécialisés ont des compétences basiques ou aucune compétence de TI et un équipement informatique moyennement ou pas du tout sophistiqué ;
- les tribunaux ont des niveaux minimes de spécialisation et seulement 10 % des pays mentionnent des services judiciaires spécialisés. La majorité des cas sont traités par des juges non spécialisés qui ne reçoivent aucune formation en matière de cybercriminalité dans 40 % des pays répondants.

Si les enquêtes sur la cybercriminalité ou liées à des preuves électroniques requièrent la spécialisation des services répressifs, il en est de même pour le système de justice pénale pour poursuivre et condamner les cyberdélits. Cette spécialisation implique que le personnel comprenne les concepts d´informatique et d´internet, aient des connaissances en matière de cadres juridiques pour la cybercriminalité et soit capable de présenter et de comprendre des preuves électroniques au tribunal.

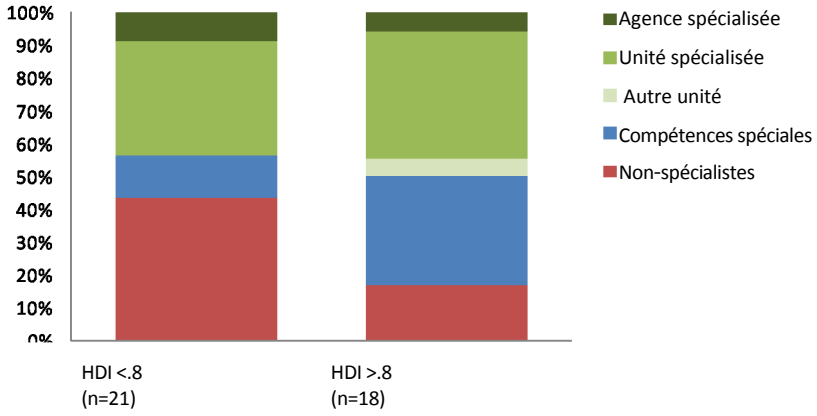
Cette section présente les informations fournies par les pays concernant la capacité des procureurs et des tribunaux de poursuivre et de condamner des cyberdélits. Comme mentionné au chapitre cinq (application des lois et enquêtes), la capacité institutionnelle comprend de nombreux éléments qui incluent les capacités stratégiques et opérationnelles, les compétences techniques du personnel, des effectifs et des ressources suffisantes ; ainsi que le niveau de spécialisation. La constatation faite au chapitre cinq, concernant la nécessité croissante pour tous les officiers des services répressifs de gérer et de collecter des preuves électroniques de manière routinière, est également applicable aux procureurs et aux juges. Avec la progression du monde numérique, il pourra être difficile de concevoir la condamnation d´une infraction sans présenter et tenir compte des preuves électroniques.

Spécialisation organisationnelle

Les réponses des pays au questionnaire de l´étude montrent que le degré de spécialisation organisationnelle en matière de cybercriminalité des autorités chargées des poursuites est significativement inférieur à celui des services répressifs. Alors que plus de 90 % des pays ont mentionné un certain niveau de spécialisation des services répressifs en matière de cybercriminalité, cette proportion tombe à environ 60 % dans le cas des autorités chargées des poursuites, dans tous les pays répondants.[80] Ces chiffres dissimulent toutefois des différences significatives aux niveaux de développement des pays.

Presque 80 % des pays les plus développés mentionnent un type de spécialisation des autorités chargées des poursuites en matière de cybercriminalité. Environ la moitié de ces pays a une unité spécialisée et l´autre moitié dispose d´une agence spécialisée, d´une autre unité spécialisée (par exemple pour la criminalité organisée), ou de personnel spécialisé qui ne fait pas partie d´une unité séparée. Par contre, moins de 60 % des pays moins développés mentionnent une spécialisation en matière de cybercriminalité des autorités chargées des poursuites.

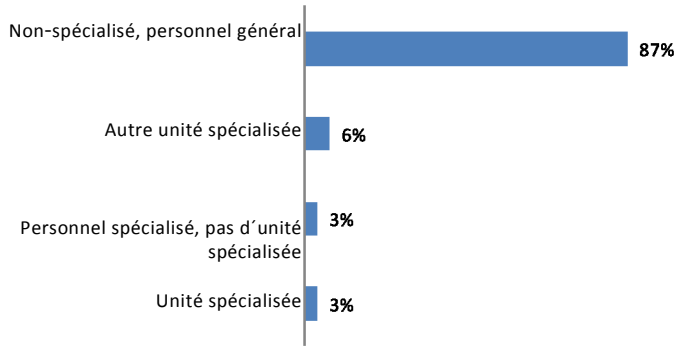
Figure 6.8 : structure des organismes chargés des poursuites pour prévenir et lutter contre la cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalitéQ157.

Dans la plupart de ces pays, la spécialisation concerne l´unité spécialisée. Dans le cas des pays développés qui mentionnent une spécialisation organisationnelle, plusieurs ont indiqué qu´il existait une unité ou une division spécialisée au niveau fédéral, provincial de l´état au ministère de la justice ou dans les organes nationaux chargés des poursuites, qui souvent surveille, coordonne ou appuie les unités générales ou spécialisées des bureaux locaux et sur le terrain. Certains pays ont aussi mentionné un appui technique et en matière d´enquête apporté par « *une équipe spécialisée d´enquêteurs de police, d´ingénieurs informatiques et de procureurs qui enquêtent et poursuivent la cybercriminalité* ».[81]

Figure 6.9 : structure des tribunaux pour les cas de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité. Q186. (n=31)

80 Questionnaire de l´étude sur la cybercriminalité Q157.
81 Questionnaire de l´étude sur la cybercriminalité. Q157.
82 *Ibid.*

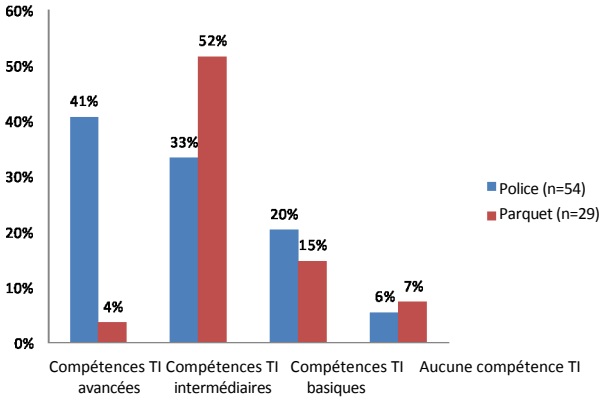
Dans certains cas, les bureaux individuels chargés des poursuites ont des compétences spéciales pour traiter d´importants ensembles de procédures liées aux délits relatifs à l´information et la communication et à la cybercriminalité proprement dite ». Un autre pays développé a déclaré que : « *il existe des variations, mais un petit nombre de bureaux locaux ont des équipes spécialisées en exploitation infantile sur internet* ».[82] Dans les pays les moins développés, les arrangements sont souvent moins établis. Un pays d´Afrique a signalé qu´une unité récemment établie était chargée des poursuites « *ainsi que des orientations en matière de politiques et de législation ; elle fournit une assistance technique à d´autres procureurs et aux services répressifs, mais les besoins de la nouvelle unité en matière d´équipement et de formation ne sont pas encore satisfaits* ».[83] Certains pays mentionnent « *beaucoup d´améliorations à faire* ». Un pays d´Afrique a signalé *« il n´y a pas de procureurs spécialement assignés aux affaires de cybercriminalité. Tous les procureurs sont appelés à traiter des affaires de cybercriminalité même s´ils n´ont pas reçu de formation* ».[84]

Quelques pays qui n´ont pas de structures de poursuites spécialisées ont mentionné leur intention d´établir une nouvelle structure de poursuites pour la cybercriminalité. Ces projets incluaient « *la création de nombreuses unités spécialisées* » et « *la création de groupes de travail dans les villes principales qui n´ont actuellement aucune structure spécialisée de poursuite* ».[85] Un pays d´Europe envisageait de créer « *des unités indépendantes dans les bureaux des procureurs qui ont un grand volume d´activités et, dans les autres bureaux, de mélanger des procureurs spécialisés en cybercriminalité avec d´autres types d´unités spécialisées* »[86]. D´autres pays n´envisagent pas de créer des unités spécialisées, bien que certains d´entre eux aient mentionné qu´ils comptaient intégrer des spécialistes en cybercriminalité dans les structures de poursuites existantes.

Les structures des tribunaux révèlent un niveau moindre de spécialisation et environ 10 % de tous les pays répondants ont mentionné un certain niveau de spécialisation des tribunaux en matière de cybercriminalité. Seulement trois % de tous les pays répondants ont mentionné une unité judiciaire spécialisée en cybercriminalité. Six % des pays ont mentionné un autre type d´unité judiciaire spécialisée, comme les tribunaux pour les délits commerciaux. Trois % ont signalé la surveillance judiciaire des affaires de cybercriminalité exercée par le personnel judiciaire spécialisé.

Quelques pays ont déclaré qu´il y avait actuellement des projets en cours, avec des mesures législatives ou administratives, pour créer des tribunaux spécialisés en cybercriminalité. Cependant, les pays répondants considéraient que « *cela n´exige généralement pas des tribunaux spécialisés basés sur ces thèmes, bien que, dans la pratique, certains juges se spécialisent dans des affaires pénales et les juges en chef tendent à leur assigner ces cas* ».[87]

Figure 6.10 : capacités techniques de la police et des procureurs



Source : questionnaire de l´´étude sur la cybercriminalitéQ116 et Q160. (n=54, 29)

Spécialisation du personnel

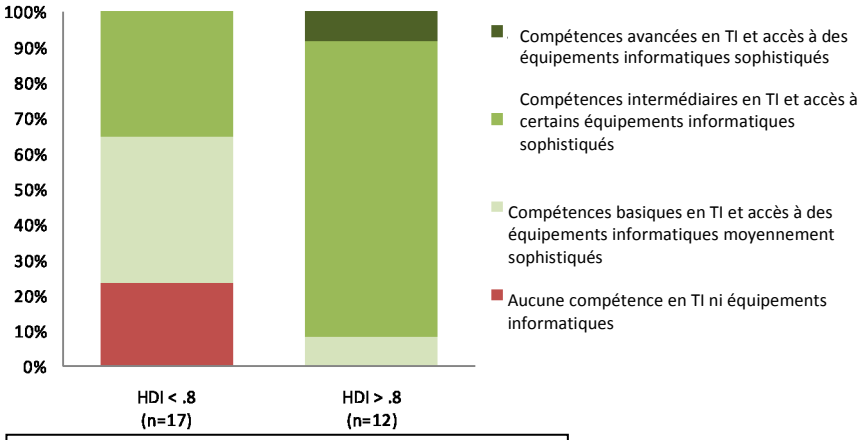
Les structures de poursuites montrent une spécialisation organisationnelle en matière de cybercriminalité moindre que celle desservices répressifs et les pays mentionnent également des niveaux plus faibles de compétences techniques des procureurs que des officiers des services répressifs. La figure 6.10 montre les réponses des pays concernant les compétences en TI des organes chargés des poursuites et des services répressifs.[88]

Le fait que très peu de procureurs s´occupant de cyberdélits aient des compétences avancées en TI par rapport aux officiers des services répressifs, peut partiellement s´expliquer par leurs rôles fonctionnels. Même si l´implication des procureurs dans les enquêtes varie en fonction des systèmes juridiques, les officiers des services répressifs sont généralement amenés plus souvent à mener ou superviser les enquêtes criminalistiques initiales et à collecter des preuves électroniques.

---

83 *Ibid.*
84 Questionnaire de l´étude sur la cybercriminalité. Q160.
85 Questionnaire de l´étude sur la cybercriminalité. Q157.
86 *Ibid.*
87 Questionnaire de l´étude sur la cybercriminalité. Q187.
88 Questionnaire de l´étude sur la cybercriminalité. Q116 et Q160.

Figure 6.11 : compétences techniques des procureurs



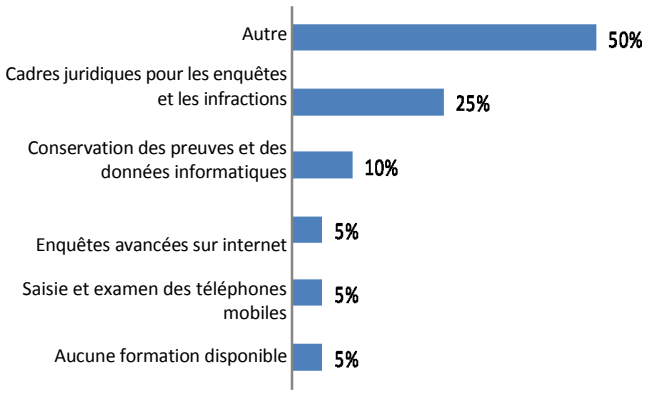
Source : questionnaire de l'étude sur la cybercriminalité Q160. (n=29

Les compétences techniques des procureurs varient significativement selon le niveau de développement du pays. Les pays les plus développés ont signalé qu´environ 80 pour cent des procureurs ont des niveaux de compétences intermédiaires en TI et ont accès à un équipement sophistiqué et huit pour cent ont des compétences avancées en TI. Aucun pays développé n´a indiqué que ses procureurs n´ont pas de compétences en TI ou d´équipement informatique. Par contre, plus de 60 pour cent des pays les moins développés ont déclaré que leurs procureurs n´ont pas de compétences en TI ou ont des compétences et ont accès à des équipements informatiques moyennement sophistiqués ou à aucun équipement. Ces résultats indiquent des manques en matière de capacité. Un pays en développement a déclaré que l´équipement informatique nécessaire est « *disponible sur demande* »[89] et presque tous les pays ont déclaré qu´ils faisaient face à des difficultés en matière de formation et d´équipement et que la « *formation technique est insuffisante* » et plus *« d´appui dans le domaine de la formation est nécessaire pour améliorer les résultats»...*[90] Un pays développé a signalé que l*es procureurs ont des compétences avancées et intermédiaires en TI mais n´ont pas accès à des équipements informatiques sophistiqués ou même moyennement sophistiqués*'.'[91]

Développement du personnel

La moitié des pays répondants a indiqué que la formation pour les procureurs spécialisés aborde une gamme de thèmes. Outre les thèmes mentionnés dans la figure 6.12, sont aussi inclus des thèmes concernant « *le fonctionnement d´internet, les types de cyberdélits et les enquêtes et la jurisprudence*, »[92] la sécurité des informations et la « *conservation des preuves électroniques concernant des infractions de blanchiment de capitaux* ». Un pays a déclaré que « *parfois les procureurs participent aux formations que les organisations policières fournissent à leurs propres experts »*[93]

Figure 6.12 : thèmes de formation pour les procureurs spécialisés



Source : questionnaire de l´étude sur la cybercriminalitéQ161. (n=20)

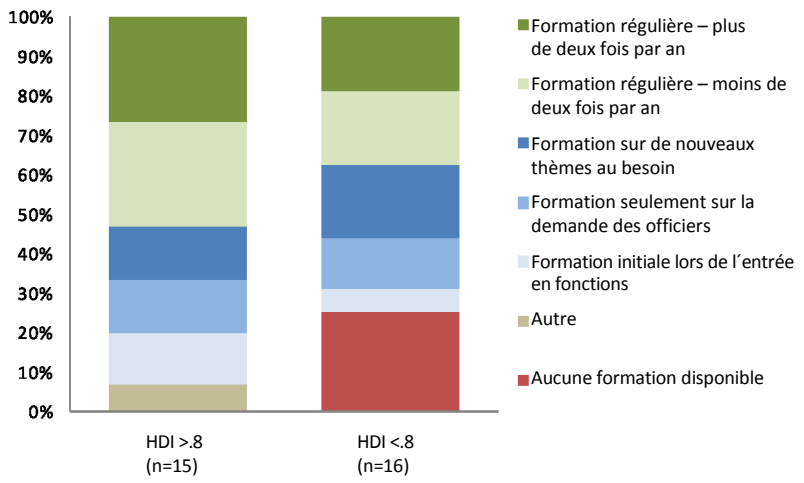
89 Questionnaire de l´étude sur la cybercriminalité Q160
90 Ibid
91 Ibid

92 Questionnaire de l´étude sur la cybercriminalité. Q161

Les thèmes de formation pour les procureurs spécialisés ne sont pas aussi variés que pour le personnel des services répressifs et cela est probablement dû aux différents rôles qu´ils jouent dans le processus de justice pénale. Plusieurs pays en développement ont souligné le besoin de fournir plus de formation technique aux procureurs. Un pays a, par exemple, déclaré que la « *préparation en droit pénal est de grande qualité mais la formation technique est insuffisante* »[94] et un autre pays a indiqué que « *plus d´appui en matière de formation est nécessaire afin d´améliorer les résultats* ».[95] D´autres pays ont souligné qu´ils « *nécessitaient plus de formation dans des domaines tels que la technologie de l´information* ».[96]

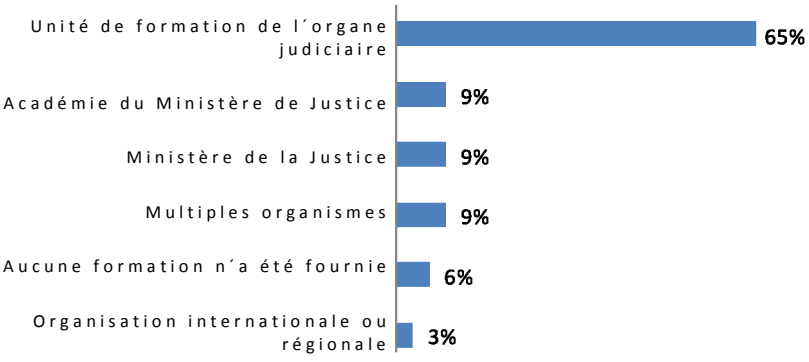
Les réponses des pays présentaient aussi des variations importantes dans la fréquence et la durée de la formation pour les procureurs spécialisés. Plus de 40 % des pays répondants signalèrent que les procureurs recevaient régulièrement une formation et un peu de plus de 20 % dirent que la formation était fournie plus de deux fois par an. Comme dans le cas de la spécialisation organisationnelle et des compétences techniques, ces différences sont aussi associées au niveau de développement des pays. Un quart des procureurs spécialisés des pays les moins développés n´ont pas accès à une formation spécialisée et environ 40 % reçoivent régulièrement une formation. En revanche, aucun des pays de la cohorte des pays les plus développés, n´a déclaré ne pas avoir de formation disponible et plus de la moitié de ces pays a déclaré que leurs procureurs spécialisés recevaient régulièrement des formations plus d´une fois par an. Plusieurs pays développés ont également fourni des détails sur des aspects liés à la fréquence des formations comme « *des programmes de formation interdisciplinaires annuels*, » « *des modules d´apprentissage en ligne*, » « *des participations aux conférences* » et « *des formations mensuelles sur des thèmes spécialisés impartis, par des experts internes et externes* ».[97]

Figure 6.13 : fréquence de la formation pour les procureurs spécialisés



Source : questionnaire de l´étude sur la cybercriminalité Q162. (n=31)

Figure 6.14 : fournisseurs de formation pour les procureurs spécialisés

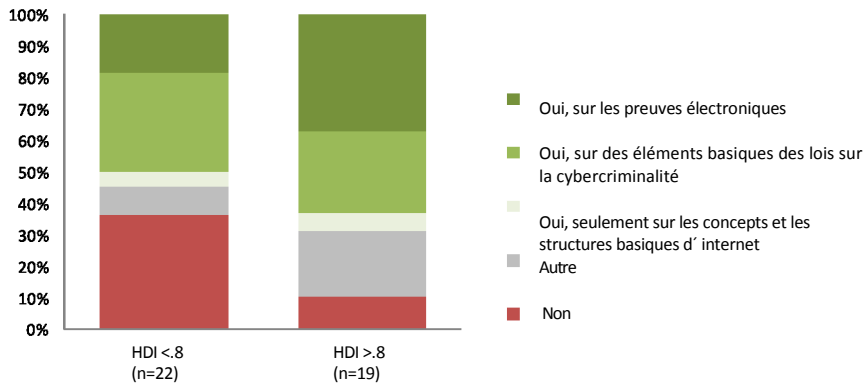


Source : questionnaire de l´étude sur la cybercriminalité. Q163. (n=34)

94 Questionnaire de l´étude sur la cybercriminalité. Q160.
95 *Ibid.*
96 *Ibid.*
97 Questionnaire de l´étude sur la cybercriminalité. Q162.

Le prestataire de formation pour les procureurs spécialisés le plus souvent mentionné a été l´unité de formation de l´organe de poursuites. L´académie judiciaire et celle du ministère de la justice, ainsi que de multiples agences, constituent environ 10 % des fournisseurs de formation pour les procureurs spécialisés. Il a été signalé qu´une très faible proportion – trois % – de procureurs spécialisés avaient été formés par des organisations régionales ou internationales. Six % des pays ont déclaré que le personnel chargé des poursuites n´avait reçu aucune formation spécialisée.

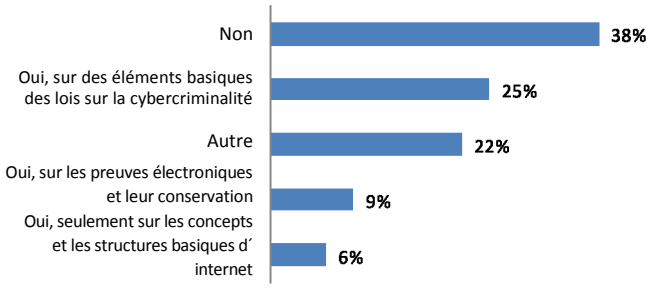
Figure 6.15 : formation pour les procureurs non spécialisés



Source : questionnaire de l´étude sur la cybercriminalité Q164. (n=41)

De nombreux pays répondants ont reconnu l´importance de fournir également une formation en matière de cybercriminalité aux procureurs non spécialisés. Un pays a, par exemple, déclaré que « *Durant ces dernières années nous avons développé plusieurs activités en vue de transmettre à tous les procureurs les connaissances adéquates en matière de cybercriminalité, afin qu´ils acquièrent les meilleures compétences liées aux nouvelles technologies* ».[98] Un autre pays a souligné qu´une formation plus ample était « *destinée non seulement à enrichir les connaissances relatives à la doctrine juridique de ces délits mais visait également à attirer l´attention sur l´importance d´adapter les concepts classiques de procédure aux nouvelles technologies et aux possibilités criminalistiques* ».[99] En général, environ 60 % des pays ont signalé l´existence de formation en cybercriminalité pour les procureurs non spécialisés. La figure 6.15 montre toutefois des différences liées au niveau de développement des pays car environ 40 % des pays les moins développés ont déclaré que les procureurs non spécialisés ne recevaient aucune formation en matière de cybercriminalité. Pour ce qui concerne la magistrature, environ 40 % de tous les pays répondants ont déclaré qu´il n´y avait aucune formation spécifique sur la cybercriminalité pour les juges. Un quart des pays répondants mentionnèrent une formation sur les éléments basiques des lois sur la cybercriminalité. Les réponses de plusieurs furent similaires à celles de ce pays d´Europe du nord qui commenta que : « *étant donné qu´il n´y a pas de juges spécialisés, la formation est couverte par des programmes de formation continue organisés par la magistrature et ouverts à tous les magistrats. Ils sont organisés annuellement et durent généralement deux jours. Ce type de formation a un caractère général, et c´est une introduction à la cybercriminalité* ».[100] Un pays a déclaré que la formation judiciaire « *visait à couvrir des cas basés sur la législation nationale relative à la cybercriminalité, ainsi que des résumés des affaires récentes* ».[101] Les pays ont en général souligné qu´il existe un besoin significatif en matière de formation judiciaire sur « *les lois sur les cyberdélits, la collecte des preuves et les connaissances informatiques basiques et avancées* ».[102]

Figure 6.16 : formation sur les enquêtes des cyberdélits pour les juges non spécialisés



Source : questionnaire de l´étude sur la cybercriminalité Q192.

98 Questionnaire de l´étude sur la cybercriminalité. Q164
99 *Ibid.*
100 Questionnaire de l´étude sur la cybercriminalité. Q189.
101 *Ibid.*
102 *Ibid.*

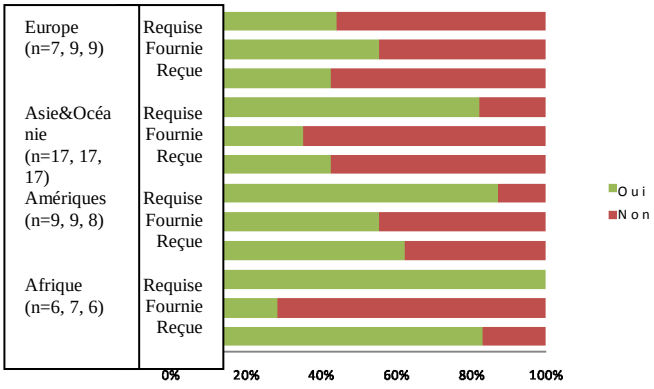
Il a été signalé que cette formation est actuellement impartie par des centres et des commissions de formation judiciaire, des unités de formation judiciaire et des tribunaux et des ministères ou des organismes de justice. Plusieurs pays ont déclaré que les juges peuvent « *choisir volontairement de participer à des programmes de développement professionnel. Le contenu des programmes varie et il n´y a pas de matériel de formation prescrit pour les juges ou les magistrats impliqués dans des affaires de cybercriminalité* ».[103]

6.5 Le renforcement des capacités et l´ assistance technique

PRINCIPAUX RÉSULTATS :

- 75 % des pays répondants de toutes les régions du monde, ont déclaré requérir une assistance technique en matière de cybercriminalité ;
- l´assistance technique a été fournie jusqu´à présent essentiellement dans le domaine des enquêtes générales sur les cyberdélits, les preuves électroniques et la criminalistique informatique. Les besoins signalés suggèrent qu´il existe une nécessité d´assistance dans le domaine des poursuites et de la coopération internationale et notamment l´appui aux procès ;
- diverses institutions gouvernementales ont déclaré avoir besoin d´une assistance technique, et ont souligné la nécessité d´une approche holistique et multidisciplinaire à l´assistance technique en matière de cybercriminalité ;
- la prédominance des activités d´assistance technique durant moins d´un mois indique un besoin évident d´un investissement durable à plus long terme.

Parallèlement aux questions sur la capacité des services répressifs, des autorités chargées des poursuites et des tribunaux de prévenir et de lutter contre la cybercriminalité, le questionnaire de l´étude inclut aussi des questions sur les besoins et l´octroi d´assistance technique, par pays.



Source : questionnaire de l´étude sur la cybercriminalité Q241, Q253, Q250 (n=40, 42, 39)

Globalement, 75 % des pays répondants de toutes les régions du monde, ont déclaré nécessiter une assistance technique dans des domaines liés à la cybercriminalité. Chaque pays d´Afrique qui a répondu au questionnaire a déclaré avoir besoin d´assistance technique.

Plus de 70 % de tous les pays répondants ont déclaré avoir fourni une forme quelconque d´assistance technique à d´autres pays, bien que moins de 20 % des pays aient déclaré avoir reçu une assistance technique. Ceci pourrait indiquer qu´un grand nombre de pays qui ont fourni une assistance se sont concentrés sur un petit nombre de pays, ou bien qu´une importante proportion des pays les moins développés dans le monde n´a pas répondu au questionnaire de l´étude.

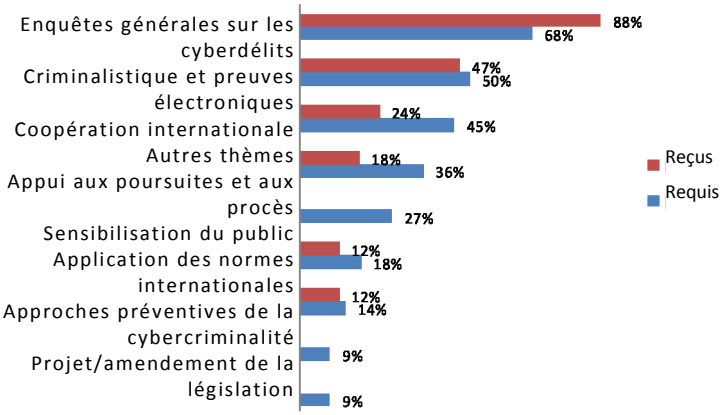
Dans le cas des pays européens, un peu plus de la moitié a déclaré avoir reçu une assistance technique et moins de la moitié a déclaré avoir besoin ou avoir fourni une assistance technique en matière de cybercriminalité. En Asie, en Océanie et en Amérique, plus de 80 % des pays ont déclaré avoir demandé une assistance technique.

103 Questionnaire de l´étude sur la cybercriminalitéQ192.

Une majorité de pays d´Asie et d´Océanie a signalé avoir fourni une assistance technique et un peu moins de la moitié ont reçu une assistance technique. En Amérique, moins de la moitié ont fourni une assistance technique et plus d´un tiers ont reçu une forme quelconque d´assistance technique.

Les thèmes - « les enquêtes générales sur la cybercriminalité » ont été le domaine le plus souvent mentionné pour ce qui concerne l´assistance technique requise et reçue, et le seul domaine pour lequel l´assistance technique a été reçue plus souvent qu´elle n´a été requise. Ceci peut indiquer que l´assistance technique en matière de cybercriminalité pourrait aller au-delà d´une approche traditionnelle sur les enquêtes des services répressifs et inclure une gamme plus vaste de domaines. Notamment, les domaines de la « coopération internationale » et de « l´appui aux poursuites et au procès », qui représentent des points pour lesquels l´assistance a été requise, mais qui a été reçue dans une faible proportion. Une entité des Nations Unies a signalé que les « *Gouvernements requièrent davantage d´assistance dans ces domaines* ».[104]

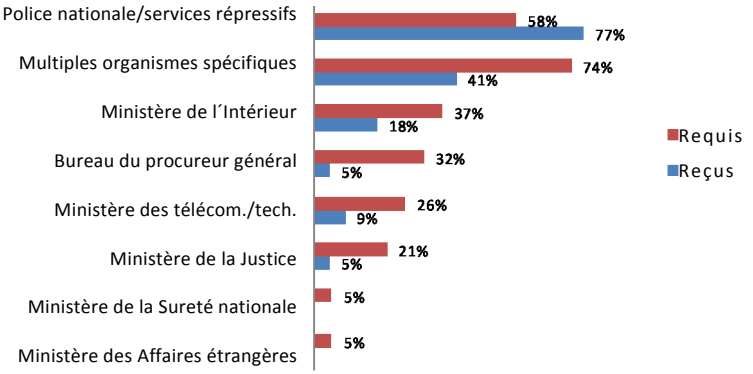
Figure 6.18 : thèmes d´assistance technique requis et reçus



Source : questionnaire de l´étude sur la cybercriminalité Q243 et Q251. (n=17, r=36; n=22, r=61)

Institutions – une vaste gamme d´organismes gouvernementaux requièrent et reçoivent une assistance technique – et ceci met l´accent sur l´importance d´une riposte holistique et multidisciplinaire à la cybercriminalité. La police nationale et les services répressifs signalent avoir reçu une assistance technique plus fréquemment qu´ils ne l´ont requise. Ceci peut indiquer la mesure dans laquelle l'accent a été mis surle renforcement des capacités des services répressifs, qui sont les intervenants de première ligne face à la cybercriminalité. Le niveau plus élevé d´assistance technique fournie aux services répressifs qui a été signalé pourrait aussi correspondre à des niveaux plus élevés de spécialisation organisationnelle et du personnel des services répressifs par rapport à d´autres organismes de justice pénale (voir le chapitre cinq (application des lois et enquêtes). La figure 6.19 montre aussi le niveau relativement limité d´assistance technique reçue par des institutions, telles que les tribunaux et les bureaux des procureurs, et cela confirme le panorama thématique de la figure 6.18.

Figure 6.19 : organismes qui requièrent et reçoivent une assistance technique

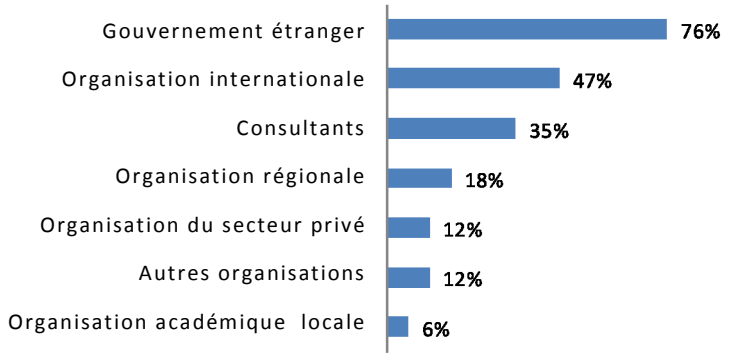


Source : questionnaire de l´étude sur la cybercriminalité Q244 et Q252. (n=22, r=34 ; n=19, r=49)

104 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q20.

Prestataires – on a signalé que les gouvernements étaient les institutions qui fournissaient le plus fréquemment une assistance technique (plus de 75 %), suivis par les organisations internationales et les consultants internationaux. Les organisations régionales comme l´Union africaine, l´Organisation des états américains et le Conseil de l´Europe, ont été mentionnées comme des fournisseurs d´assistance technique par 20 % des pays répondants. Il faut toutefois signaler que les structures « prestataires » d´assistance technique peuvent comporter de multiples modalités. L´impartition d´un programme ou d´un projet déterminé d´assistance technique, peut, par exemple, être mise en place par le biais de partenariats entre les gouvernements, les organisations régionales ou internationales, les consultants indépendants et les organisations académiques. Les organisations internationales du secteur privé – avec lesquelles ces partenariats existent déjà souvent – ont notamment été mentionnées comme étant des fournisseurs d´assistance technique par environ 10 % des pays répondants et cela met l´accent sur l´importance des organisations du secteur privé qui sont des partenaires essentiels dans ce domaine.

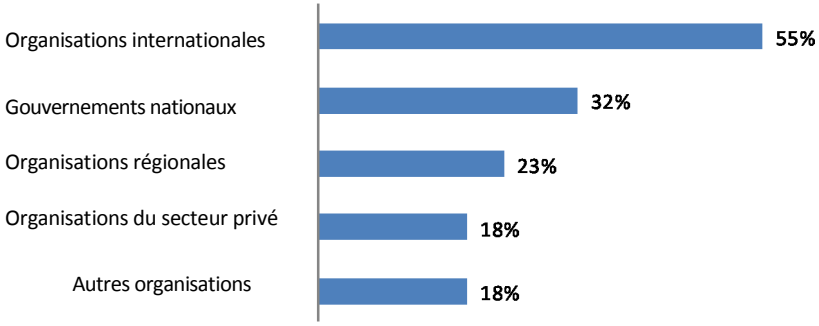
Figure 6.20 : institutions qui fournissent une assistance technique



Source : questionnaire de l´étude sur la cybercriminalité Q247. (n=17, r=35)

Les réponses fournies au questionnaire de l´étude par les organisations intergouvernementales soulignaient le rôle de ces organisations dans la fourniture d´assistance technique. Les organisations apportent une assistance technique pour une gamme de thèmes qui comprennent les techniques d´enquêtes générales, la conservation des preuves et la criminalistique, le développement des législations, la coopération public-privé et les actions internationales normatives et la sensibilisation. De nombreuses entités des Nations Unies ont souligné l´importance d´une « *approche holistique et à plusieurs niveaux* » de l´assistance technique .[105]

Figure 6.21 : organisation qui appuie l´assistance technique reçue



Source : questionnaire de l´étude sur la cybercriminalité Q245. (n=22, r=32)

Plusieurs pays ont déclaré qu´il était important de renforcer la capacité de partenariat par le biais de « *réseaux d´institutions de formation judiciaire* »[106] et en utilisant une approche de « *formation des formateurs* » *pour les enquêteurs/examinateurs de TI.*[107] Une organisation a, par exemple, mentionné qu´il était important que « *toutes les informations et le matériel* » puissent être utilisés par les « *participants pour qu´ils fournissent la même formation dans leur propre pays* ».[108]

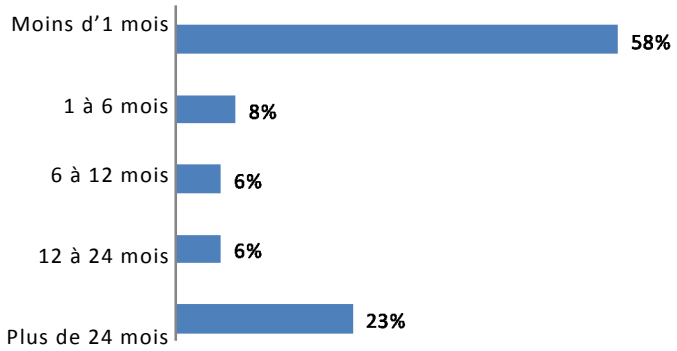
105 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q52.
106 *Ibid.*
107 *Ibid.*
108 *Ibid.*

Selon l´orientation du programme, l´audience visée va des individus, comme les officiers des services répressifs et les enquêteurs criminalistiques, aux institutions telles que les ministères de l´intérieur, de la justice et de la communication. Les organisations internationales ont fourni une formation dans chaque région ; la plupart a signalé que les programmes de formation étaient continus et qu´il y avait une forte demande, même si elles étaient parfois limitées par la disponibilité des ressources.

De nombreuses organisations intergouvernementales ont abordé l´importante question des *normes* et de la *certification*. Une organisation a mentionné l´utilisation d´une formation criminalistique « *reconnue par l´Université... impartie en 3 segments ; un cours de niveau basique en 2010, des cours avancés en 2011, avec une maîtrise en ligne prévue pour 2012* ».[109] Une entité des Nations Unies a mentionné la difficulté d´identifier et de connaître les normes professionnelles qui devraient être suivies et promues lors de l´impartition de la formation. La même entité a, par exemple, déclaré que « *il n´y a pas encore de consensus sur les exigences du cursus de criminalistique* ».[110] D´autres entités des Nations Unies ont mentionné la difficulté causée par le manque de ressources et de sensibilisation en matière de cybercriminalité, qui inhibent la fourniture d´assistance technique. Une entité des Nations Unies a indiqué que « *nous avons l´expertise mais nous n´avons pas les ressources pour lutter contre la cybercriminalité* ».[111]

L´appui pour l´assistance technique provient d´un nombre relativement restreint de gouvernements nationaux, internationaux et régionaux, et d´organisations du secteur privé. Les principales sources d´appui en matière d´assistance technique sont les organisations internationales et une majorité de pays (55 %) a déclaré qu´une forme quelconque d´assistance technique en provenait. Une entité des Nations Unies a signalé l´importance de la « *formation fournie par des organisations expérimentées de la région* ».[112]. Les gouvernements nationaux ont été mentionnés comme des prestataires ou des appuis pour la fourniture d´assistance technique par environ un tiers des pays répondants et les organisations régionales représentaient presque un quart des appuis en matière d´assistance technique. Les organisations du secteur privé et d´autres types d´organisations furent mentionnées comme des prestataires ou des sponsors en matière d´assistance technique, par presque 20 % des pays répondants.

Figure 6.22 : durée de l´ assistance technique reçue



Source : questionnaire de l´étude sur la cybercriminalité Q246. (n=24, r=52)

Durée – presque 60 % des programmes d´assistance technique mentionnés durèrent moins d´un mois. Seulement un quart avait une durée supérieure à deux ans. Si les besoins d´assistance technique liés à la cybercriminalité peuvent être à court, moyen ou long terme, la prédominance des activités d´assistance technique à court terme indique un besoin évident d´un investissement durable à plus long terme, axé sur le renforcement de la capacité structurelle de diverses autorités gouvernementales et des intervenants impliqués dans la riposte à la cybercriminalité.

109 *Ibid.*
110 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q51.
111 *Ibid.*
112 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q52

Page intentionnellement laissée vierge

CHAPITRE SEPT : COOPÉRATION INTERNATIONALE

Ce chapitre examine les ripostes formelles et informelles de la coopération internationale au défi transnational représenté par la cybercriminalité. Il constate que le recours généralisé à des mécanismes traditionnels lents, tels que l´entraide judiciaire, l´émergence de groupements de coopération dans les pays et un manque de clarté sur l´accès permissible direct des services répressifs aux données extraterritoriales, représentent des difficultés pour une riposte globale efficace.

7.1 Souveraineté, juridiction et coopération internationale

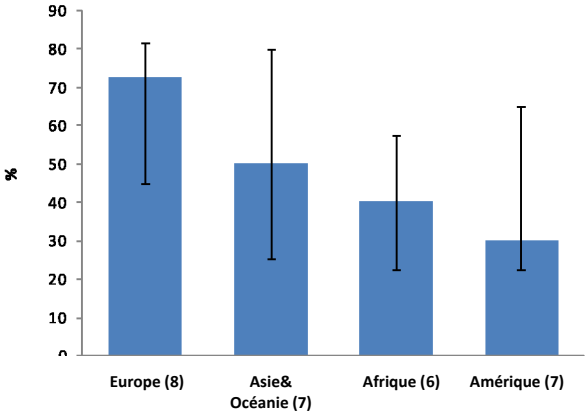
Principaux résultats :

- la dimension transnationale des délits de cybercriminalité surgit lorsqu´un effet ou un élément important du délit se trouve dans un autre territoire, ou si une partie du *modus operandi* du délit a eu lieu dans un autre territoire ;
- les pays qui ont répondu au questionnaire de l´étude signalent qu´entre 30 et 70 % des actes de cybercriminalité impliquent une dimension transnationale ;
- ceci met en jeu des questions d´enquêtes transnationales, de souveraineté, de juridiction, de preuves extraterritoriales et de la nécessité de la coopération internationale.

Les cyberdélits comme des délits transnationaux

La cybercriminalité n´est pas la première forme de criminalité qui requiert une riposte globale. Durant ces dernières décennies, une action globale a été nécessaire pour faire face à des défis tels que le trafic illicite de stupéfiants et la criminalité organisée transnationale, en développant des accords internationaux. Néanmoins, dire que la cybercriminalité actuelle représente des défis uniques en matière de coopération internationale, est devenu un truisme. Lors de la collecte des informations pour l´étude, plus de la moitié des pays a signalé qu´entre 50 et 100 % des actes de cybercriminalité enregistrés par la police comprenaient un « *élément transnational* ».[1] La figure montre que les pays d´Europe percevaient une proportion plus élevée d´actes de cybercriminalité impliquant une dimension transnationale alors que les pays d´Afrique et d´Amérique percevaient une proportion plus faible.[2]

Figure 7.1 : pourcentage des actes de cybercriminalité qui impliquent une dimension transnationale



Source : questionnaire de l´étude sur la cybercriminalitéQ83. (n=28)

1 Questionnaire de l´étude sur la cybercriminalité Q83. Certains pays qui n´ont pas pu fournir de chiffres exacts ont estimé que le pourcentage était « très élevé ».

2 La figure montre les valeurs médianes avec les quartiles supérieurs et inférieurs représentés par des barres d´erreur.

Un pays d´Europe de l´est a signalé que « *environ 80 % des actes de cybercriminalité examinés par les services répressifs nationaux étaient liés à plus d´un pays* ».[3] Un autre pays, d´Afrique de l´ouest, a déclaré que la plupart des victimes visées par les auteurs de cyber délits sur son territoire se trouvait « *hors des frontières nationales* ».[4] D´autres pays signalèrent que la plupart des infractions signalées « *commençaient à l´extérieur* » de leur territoire et d´autres pays déclarèrent que « *la plupart du temps nous agissons en tant qu´intermédiaires* ».[5] Les pays ont noté que l´utilisation de serveurs proxy et l´influence croissante des médias sociaux faisaient partie des facteurs qui entraînaient un nombre croissant de cas avec une dimension transnationale.[6] Un pays a même affirmé que les délinquants étaient pleinement conscients des questions juridictionnelles et utilisaient sciemment des ressources d´internet telles que les serveurs de messagerie localisés à l´étranger pour tenter de dissimuler les preuves de leurs activités illégales.[7] Cependant, cette perception n´est pas uniforme et un pays d´Amérique du sud a signalé qu´un nombre considérable de cas transnationaux signalés étaient « *d´origine nationale* ».[8]

Ce chapitre examine les approches juridictionnelles et de coopération internationale pour lutter contre la cybercriminalité – avec des instruments régionaux et internationaux sur la cybercriminalité, ainsi que les pratiques et les législations des états. Il présente les informations fournies pour le questionnaire de l´étude dans le cadre juridique international de la souveraineté, la juridiction et la coopération internationale en matière pénale.

Le point de départ – la souveraineté et la juridiction

Le point de départ de la coopération internationale et de la juridiction de l´état est la souveraineté. L´égalité souveraine des états est protégée par les règles du droit coutumier international. Ceci inclut l´obligation des états de ne pas *« s´immiscer sous quelque forme, ou quelque la raison que ce soit dans les affaires internes et externes d´autres états ».*[9]

Les questions d´application des lois et de justice pénale relèvent exclusivement du domaine de la souveraineté de l´état– et par conséquent la juridiction pénale a traditionnellement été liée au territoire géographique. Les états doivent donc s´abstenir d´exercer des pressions sur d´autres états pour ce qui concerne la conduite d´organismes nationaux spécifiques tels que les organismes judiciaires ou d´application de la loi .[10] Il ne sera pas possible d´arrêter des personnes, de signifier des notifications et d´engager des enquêtes policières ou fiscales sur le territoire d´un autre état, sauf dans les conditions prévues par un traité ou un accord.[11]

Tous les délits ne sont évidemment pas commis exactement dans la juridiction territoriale. Lorsque c´est le cas, les lois internationales reconnaissent de nombreux fondements de juridiction extraterritoriale en matière pénale.[12] Les fondements communs des lois nationales et des accords internationaux sont résumés dans le tableau ci-dessous.

3 Questionnaire de l´étude sur la cybercriminalité Q83.
4 *Ibid.*
5 *Ibid.*
6 *Ibid.*
7 *Ibid.*
8 *Ibid.*
9 Ainsi les états ont droit à la souveraineté et à l´intégrité territoriale, à librement déterminer leur propre système social, politique, économique et culturel, ainsi que toutes les affaires qui relèvent essentiellement de leur compétence nationale. Voir la Déclaration de l´inadmissibilité de l´intervention dans les affaires intérieures des états, annexe à la résolution GA A/RES/20/2131 (XX), du 21 décembre 1965. Veuillez vous référer à l´affaire *Corfu Channel*, ICJ Rapports 1949, 35, le cas sur les *activités militaires et paramilitaires*, ICJ Rapports 1986, 202, et l´affaire *Nicaragua*, ICJ Rapports 1986, 14, 109-10.
10 Lorsque, par exemple, les ressortissants d´un état sont jugés dans un procès à l´étranger, le principe basique sous-jacent est que l´état ne peut s´immiscer dans les procédures judiciaires d´un autre état souverain au nom de son ressortissant. De même les états ne peuvent pas prendre de mesures sur le territoire d´un autre état en appliquant leurs propres lois nationales sans le consentement de l´état concerné. Voir Cassese, A., *droit international.* p.53.
11 Brownlie, I., 2003. *Principes du droit public international* .6ieme ed. Oxford : Oxford University Press. p.306.
12 Jeschek, H. H., Weigend, T., 1996. *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5ieme edn. Berlin : Duncker & Humbold. pp.167 et seq.

Tous ces principes ont en commun le sens général de l´exigence d´un « lien suffisant » ou d´un « véritable lien » existant entre l´infraction et l´état qui exerce la juridiction.[13]

Principes de la juridiction pénale

Principe de la territorialité (principe objectif de territorialité)	Un état peut poursuivre des activités sur son territoire, même lorsque le délinquant est un citoyen étranger. Si le délinquant se trouve hors du territoire, la juridiction territoriale inclut le fait qu´un des éléments constitutifs de l´infraction, et plus particulièrement ses effets, aient eu lieu sur le territoire. Le principe objectif de territorialité garantit donc que l´état ou l´acte a commencé et l´état ou l´infraction a été accomplie peuvent légalement juger l´auteur présumée.[14]
Doctrine des effets	La juridiction est établie sur les comportements à l´étranger qui produisent des effets substantiels sur le territoire.[15]
Principe de nationalité **(Active)** **(Passive)**	La juridiction est établie en fonction de la nationalité de l´individu concerné.[16] La juridiction est établie en se basant sur la nationalité de l´auteur du délit, où que le délit ait été commis. La juridiction est établie en se basant sur la nationalité de la victime, où que le délit ait été commis.
Résidence habituelle	La juridiction est établie en se basant sur le lieu de la résidence habituelle de l´auteur du délit.[17]
Principe de protection	La juridiction est établie si un acte criminel commis à l´étranger est dérogatoire à la sécurité de l´état concerné et/ou concerne ses intérêts vitaux.[18]
Principe d´universalité	La juridiction est établie sur toute personne accusée d´avoir commis certains délits internationaux tels que la piraterie, des crimes de guerre ou de graves infractions à la Convention de Genève, indépendamment du territoire ou de la nationalité de l´individu impliqué.[19] Ce principe est généralement limité aux situations où l´état n´est pas à même d´intenter des poursuites ou refuse de le faire avec une juridiction territoriale.

Il est important de noter que l´utilisation de ces formes de juridiction par pays – sur la base de législations nationales ou d´accords internationaux – n´outrepasse pas automatiquement l´application des principes de souveraineté et de non-ingérence. Mener une enquête pénale sur un territoire étranger (en vertu du principe de protection ou du principe de la nationalité passive par exemple) requiert le consentement de l´état étranger.[20] La juridiction qu´un état fait valoir est donc liée, mais *séparable* de, à la question de la non-ingérence et à la violation de la souveraineté.

13 Epping, V. et Gloria, C., 2004. Der Staat im Völkerrecht. *In :* Ipsen, K., (ed.) *Völkerrecht.* 5ieme ed. Munich : C.H. Beck. pp. 321-22.
14 *Lotus* case, PCIJ, Series A, n°. 10, 1927, 23, 30.
15 Voir Hayashi, M., 2006. Principe objectif de territorialité ou doctrine des effets ? Juridiction et Cyberespace. *Droit* 6 :285.
16 Voir Shaw, M., 2003. *Droit internationa* p.579 et seq. et Cassese, A., 2005. *Droit international* pp.451 et seq.
17 Jeschek, H. H., Weigend, T., 1996. *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5th edn. Berlin : Duncker & Humbold. p.169.
18 Simma, B., Mueller, A., 2012. L´exercice et les limites de la juridiction. *dans* Crawford, J. and Koskenniemi, M., (eds.) *le compagnon de Cambridge au droit international.* pp.134, 143.
19 Cassese, A., 2005. *Droit international.* pp.451-452.
20 Brownlie, I., 2003. *Principes du droit public international.* 6ieme ed. Oxford : Oxford University Press. p.306. pour un exemple national juridique de l´interdiction des « activités illicites au nom d´un état étranger » voir l´Art. 271 du code pénal suisse : « *Celui qui, sans y être autorisé, aura procédé sur le territoire suisse pour un Etat étranger à des actes qui relèvent des pouvoirs public... sera puni d »une peine privative de liberté* ». Pour un exemple pratique de l´approche des enquêteurs criminels étrangers, voir : http ://www.rcmp-grc.gc.ca/interpol/fcip-pcece-eng.htm

Régimes d´assistance juridique internationale

Pour gérer le processus de consentement, afin de mener une enquête policière ou pénale hors du territoire de l´état, il existe de nombreux arrangements juridiques et informels entre les états, bilatéraux ou multilatéraux. Les traités relatifs à la remise formelle des suspects d´un pays à l´autre, par exemple, sont les exemples les plus anciens et les mieux connus du droit international.[21] Ces traités d´ »extradition » – ainsi que d´autres formes de coopération internationale (examinées ci-après) – sont soigneusement rédigés, afin de garantir que leurs mécanismes respectent le principe sous-jacent de souveraineté. L´Article 4 de la Convention sur la criminalité organisée stipul,e par exemple, que « *les états parties exécutent leurs obligations au titre de la présente convention d´une manière compatible avec les principes de l´égalité souveraine et de l´intégrité territoriale des états et avec celui de la non-intervention dans les affaires intérieures d´autres états* ». La Convention précise que : « *aucune disposition de la présente Convention n´habilite un état partie à, sur le territoire d´un autre état partie, exercer sa juridiction et accomplir des fonctions intrinsèquement étatiques au regard du droit international ou du droit interne* ».

Outre l´extradition, les principaux outils de coopération internationale incluent l´assistance accordée pour collecter des preuves dans les affaires pénales (« entraide judiciaire ») et les arrangements pour le transfèrement international des personnes condamnées.[22] L´extradition peut être définie comme un processus formel par le biais duquel un état requiert le retour forcé d´une personne accusée ou condamnée pour un délit, afin qu´elle soit jugée ou qu'elle purge une peine dans l´état requérant.[23] *Le droit international coutumier* ne comprend aucune « obligation d´extrader »[24] générale. Les arrangements sont donc généralement basés sur des accords bilatéraux ou multilatéraux, ou sur la réciprocité – la promesse faite par un état à un autre état d´accorder le même type d´assistance à l´avenir si cet état le requiert.[25] Afin d´éviter des lacunes juridictionnelles, les traités incluent généralement le principe fondamental « d´extrader ou de poursuivre ».[26] De même, les procédures d´entraide judiciaire sont généralement régies par des accords multilatéraux – surtout régionaux [27] – ou bilatéraux[28]. Les dispositions des traités sur l´extradition et l´entraide judiciaire peuvent être « autonomes » dans le sens où elles sont applicables aux « affaires pénales » en général,[29]ou d´une portée limitée si elles sont incluses dans un traité spécifique.[30]

Si un état est partie à ces accords, la procédure à suivre pour les requêtes envoyées et reçues est souvent établie par la législation nationale. De plus, dans certains pays, le droit interne peut souvent fournir une base pour la coopération internationale, plutôt que de s´appuyer sur un traité.[31] Le principal objectif de l´entraide judiciaire est d´obtenir des preuves, afin de les utiliser lors des procès et des poursuites pénales, le processus est donc intrinsèquement lié aux lois nationales sur la procédure pénale. Les preuves obtenues à l´étranger – souvent par l´état requis selon ses propres procédures – devront satisfaire les règles régissant la preuve de l´état requérant. Ceci peut inclure des normes relatives à l´ouïe dire et à la pérennité de la chaîne de garde des preuves ».[32] Afin de coordonner les requêtes d´extradition et d´entraide judiciaire envoyées et reçues, de nombreux états désignent une « autorité centrale » qui a le pouvoir de recevoir les demandes et de les exécuter ou de les transmettre aux autorités compétentes.[33]

---

21 Magnuson, W., 2012. Les politiques intérieures sur l´extradition internationale. *Journal de Virginie de droit international,* 52(4) :839-891.

22 Pour une vue d´ensemble voir *le Manuel sur l´entraide judiciaire et l´extradition* de l´ONUDC, 2012,et *le manuel sur le transfèrement international des personnes condamnées* de l´ONUDC, 2012..

23 *Ibid.* (*Manuel sur l´entraide judiciaire et l´extradition.* p.19).

24 *Le cas Lockerbie* , Déclaration conjointe des juges Evensen, Tarassov, Guillaume et Aguilar Maudsley, *ICJ Rapports* 1992, 3 :24.

25 ONUDC, 2012. *Manuel sur l´entraide judiciaire et l´extradition*. p.23.

26 Voir la Convention sur la criminalité organisée, Art. 16(10).

27 Voir, par exemple, *le traité sur l´entraide judiciaire en matière pénale* de l´Association des nations de l´Asie du sud-est (ASEAN), 2004. ; et la *Convention européenne sur l´entraide judiciaire en matière pénale entre les états membres de l´Union européenne* du Conseil de l´Europe, 2000..

28 Par exemple, l´Accord entre le gouvernement du Royaume Uni de Grande-Bretagne et d´Irlande du nord et le gouvernement de la république d´Argentine concernant l´entraide judiciaire contre le trafic illicite de drogue, signé le 27/08/1991 et entré en vigueur le 01/06/1994 ; le traité d´entraide judiciaire en matière pénale entre les états Unis d´Amérique et Panama, signé le 04/11/1991 et entré en vigueur le 09/06/1995.

29 Voir, par exemple, l´Accord d´entraide judiciaire en matière pénale entre l´Union Européenne et le Japon. OJ L 39/20. 12 février 2010.

30 Voir, par exemple l´article 7 de la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes de 1988, qui stipule que les états parties accorderont leur assistance pour ce qui concerne « *les infractions pénales établies conformément au paragraphe 1 de l´article 3* ». Les infractions en cause concernent la production, la manufacture, l´extraction etc. de stupéfiants et de substances psychotropes

31 UNODC, 2012. *Manuel sur l´entraide judiciaire et l´extradition,* p.22.

32 *Ibid.* p.15. Voir aussi le chapitre Six (preuves électroniques et justice pénale).

33 Voir le questionnaire de l´étude sur la cybercriminalité Q195 (extradition) et Q217 (entraide judiciaire).

L´Article 18 de la Convention sur la criminalité organisée demande, par exemple, aux états parties de désigner une autorité centrale pour les demandes d´entraide judiciaire.[34]

Une alternative évolutive à l´entraide judiciaire est le principe de *reconnaissance mutuelle* en matière d´enquêtes criminelles. L´entraide judiciaire traditionnelle exige généralement une vérification prolongée de la validité de la demande – notamment pour ce qui est de savoir si l´acte qui fait l´objet de la demande constitue une infraction au regard du droit interne de l´état requis.[35] La reconnaissance mutuelle entre les états vise à créer une procédure accélérée et simplifiée avec des possibilités limitées de refuser les demandes, basée sur le principe de la confiance mutuelle dans les systèmes pénaux et l´unité des lois. Son bon fonctionnement requiert des règles minimales concernant la définition des sanctions et des infractions pénales, ainsi que des possibilités harmonisées de protection des droits individuels.[36] Dans le contexte européen, le cadre de l´entraide judiciaire est accompagné d´une tendance émergente vers la reconnaissance mutuelle – par le biais du développement d´un mandat européen d´arrêt et d´obtention de preuves, et la proposition d´une « décision d´instruction européenne ».[37]

Outre les formes de coopération internationale formelle, certaines parties du processus des enquêtes extraterritoriales peuvent être traitées par le biais d´une communication informelle entre les polices ou les organismes. Cette communication peut être utilisée avant qu´une demande formelle d´entraide judiciaire ne soit présentée à une autorité compétente ou pour faciliter une demande formelle. Les réseaux informels entre les polices sont utilisés dans des cas de localisation de témoins ou de suspects, pour conduire des entretiens ou pour partager des documents ou des fichiers de police, et il existe deux préoccupations particulières : (i) que la demande ne soit pas perçue par l´état requis comme une tentative de mener une enquête étrangère en matière pénale sans le consentement approprié ; et (ii) que les preuves obtenues et destinées à être utilisées lors des poursuites ou du procès satisfassent les normes sur la preuve de l´état requérant ainsi que les exigences relatives à la chaîne de garde.[38]

Outre le réseau de relations bilatérales informelles entre les organismes d´application de la loi, INTERPOL maintient un système de bureaux centraux nationaux dans 190 pays. Les bureaux sont généralement des sections désignées des organismes nationaux d´application de la loi.[39] Par le biais d´un système en ligne « I-24/7 », les bureaux peuvent faciliter les demandes informelles bilatérales ou multilatérales entre les polices, ou la transmission d´une demande formelle d´entraide judiciaire d´une autorité centrale à l´autre par le biais des bureaux centraux nationaux .[40]

Qu´est-ce qu'une « dimension transnationale»?

La perception générale de la cybercriminalité qui implique une « dimension » transnationale exige une analyse approfondie. Quand et comment, peut-on dire qu´une infraction de cybercriminalité implique une dimension transnationale ?

34 L´Art. 18(13) de la Convention sur la criminalité organisée. Un répertoire des autorités compétentes désignées conformément à la Convention sur la criminalité organisée et ses protocoles et à la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes se trouve sur www.unodc.org/compauth

35 Voir l´Art. 18(9) de la Convention sur la criminalité organisée.

36 Dans le contexte européen voir, par exemple, le programme Stockholm. OJ C115, 4 mai 2010. 1-38.

37 Voir la décision cadre du Conseil 2008/978/JHA du 18 décembre 2008 sur le mandat européen d´obtention de preuves pour obtenir des objets, des documents et des données afin de les utiliser dans des procédures en matière pénale ; et l´Initiative du royaume de Belgique concernant la Décision d´instruction européenne en matière pénale. OJ C165/22. 24 juin 2010. Voir également l´Agence européenne des droits fondamentaux, 2011. *Opinion de l´agence européenne des droits fondamentaux sur le projet de directive concernant la décision d´instruction européenne.*

38 ONUDC, 2012. *Manuel sur l´entraide judiciaire et l´extradition.* pp.66-67.

39 voirhttp ://www.interpol.int/About-INTERPOL/Structure-and-governance/National-Central-Bureaus

40 ONUDC, 2012. *Manuel sur l´entraide judiciaire et l´extradition.* p.31.

Un point de départ est l´approche de la Convention des Nations Unies sur la criminalité organisée qui stipule qu´une infraction est de « *nature transnationale* » si : (i) elle est commise dans plus d´un état ; (ii) elle est commise dans un état mais une partie substantielle de sa préparation, de sa planification, de sa conduite ou de son contrôle a lieu dans un autre état ; (iii) elle est commise dans un état mais implique un groupe criminel organisé qui se livre à des activités criminelles dans plus d´un état ou (iv) elle est commise dans un état mais a des effets substantiels dans un autre état.[41]

L´approche comprend plusieurs caractéristiques importantes – y compris le principe d´effets substantiels dans un état. Toutefois, quand il s´agit d´actes de cybercriminalité, elle peut ne pas offrir une approche complète. Comme cela a été mentionné dans la section « auteurs de délits de cybercriminalité » du chapitre deux (la perspective d´ensemble), il n´y a aucune raison pour que les groupes criminels organisés soient au cœur des actes de cybercriminalité.[42] De plus, en raison du flux global de données dans les transactions d´internet, une « dimension » transnationale peut surgir sans qu´il y ait une « préparation, planification, conduite ou contrôle » dans un autre état.

Une approche de la cybercriminalité consiste à reconnaitre que la « dimension transnationale » prend tout son sens lorsqu´elle est examinée dans le cadre de considérations telles que (i) l*a juridiction* ; et (ii) les preuves criminelles. Une méthode pour caractériser une infraction vise à distinguer les *éléments* de la « *conduite* », *les* « *circonstances* », et les « *résultats*[43] de l´acte. Quand plusieurs de ces éléments sont présents ou produisent des effets substantiels dans une autre juridiction territoriale,[44] il existe une « dimension transnationale ». Comme cela a été mentionné précédemment, ceci aura des implications pour les revendications juridictionnelles. Conformément à cette approche, l´emplacement d´une infraction de cybercriminalité en soi pourrait ne pas être déterminante ou même pertinente. Le point important est donc l´ identification des éléments ou des effets substantiels qui permettent à un état d´établir sa juridiction – toujours sous réserve de l´existence d´un « lien suffisant ».

De plus, d´un point de vue plus général, la « dimension » transnationale d´un cyber délit peut provenir du fait qu´une partie du *modus operandi* de l´infraction a eu lieu dans une autre juridiction. La simple présence de données informatiques liées à l´infraction dans des serveurs extraterritoriaux pourrait, par exemple, ne pas être suffisante (en fonction du droit local) pour relever de la juridiction du pays où se trouve le serveur. Ceci serait, néanmoins, extrêmement important pour les preuves et le processus d'enquête des pays qui font valoir leur compétence – probablement en requérant une mesure telle qu´une demande d´entraide judiciaire au pays où se trouve le serveur. Dans cette situation, on pourrait dire qu´un cas de cybercriminalité revêt une dimension transnationale. Un grand nombre de cas de cybercriminalité entrent vraisemblablement dans cette catégorie. Toutefois, ils ne peuvent pas toujours être caractérisés comme tels – car il existe suffisamment de preuves dans la juridiction de poursuite ou bien les preuves extraterritoriales ne peuvent pas être identifiées.

Deux points sont particulièrement importants quand il s´agit de la dimension extraterritoriale des preuves : (i) la présence croissante de preuves électroniques dans tous les types de délits et non seulement pour les cyberdélits et (ii) l´utilisation croissante d´informatique en nuage qui implique un stockage de données parallèle et distribué. Le placement de données dynamique automatisé des services en nuage dans des centres de données physiquement répartis dans divers pays peut poser des problèmes pour identifier l´emplacement des données ».[45] Aprés avoir examiné la manière dont les approches nationales et internationales traitent les aspects transnationaux de la cybercriminalité en général, ce hapitre se clôt en mettant l´accent sur l´obtention des preuves extraterritoriales auprès des individus et des tiers fournisseurs de services.

41 L´Art. 3(2) de la Convention sur la criminalité organisée

42 Bien que dans la pratique plusieurs puissent être impliqués. Voir la Section 2.3 les auteurs d´infractions de cybercriminalité, le rôle des groupes criminels organisés du hapitre deux (la perspective d´ensemble)

43 Fletcher, G., 1978. *Reconsidérer le droit pénal*. Oxford : Oxford University Press. Par exemple, une infraction d´ « interférence avec un système informatique » peut requérir l´intention de « endommager, effacer, altérer ou supprimer des données informatiques » (conduite) « en entravant gravement » (résultat) le « fonctionnement d´un système informatique » (circonstance).

44 Il a été allégué que la doctrine des effets représente une extension du principe objectif de territorialité, car elle ne requiert pas qu´un élément de l´infraction soit localisé dans la juridiction. Voir, par exemple, *Ahlstrom et autres contre la Commission des communautés européennes* [1988] ECR 5193. Dans le contexte de la cybercriminalité, un examen des principes juridictionnels sur lesquels s´appuient les tribunaux nationaux dans les cas extraterritoriaux suggère que « *quelle que soit la caractérisation* [territorialité objective ou doctrine des effets] *sur laquelle un tribunal municipal choisit de s´appuyer*, *l´étendue de la juridiction justifiée sera la même* ». Voir Hayashi, M., 2006. Principe objectif de territorialité ou Doctrine des effets ? Juridiction et Cyberespace. *Dans : droit* 6 :284-302, p.285.

45 Voir, par exemple, Peterson, Z.N.J., Gondree, M. et Beverly, R., 2011. Un exposé de position sur la souveraineté des données : l´importance de la géolocalisation des données dans le nuage. *dans : Procédures de la conférence ACM sur la confidentialité et la sécurité des applications et des données* (CODASPY). Pour un exemple de technologie de placement automatisé de données dans des centres de données géo distribués, voir Agarwal, S., *et al.*, 2010. *Volley : placement automatisé de données pour des services de nuage géodistribués*. NSDI.

7.2 Juridiction

Principaux résultats :

- les lois internationales prévoient de nombreuses bases de juridiction sur les actes de cybercriminalité, y compris des formes de juridiction fondée sur le territoire et de juridiction fondée sur la nationalité ;
- certaines de ces bases sont également incluses dans les instruments multilatéraux sur la cybercriminalité ;
- aAlors que tous les pays d´Europe considèrent que leurs législations nationales fournissent un cadre juridique suffisant pour l´incrimination et la poursuite des actes de cybercriminalité extraterritoriale, près d´un tiers à un quart des pays localisés dans d´autres régions du monde signale des cadres juridiques insuffisants pour les actes de cybercriminalité extraterritoriale ;
- dans plusieurs pays, les dispositions reflètent l´idée que le délit « complet » doit avoir été commis dans le pays pour faire valoir la juridiction territoriale. Des liens territoriaux peuvent être établis par le biais des effets ou des éléments de l´acte, ou de la localisation des données ou des systèmes informatiques utilisés pour commettre le délit.
- les conflits de juridiction qui peuvent surgir sont généralement résolus avec des consultations formelles et informelles entre les pays ;
- les réponses fournies par les pays ne révèlent actuellement aucun besoin de formes additionnelles de juridictions sur la dimension putative du cyberespace. Les formes de juridiction fondée sur le territoire et de juridiction fondée sur la nationalité sont pratiquement toujours en mesure de garantir une connexion suffisante entre les actes de cybercriminalité et au moins un État.

Cette section examine l´approche juridictionnelle des pays et des instruments régionaux et internationaux contre la cybercriminalité. Comme cela a été mentionné au hapitre trois (cadres et législation) de cette étude, de nombreux instruments régionaux et internationaux contre la cybercriminalité comprennent des dispositions sur la juridiction. Les instruments stipulent généralement que les états parties doivent adopter des mesures législatives, ou autres, pour établir certaines formes de juridiction sur des infractions établies en conformité avec l´instrument.[46] Le tableau ci-après résume les dispositions concernant la juridiction dans les principaux instruments contraignants et non contraignants, internationaux et régionaux. Des détails additionnels et les numéros des articles sont aussi inclus dans le tableau de l´Annexe trois de la présente étude.

46 Voir, par exemple, l´article 22 de la Convention sur la cybercriminalité du Conseil de l´Europe

Dispositions sur la juridiction dans les instruments internationaux et régionaux sur la cybercriminalité

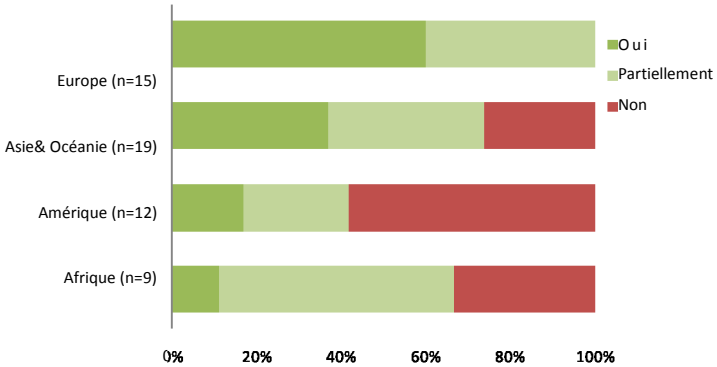
	Instruments contraignants					Instruments non contraignants		
Critères de compétence	Projet de convention qDe l´Union africaine	Accord de la communauté des états indépendants	Convention sur la cybercriminalité du Conseil de l´Europe	Convention de la Ligue des états arabes	Aaccor de l´organisation de coopération	Projet de loi type du COMESA	Loi type du Commonwealth	Textes législatifs types de l'UIT/CARICOM / CTU
Juridiction basée sur le territoire								
Territoriale	—	—	■	■	—	■	■	■
Dirigée contre système/données informatiques sur le territoire	—	—	—	—	—	■	—	—
Navires/Aéronefs	—	—	■	■	—	■	■	■
Juridiction basée sur la nationalité								
Active		—	—	■	■	—	■	■
Passive	—	—	—	—	—	—	—	—
Autre juridiction								
Résidence habituelle	—	—	—	—	—	—	—	—
Intérêts de l´état	—	—	—	■	—	—	—	—
Quand l´extradition est refusée	—	—	■	■	—	■	—	—
Dispositions additionnelles								
Règles sur la juridiction concurrente	—	—	■	■	—	■	—	

Les détails des dispositions individuelles sont examinés ci-dessous, ainsi que les pratiques et les exemples pertinents provenant des informations du questionnaire de l´étude sur la cybercriminalité fournies par les pays.

Poursuivre les infractions extraterritoriales

Durant la collecte des informations pour l´étude, on demanda aux pays s´ils considéraient que leurs cadres juridiques nationaux pour l´incrimination et la poursuite des actes de cybercriminalité commis hors de leurs pays, étaient suffisants.[47] Selon la figure 7.2, la perception générale est qu´ils sont suffisants mais il existe de nettes différences régionales. Environ un tiers du total des pays répondants considère que leurs cadres juridiques nationaux pour les infractions extraterritoriales sont suffisants » et 40 % considérait qu´ils étaient partiellement suffisants, alors que vingt-cinq % les considérait insuffisants.[48]

Figure 7.2 : est-ce que la législation nationale prévoit un cadre juridique suffisant pour l´incrimination et la poursuite des actes de cybercriminalité commis hors du pays ?



Source : questionnaire de l´étude sur la cybercriminalité.

47 Questionnaire de l´étude sur la cybercriminalité Q19.
48 *Ibid.*

En Amérique, seulement 40 % des pays déclarèrent que leurs cadres juridiques étaient suffisants ou partiellement suffisants, contre environ 67 % des pays d´Afrique, d´Asie et d´Océanie. Tous les pays répondants d´Europe – à l´exception d´un des pays qui avait signé et ratifié la Convention sur la cybercriminalité du Conseil de l´Europe – considérèrent que leurs législations étaient suffisantes ou partiellement suffisantes.

Les pays qui ne considéraient pas que leurs législations étaient suffisantes pour les actes extraterritoriaux, citèrent de nombreuses raisons. Les lacunes les plus communes incluaient un manque de dispositions dans le code pénal qui traitent les actes commis hors de la juridiction et, dans certains cas, le fait que la législation sur l´extradition et l´entraide judiciaire ne soit pas applicable aux actes de cybercriminalité.[49]

Les réponses fournies par les pays au questionnaire de l´étude montraient que les critères de juridiction dans les cas de cybercriminalité extraterritoriale sont principalement basés sur des principes tels que la territorialité (telle qu´interprétée par le principe de territorialité objective et la doctrine des effets substantiels) et la nationalité de l´auteur de l´infraction.[50] Les états requièrent donc généralement un certain niveau d´effets internes, comme la victimisation d´un ressortissant ou bien des effets ou des dommages sur le territoire. Les pays répondants ont souvent signalé qu´il pouvait être extrêmement difficile d´incriminer et de poursuivre un acte qui avait été commis *entièrement* hors du pays et sans effets pour le territoire.

Bases nationales communes pour la juridiction des cas de cybercriminalité

Territoire

- Commission partielle/complète du délit sur le territoire
- Effets/dommages sur le territoire
- Ordinateur/programme/données utilisés pour commettre un délit sur le territoire
- Commission d´un délit sur des navires et des aéronefs enregistrés sur le territoire (y compris militaires)

Nationalité

- Active – auteur de l´infraction
- Résidence habituelle
- Passive – Victime

Autres critères

- Les intérêts de l´état sont affectés
- *Ne bis in idem*

Utilisation de la juridiction territoriale

Instruments internationaux et régionaux – tous les instruments internationaux et régionaux contre la cybercriminalité qui contiennent une clause de compétence reconnaissent le principe de territorialité – qui exige que les états parties exercent leur juridiction sur toute infraction établie en conformité avec l´instrument, qui est commise sur le territoire géographique de l´état.[51] Les actes criminels commis sur des navires et des aéronefs sont aussi couverts par de nombreux instruments contraignants et non contraignants.[52] Conformément au principe de territorialité objective, plusieurs instruments régionaux et internationaux reconnaissent qu´il n´est pas nécessaire que tous les éléments de l´infraction aient lieu sur le territoire pour que la juridiction territoriale soit applicable. Le rapport explicatif sur la Convention sur la cybercriminalité du Conseil de l´Europe précise, par exemple, que selon le principe de territorialité, une partie fera valoir la juridiction territoriale si la personne qui attaque un système informatique et le système victime se trouvent sur le territoire, « *et si le système informatique attaqué se trouve sur le territoire même si l´attaque n´y est pas* ».[53]

49 *Ibid.*

50 Questionnaire de l´étude sur la cybercriminalité Q18 et Q19.

51 Voir, par exemple, l´Art. 22(1)(a) de la Convention sur la cybercriminalité du Conseil de l´Europe ; Convention, Art. 30(1)(a) de la Convention de la ligue des états arabes ; l´Art. 4(1) de l´UNOP-CRC-SC, l´Art. 40(a)(1) du projet de loi type du COMESA, l´Art. 19(a) des textes législatifs types de l´UIT/CARICOM/CTU, l´Art. 4(a) de la loi type du Commonwealth

52 Voir, par exemple, l´Art.40(b) du projet de loi type du COMESA, l´Art.4(b) de la loi type du Commonwealth.. Art. 22(1)(b), (c) de la Convention sur la cybercriminalité du Conseil de l´Europe ; l´Art. 25(1)(b), (c) de la Convention sur la protection des enfants du Conseil de l´Europe, ; l´Art. 19(b) des textes législatifs types de l´UIT/CARICOM/CTU ; l´Art. 30(1)(b), (c) ; de la Convention de la ligue des états arabes ; et l´Art. 4(1) de l´ OP-CRC-SC des Nations Unies

53 Conseil de l´Europe, 2001. *Rapport explicatif de la Convention sur la cybercriminalité.*

Le projet de loi type du COMESA inclut dans l´instrument une disposition sur « *l´endroit où l´infraction a été commise* ».[54] Un élément de cette disposition inclut : *« [une infraction est commise si]... (iii) en tout lieu où l´acte résultant est un élément d´une infraction qui conformément à... la présente loi a été commise ou aurait été commise* ».[55] La Directive de l´UE sur l´exploitation des enfants fait valoir la juridiction si l´infraction est commise totalement ou « *en partie* » sur le territoire. Elle précise que cela inclut le fait que l´infraction ait été commise au moyen d´une technologie de l´information et de la communication « *accessible depuis* » le territoire, que la technologie en cause *« se trouve ou non* » sur le territoire.[56] La décision de l´UE relative aux attaques visant les systèmes d´information couvre les attaques commises par un délinquant qui est physiquement présent sur le territoire (que le système d´information qui a fait l´objet d´une attaque se trouve ou non sur le territoire), et les attaques commises contre un système d´information qui se trouve sur le territoire (que le délinquant soit physiquement présent ou non sur le territoire).[57]

Exemple de législation spécifique sur la cybercriminalité qui couvre la juridiction territoriale dans des cas de cyberdélits d´un pays d´Afrique australe

Juridiction des tribunaux.
Un tribunal dans la République qui juge une infraction aux termes de la présente loi est compétent si :

(a) l´infraction a été commise dans la République ;
(b) la préparation de l´infraction ou une partie de l´infraction a été commise dans la République, ou un résultat de l´infraction a un effet dans la République ;
(c) ...
(d) l´infraction a été commise à bord d´un navire ou un aéronef enregistré dans la République ou lors d´un voyage ou d´un vol vers ou en provenance de la République.

Approches nationales – on observe au niveau national une influence des approches de territorialité des instruments régionaux et internationaux. Les pays mentionnent diverses dispositions qui reflètent l´idée qu´il n´est pas nécessaire que la « totalité » de l´infraction ait été commise dans le pays pour faire valoir la juridiction territoriale. Néanmoins, les mécanismes pour vérifier l´existence d´un lien territorial varient.

Dans certains cas, l´accent est mis sur « l´acte », dans d´autres cas sur l´emplacement des « données et des systèmes ».[58] Certains pays ont, par exemple, mentionné que la juridiction territoriale incluait les délits qui avaient été initiés, continués ou complétés dans quelque lieu que ce soit, mais qui avaient été *« partiellement commis,* » ou « *affectaient* » des biens, ou « *causaient* » un préjudice personnel sur le territoire de l´état.[59] D´autres pays mentionnèrent l´affirmation de la juridiction : si « *un serveur ou du matériel informatique utilisé pour commettre un délit* » se trouvait hors du territoire mais s'il existait « *un quelconque élément ou effet sur le territoire ».* [60] L´examen de la jurisprudence montre aussi que les tribunaux nationaux ont fait valoir leur juridiction lorsque tous les éléments d´un délit se trouvaient dans le pays, *à l´exception* du *résultat* (dans ce cas, le préjudice causé à une victime qui se trouvait hors du territoire et recevait des messages de harcèlement).[61] À l´inverse, les autorités d´application de la loi avaient aussi porté des accusations lorsque le *résultat* du délit (d´accès illégal et de perte pour fraude) était dans le pays, mais la *conduite* et l´emplacement des auteurs du délit étaient hors du territoire.[62] Les pays déclarèrent que ces concepts avaient été appliqués à des cas de paris sur internet et de pornographie infantile.[63] Un petit nombre de pays d´Europe et d´Amérique signalèrent, toutefois, que la législation nationale était insuffisante pour traiter des actes spécifiques de cybercriminalité extraterritoriaux – qui incluaient le déni de service, l´envoi de spam, et les attaques d´hameçonnage.[64]

54 L´Art. 40(f) du projet de loi type du COMESA.
55 *Ibid.* Art 40(f)(iii).
56 L´Art. 17 de la directive de l´UE sur l´exploitation des enfants
57 L´Art. 10 de la décision de l´UE sur les attaques contre les systèmes d´information
58 Questionnaire de l´étude sur la cybercriminalité Q18.
59 *Ibid.*
60 *Ibid.*
61 *DPP contre Sutcliffe* [2001] VSC 43. 1 mars 2001.
62 *UScontre Tsastsin et al.* Cour de district des États-Unis. District sud de New York. S2 11 Cr. 878.
63 Questionnaire de l´étude sur la cybercriminalité. Q18.
64 Questionnaire de l´étude sur la cybercriminalité. Q19.

Plusieurs pays ont déclaré qu´ils n´avaient pas de juridiction sur un acte entièrement commis et produisant des effets hors du territoire. Cependant, un pays d´Asie mentionna qu´il pourrait faire sa juridiction dans ces circonstances si les systèmes informatiques ou d´autres équipements utilisés pour commettre le délit se trouvaient sur son territoire.[65] Il existe une distinction conceptuelle entre le terme « les éléments et les effets de l´infraction, » et « les systèmes informatiques utilisés pour commettre l´infraction », bien qu´il y ait un chevauchement important entre ces deux approches – notamment lorsque l´utilisation d´un système informatique peut être caractérisée comme faisant partie de la « conduite » ou des « circonstances » des éléments de l´infraction.

Exemple de législation d´un pays des Caraïbes qui étend sa juridiction territoriale aux étrangers

(1) Sous réserve de l´alinéa (2), lorsqu´une infraction établie en conformité avec la présente loi est commise par une personne hors du territoire, la présente loi produira ses effets sur toute personne, quelle que soit sa nationalité ou sa citoyenneté, hors ou sur le territoire, comme si l´infraction avait été commise sur le territoire.
(2) Aux fins de l´alinéa (1), la présente loi sera appliquée si, pour l´infraction en cause :
(a) l´accusé se trouvait sur le territoire au moment matériel où l´infraction a été commise ;
(b) l´ordinateur, le programme ou les données se trouvaient sur le territoire au moment matériel où l´infraction a été commise ; ou
(c) des dommages sont survenus sur le territoire, que les paragraphes (a) ou (b) soient ou non applicables.

Enfin, certains pays mentionnèrent les contraintes de la nationalité sur la territorialité. Même lorsque une juridiction territoriale peut être revendiquée – lorsqu´un acte extraterritorial est couvert par la doctrine des effets – plusieurs pays ont déclaré que la situation était peu claire lorsque l´auteur d´une infraction extraterritoriale était un ressortissant étranger. Divers pays ont déclaré qu´ils engagent des procédures seulement si des exigences additionnelles sont satisfaites.[66] Dans un pays, par exemple, l´incrimination et la poursuite de ces suspects étrangers dépend du fait que l´infraction cause un préjudice important aux intérêts et à la sécurité internes.[67] Un petit nombre de pays d´Asie et d´Amérique ont signalé qu´ils faisaient valoir une juridiction sur les délinquants de toutes les nationalités, indépendamment du lieu où l´infraction avait été commise – si un lien pouvait être établi, comme la présence de l´auteur de l´infraction, ou les données ou le dispositif utilisé pour commettre l´infraction sur le territoire au moment où l´infraction a été commise, ou l´apparition de dommages sur le territoire.[68] Dans les cas où l´auteur étranger présumé de l´infraction est physiquement présent sur le territoire, plusieurs pays mentionnèrent l´obligation de « extrader ou poursuivre ».

Utilisation de la juridiction basée sur la nationalité

Les instruments régionaux et internationaux – lorsque les instruments régionaux ou internationaux contre la cybercriminalité reconnaissent le principe de territorialité, ils incluent aussi fréquemment le principe de nationalité active – qui requiert qu´un pays fasse valoir sa juridiction si un acte a été commis par un de ses ressortissants, y compris hors du territoire national.[69] Certains instruments requièrent que le comportement des ressortissants soit aussi incriminé dans le pays où l´acte a été commis.[70] Un nombre limité d´instruments prévoient la juridiction basée sur le principe de nationalité passive – notamment lorsque cela concerne les droits des enfants. La directive de l´UE sur l´exploitation des enfants et le OP-CRC-SC des Nations Unies exigent que les états établissent leur juridiction sur les

65 Questionnaire de l´étude sur la cybercriminalitéQ18.
66 *Ibid.*
67 *Ibid.*
68 Voir, par exemple, l´art.9 de la loi sur les délits informatiques de la Malaisie (1997 ; l´art. 11 de la loi sur l´utilisation abusive de l´informatique de Singapour (Révisé, 2007 ;l´art.12 de la loi sur l´utilisation abusive de l´informatique de Trinité et Tobago (2000)

69 Voir, par exemple, l´art. 25(1)(d) de la Convention sur la protection des enfants du Conseil de l´Europe, et l´art. 17(1)(b) de la directive sur l´exploitation des enfants de l´UE.

70 Voir l´Art.40(c) du projet de loi type du COMESA ; l´art. 4(d) de la loi type du Commonwealth ; l´art. 22(1)(d) de la Convention sur la cybercriminalité du Conseil de l´Europe, et l´art. 30(1)(d) de la loi type de 2004 de la Ligue des états arabes

infractions commises hors du territoire contre « *un de ses ressortissants,* » ou une personne qui est un « *résident habituel* ».[71] La Convention sur la protection des enfants du Conseil de l´Europe stipule que les états parties devront « *s´efforcer* » d´établir cette juridiction.[72] Ces dispositions offrent aux pays le pouvoir juridictionnel de garantir la protection des enfants ressortissants du pays qui se trouvent à l´étranger.

Approches nationales – de nombreux pays ont mentionné l´utilisation du principe de nationalité active pour faire valoir la juridiction sur des infractions commises par leurs ressortissants, quel que soit le lieu où elles ont été commises. Bien que cela ne soit pas une exigence commune, quelques pays ont signalé qu´il était nécessaire que l´acte constitue aussi une infraction dans l´état où il a été commis.[73]

Quelques pays ont également mentionné le principe de nationalité passive pour la juridiction sur des infractions qui affectent des ressortissants, quel que soit le lieu où elles ont été commises. Un pays d´Europe a, par exemple, signalé que de nombreux cas de cybercriminalité traités comprenaient des éléments extraterritoriaux et dans certains cas, les victimes ressortissantes du pays se trouvaient à l´étranger – et cela créait des complications juridictionnelles.[74] Un autre pays d´Europe a déclaré qu´il avait adopté un nouveau code pénal qui incluait le principe de nationalité passive spécifiquement pour réduire les difficultés juridictionnelles dans les cas où le délinquant est un étranger qui commet un délit à l´étranger affectant un ressortissant qui se trouve hors du territoire.[75]

Utilisation d´autres bases de juridiction

Instruments régionaux et internationaux – Deux instruments, la loi type et la Convention de la Ligue des états arabes, prévoient spécifiquement le principe de protection. La Convention spécifie, par exemple, que les états parties devront étendre leur compétence sur les infractions qui affectent « *un intérêt primordial de l´état* ».[76] Les instruments européens, y compris la Décision de l´UE sur les attaques contre les systèmes d´information, incluent aussi une base additionnelle de juridiction couvrant les infractions commises pour le bénéfice d´une *personne morale* dont le siège se trouve sur le territoire.[77] Enfin, conformément au principe « d´extrader ou poursuivre, » de nombreux instruments prévoient la juridiction sur des cas où l´auteur de l´infraction est présent sur le territoire et l´état, après avoir reçu un demande d´extradition, ne l´extrade pas vers un autre état, sur la seule base de sa nationalité,.[78]

Approches nationales – quelques pays répondants ont mentionné le principe de protection dans le contexte de conditions liées à d´autres formes de juridiction. Pour ce qui concerne d´autres bases de juridiction, comme la compétence universelle, de nombreux pays mentionnent la situation où l´auteur étranger d´une infraction entièrement commise hors du territoire se trouve sur le territoire sans qu´il y ait une demande d´extradition. Certains pays ont déclaré que la compétence universelle est limitée aux véritables délits internationaux et ne couvre généralement pas les actes de cybercriminalité.[79] D´autres pays déclarèrent toutefois que certains actes graves de cybercriminalité, comme la pornographie infantile, pourraient relever de cette forme de jurisdiction.[80]

---

71 Art. 17(2)(a) de la directive de l´UE sur l´exploitation des enfants, et l´art. 4(2)(b)de l´ OP-CRC-SC des Nations Unies.
72 l´Art. 25(2) de la Convention sur la protection des enfants du Conseil de l´Europe
73 Questionnaire de l´étude sur la cybercriminalité Q18.
74 Questionnaire de l´étude sur la cybercriminalité Q19.
75 *Ibid.*
76 L´Art. 30(1)(e) de la Convention de la Ligue des états arabes
77 L´Art. 10(1)(c) de la décision de l´UE sur les attaques contre les systèmes d´information ; l´Art. 17(2)(b)de la directive de l´UE sur l´exploitation des enfants on Child Exploitation, ; l´Art. 9(1)(c) de la décision de l´UE sur la fraude et la contrefaçon ; et l´Art. 13(1)(c) de la proposition de directive de l´UE sur les attaques contre les systèmes d´information
78 L´Art.40(d) du projet de loi type du COMESA de 2011 ; l´Art. 22(3) de la Convention sur la cybercriminalité du Conseil de l´Europe ; l´Art. 25(7) de la Convention sur la protection des enfants du Conseil de l´Europe ; l´Art. 10(3) de la décision de l´UE

sur les attaques contre les systèmes d´information, l´Art. 10(1) de la décision de l´UE sur la fraude et la contrefaçon, l´Art. 30(2) de la Convention de la Ligue des états arabes, et l´Art. 4(3) de l´OP-CRC-SC des Nations Unies

79 Questionnaire de l´étude sur la cybercriminalité Q18.

80 *Ibid.*

Conflits juridictionnels

Les instruments régionaux et internationaux – l´application de plusieurs bases juridictionnelles de différents pays peut donner lieu à une situation où plus d´un pays fait valoir sa juridiction sur un acte de cybercriminalité. De nombreux instruments régionaux et internationaux traitent ce problème de compétence concurrente. Certains stipulent, par exemple, que si une infraction relève de la juridiction de plus d´un état et si chacun des états concernés peut valablement engager des poursuites sur la base des mêmes faits, les états doivent coopérer et se consulter pour décider la juridiction la plus appropriée pour engager des poursuites.[81] Les instruments européens visent notamment à « *centraliser les procédures dans un seul état* ».[82] La Convention de la ligue des états arabes prévoit un ordre de priorité détaillé pour faire valoir la juridiction comme suit : (i) les états dont la sécurité ou les intérêts ont été affectés par l´infraction ; (ii) les états sur les territoires desquels l´infraction a été commise et (iii) l´état correspondant à la nationalité de l´auteur de l´infraction. Si on ne peut trouver un équilibre en suivant cet ordre la priorité est alors accordée au premier état requérant. [83]

Approches nationales – Durant la collecte des informations pour l´étude, les pays ont déclaré que, en général, ils n´avaient pas de législation spécifique pour résoudre les conflits de juridiction dans les cas de cybercriminalité.[84] De nombreux pays ont toutefois mentionné des projets pour traiter d´éventuels conflits de juridiction dans une législation spécifique en matière de cybercriminalité par le biais d´études ou de positions de principe juridiques. Un pays a déclaré qu´en matière de cybercriminalité « *le développement de règles juridiques universelles concrètes basées sur l´exclusivité juridictionnelle peut être difficile, et vraisemblablement déconseillée, en raison de la gamme de cas et de scénarios possibles* ».[85]

Les pays ont déclaré qu´ils résolvent les disputes juridictionnelles en s´appuyant sur des consultations formelles et informelles avec d´autres pays afin d´éviter les doubles enquêtes et les conflits juridictionnels.[86] Comme le signalait un pays d´Europe, « *[la plupart du temps les conflits de juridiction peuvent être évités avec une consultation informelle préalable, ou l´échange spontané d´informations. Les opérations d´enquêtes conjointes peuvent aussi y contribuer [...]* ».[87] La communication est conduite de manière bilatérale ou par les voies de communication mises à disposition par des institutions comme INTERPOL, Europol et Eurojust.[88] Un pays d´Amérique a indiqué qu´étant donné que la poursuite de ces délits fragmentés est extrêmement difficile, les procédures sont engagées seulement si l´auteur de l´infraction ou la victime est un de ses citoyens. Tous les autres cas sont transmis aux pays d´origine par le biais d´INTERPOL.[89] De plus, de nombreux pays ont mentionné le principe *ne bis in idem* (« pas deux fois »), et n´engagent de procédures que si le pays où l´acte a été commis n´a engagé aucune procédure. Avant de faire valoir leur juridiction, certains pays s´assurent que l´autre état qui réclame la juridiction respectera les normes relatives aux droits de l´homme lors des procédures et des enquêtes.[90]

81 L´Art. 25(8) de la Convention sur la protection des enfants du Conseil de l´Europe ; l´art. 22(5) de la Convention sur la cybercriminalité du Conseil de l´Europe ; l´art. 10(4) de la Décision de l´UE sur les attaques contre les systèmes d´information et l´art. 40(e) du projet de loi type du COMESA
82 Voir, par exemple, l´art. 10(4) de la Décision de l´UE sur les attaques contre les systèmes d´information
83 Art. 30(3) de la Convention de la Ligue des états arabes.
84 Questionnaire de l´étude sur la cybercriminalité Q18.
85 *Ibid.*
86 *Ibid.*
87 *Ibid.*
88 *Ibid.*
89 *Ibid.*
90 Questionnaire de l´étude sur la cybercriminalité Q19.

Juridiction suffisante ?

En général, l´analyse des dispositions des instruments régionaux et internationaux, et des lois et des pratiques des états, suggère que les problèmes de juridiction en matière de cybercriminalité peuvent être résolus en veillant à la clarté et à l´application innovatrice des principes existants.

Comme l´ont souligné les commentateurs, *« les transactions dans le cyberespace impliquent des personnes réelles dans une juridiction territoriale (i) qui effectuent des transactions avec des personnes réelles dans d´autres juridictions territoriales ou (ii) qui se livrent à des activités dans une juridiction qui causent des effets dans le monde réel dans une autre juridiction territoriale ».*[91] En conséquence, les formes de juridictions basées sur la territorialité et la nationalité sont presque toujours à même d´assurer l´existence d´un « lien suffisant » ou d´un « lien véritable » entre les actes de cybercriminalité et au moins un état. Cette étude estime donc qu´une juridiction additionnelle portant sur le cyberespace n´est pas nécessaire pour le moment. La majorité des actes de cybercriminalité entre dans l´une des deux catégories citées précédemment et peuvent réellement être liés à des états spécifiques. Comme cela est expliqué ultérieurement dans le présent hapitre, le fait que les données soient, de plus en plus fréquemment, transitoires et dispersées dans des centres de données internationaux, représente davantage une difficulté pour recueillir des preuves plus que pour établir une *juridiction*. Dans la mesure où les *éléments* et les *effets* d´un acte isolé de cybercriminalité pourraient tous être transitoires et dispersés, les formes de juridiction peuvent toujours recourir aux principes basés sur la nationalité et (pour les personnes morales), aux principes basés sur le lieu de constitution.

Comme cela est mentionné au hapitre quatre (incrimination) dans le contexte des lois internationales sur les droits de l´homme, un risque de la projection d´une juridiction extraterritoriale extensive pourrait être la pluralité du contenu d´internet. Au cœur du débat sur la juridiction, il y a l´interprétation du placement dans des limites géographiques des éléments et des effets de l´infraction. Si l´on considère cela sous l´angle des « actes, » de la « conduite, » des « circonstances, » des « données, » ou des « systèmes informatiques, » éviter les conflits en matière de juridiction dépend du fait de maintenir un seuil suffisamment élevé pour le concept d´un « véritable lien » – ainsi que des voies claires de communication entre les états pour coordonner les actions extraterritoriales de justice pénale.

91Post, D.G., 2002. « contre la Cyber anarchie ». *Journal juridique de technologie de Berkeley* (17) :1365-1387.

7.3 Coopération internationale I – coopération formelle

Principaux résultats :

- en raison de la nature volatile des preuves électroniques, la coopération internationale en matière pénale dans le domaine de la cybercriminalité requiert des réponses en temps opportun et la capacité de requérir des mesures d´enquêtes spécialisées ;
- l´utilisation des formes traditionnelles de coopération prédomine lorsqu´il s´agit d´obtenir des preuves extraterritoriales dans des affaires de cybercriminalité, et plus de 70 % des pays ont signalé l´utilisation de demandes formelles d´entraide judiciaire à cette fin ;
- dans le cadre de la coopération formelle, près de 60 % des demandes utilisent les instruments bilatéraux comme base juridique. Les instruments multilatéraux sont utilisés dans 20 % des cas ;
- les délais de réponse des mécanismes formels sont de plusieurs mois pour les demandes d´extradition et d´entraide judiciaire ;
- il existe dans certains pays des voies pour les demandes urgentes d´entraide judiciaire, toutefois leur impact sur le délai de réponse n´est pas clair ;
- la situation actuelle de la coopération internationale est exposée à l´émergence de groupements de pays ayant les procédures et les pouvoirs nécessaires pour coopérer entre eux, mais limités, pour tous les autres pays, aux modalités « traditionnelles » de coopération internationale qui ne tiennent pas compte des spécificités des preuves électroniques et de la nature globale de la cybercriminalité.

Cette section examine les mécanismes de coopération internationale en matière de cybercriminalité existants des instruments internationaux et des pratiques et des lois nationales.

Les dispositions relatives à la coopération des instruments régionaux et internationaux

Comme le mentionne le hapitre trois (cadres et législation) de la présente étude, de nombreux instruments régionaux et internationaux contre la cybercriminalité contiennent des dispositions relatives à la coopération internationale. Les instruments comprennent normalement des obligations générales de coopération imposées aux états,[92] et/ou des mécanismes particuliers de coopération, en matière d´extradition[93] et d´entraide judiciaire.[94] Le tableau ci-dessous présente les dispositions relatives à la coopération internationale des instruments régionaux et internationaux contre la cybercriminalité, contraignants et non contraignants. Le tableau de l´Annexe trois de la présente étude inclut des détails supplémentaires et les numéros des articles.

92 L´Art. 5 de l´Accord de la communauté des états indépendants ; l´art. 23 de la Convention sur la cybercriminalité du Conseil de l´Europe ; les Art. 3-5 de l´Accord de l´organisation de coopération de Shanghai. Le projet de convention de l´Union africaine fait référence à ce principe à l´Art. III(14).

93 L´Art. 42(c) du projet de loi type du COMESA ; l´Art. 38(3) de la Convention sur la protection des enfants du Conseil de l´Europe, L´art. 10 de la Décision de l´UE sur la fraude et la contrefaçon

94 L´Art. 6 de l´Accord de la communauté des états indépendants ; les Arts. 25, 27 de la Convention du Conseil de l´Europe sur la protection des enfants, l´Art. 35 du projet de directive de la CEDEAO ; les Arts. 32, 34 de la Convention de la Ligue des états arabes.

Dispositions relatives à la coopération des instruments internationaux et régionaux contre la cybercriminalité

	Instruments contraignants					Instruments non contraignants		
Dispositions sur la coopération internationale	Projet de convention de l'Union africaine	Accord de la Communauté des états indépendants	Convention sur la cybercriminalité du Conseil de l'Europe	Convention de la ligue des états arabes	Accord de coopération l´organisation de Shanghai Agreement	Projet de loi type du COMESA	Li type du Commonwealth	Textes législatifs types de l'UIT/CARICOM/ CTU
Dispositions générales de coopération internationale								
Principe général de coopération internationale	■	■	■	–	■	■	–	–
Instrument pour l´extradition	–	–	■	■	–	■	–	–
principe général d´entraide judiciaire	–	■	■	■	–	■	–	–
Assistance spécifique								
Assistance rapide	–	■	■	■	–	■	–	–
Conservation des données informatiques	–	–	■	■	–	■	–	–
Saisie/accès/collecte/ divulgation de données informatiques	–	–	■	■	–	■	–	–
Autres formes de coopération								
Accès transfrontalier	–	–	■	■	–	■	–	–
Réseau 24/7	–	–	■	■	–	■	–	–
Dispositions additionnelles								
Exigences de double incrimination	–	–	■	■	–	■	–	–

Un point de départ essentiel pour examiner ces dispositions est la *portée* de la *coopération*. Tandis que les dispositions relatives à la *juridiction* dans les instruments régionaux et internationaux se réfèrent généralement aux infractions établies en conformité avec l´instrument, les dispositions relatives à la *coopération internationale* peuvent viser les infractions et /ou avoir une portée plus large.

L´examen de cinq instruments contraignants montre que la cybercriminalité ou d´autres concepts étroitement liés, comme les « infractions liées aux informations informatiques » ou « les infractions liés aux technologies de l´information », rentrent dans le cadre des dispositions relatives à la coopération internationale de tous les instruments. De plus, deux instruments (la convention sur la cybercriminalité du Conseil de l´Europe et la convention de la Ligue des états arabes) appliquent les dispositions relatives à l´entraide judiciaire à tous les délits. Comme le mentionne le hapitre six (preuves électroniques et justice pénale), ceci est important dans le contexte du rôle croissant des preuves électroniques dans les enquêtes et les poursuites de toutes les formes de délits. Ce chapitre examine les implications de cette variation dans le cadre de la coopération internationale.

Instrument	Portée des dispositions relatives à la coopération internationale
Projet de convention de l´Union africaine	• « Cybercriminalité »
Accord de la communauté des états indépendants	• « Infractions liées aux informations informatiques »
Convention sur la cybercriminalité du Conseil de l´Europe	• « Infractions pénales liées aux données et aux systèmes informatiques • « Collecte de preuves électroniques d´une infraction pénale »
Convention de la Ligue des états arabes	• « Infractions liées aux informations et à la technologie de l´information » • « Collecte de preuves électroniques des infractions »
Accord de l´organisation de coopération de Shanghai	• « Sécurité des informations internationales »

Les mécanismes de coopération inclus dans les instruments régionaux et internationaux contre la cybercriminalité doivent être placés dans le contexte plus large de la coopération internationale. Bien que de nombreux instruments peuvent servir de base juridique pour des actes de coopération spécifiques,[95] il ne faut pas oublier que les états parties aux instruments, sont également parties à des accords bilatéraux et multilatéraux concernant la coopération en matière pénale – cela inclut les traités tels que la Convention sur la criminalité organisée. Selon la nature de l´acte qui fait l´objet d´une enquête, il est possible que les besoins en matière de coopération relèvent de divers mécanismes juridiques et certains instruments contre la cybercriminalité reconnaissent ce point. La Convention sur la cybercriminalité du Conseil de l´Europe stipule, par exemple, que les parties devront coopérer entre elles, non seulement « *en conformité avec les dispositions du présent chapitre* » mais aussi « *en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur la législation uniforme ou réciproque et de leur droit national* ».[96]

Enfin, il est important de souligner que les instruments *non*-contraignants ne peuvent pas fournir la même base juridique internationale pour la coopération que les instruments contraignants. Lorsque, par exemple, le projet de loi type du COMESA stipule que « *les autorités judiciaires* [*de ce pays*] *devront coopérer directement dans la mesure la plus large possible avec les autorités judiciaires d´un autre pays,* »[97] il s´agit seulement d´une recommandation à inclure dans la législation nationale. Même si une telle disposition est incorporée à la législation nationale, les pays requièrent généralement des mécanismes politiques et juridiques pour des actes spécifiques de coopération – comme un traité bilatéral ou multilatéral, ou un accord de réciprocité – avec le pays requérant concerné. À cet égard, il faut toutefois signaler l´existence dans certains pays de politiques de coopération de « portes ouvertes », et de lois nationales qui permettent en principe de coopérer avec tous les pays.[98]

L´extradition et l´entraide judiciaire dans les instruments régionaux et internationaux

Deux instruments contraignants inclus dans le tableau précédent (la Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes), et un instrument non contraignant (le projet de loi type du COMESA), envisagent spécifiquement l´extradition pour les infractions visées.[99]

95 Voir, par exemple, la Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 24 et. seq. ;la Convention de la Ligue des états arabes, Arts. 31 et seq. ;l´Accord de la communauté des états indépendants, Arts. 6 et seq. ;le projet de loi type du COMESA l, Arts. 42 et seq.

96 La Convention sur la cybercriminalité du Conseil de l´Europe, Art. 24.

97 Le projet de loi type du COMESA, Art.41.

98 Quelques pays répondants ont mentionné l´existence de ces politiques (questionnaire de l´étude sur la cybercriminalité Q220).

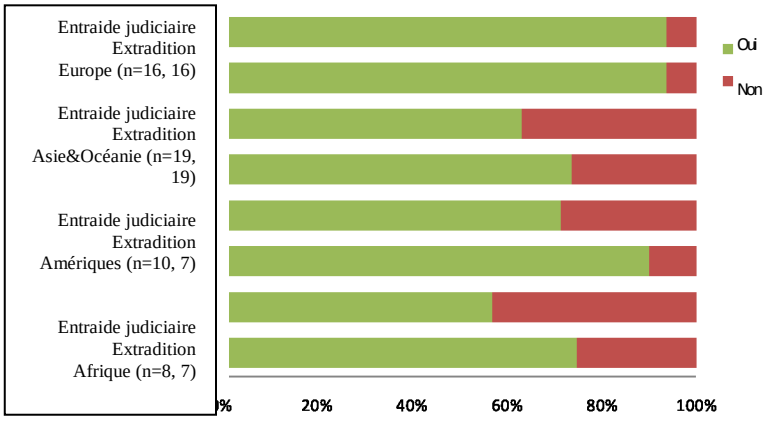
99 La Convention sur la cybercriminalité du Conseil de l´Europe, Art. 24 ; la Convention de la Ligue des états arabes, Art. 31 ; le projet de loi type du COMESA, Art42(c).

Tout ceci fait que l´extradition dépend de la double incrimination et de la gravité de l´infraction. Trois instruments contraignants (l´Accord de la communauté des états indépendants, la Convention sur la cybercriminalité du Conseil de l´Europe, et la Convention de la Ligue des états arabes) ainsi que le projet de loi du COMESA, prévoient aussi une entraide judiciaire générale.[100] Certains instruments stipulent que l´entraide judiciaire peut être soumise à la double incrimination.[101] Les instruments spécifient aussi que les demandes peuvent être refusées si leur exécution est « contraire à la législation nationale, »[102] si « la demande concernant un délit politique, »[103] ou si la demande « est de nature à porter atteinte à la souveraineté, la sécurité, l´ordre public ou d´autres intérêts essentiels ».[104]

Les instruments prévoient aussi des moyens rapides de communication, tels que les courriels et les fax, pour les demandes concernant des affaires urgentes,[105] et certains requièrent un niveau « raisonnable » de sécurité pour ces communications, et un suivi par écrit dans un délai déterminé.[106] La Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes incluent des dispositions spécifiques sur les demandes d´entraide judiciaire pour : (i) la conservation rapide des données informatiques stockées ; (ii) la divulgation rapide des données de trafic conservées ; (iii) une entraide judiciaire relative à la collecte des données de trafic en temps réel ; et (iv) une entraide judiciaire relative à l´interception des données du contenu.[107] Dans le cadre élargi des dispositions sur la coopération internationale de ces instruments, ces formes spécialisées d´assistance sont applicables non seulement aux délits liés à l´informatique mais aux délits en général.[108]

Utilisation des mécanismes de coopération dans les cas de cybercriminalité

Figure 7.3 : existence d´une législation pour l´extradition et l´entraide judiciaire dans les cas de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité Q193 et Q216. (n=53, 49)

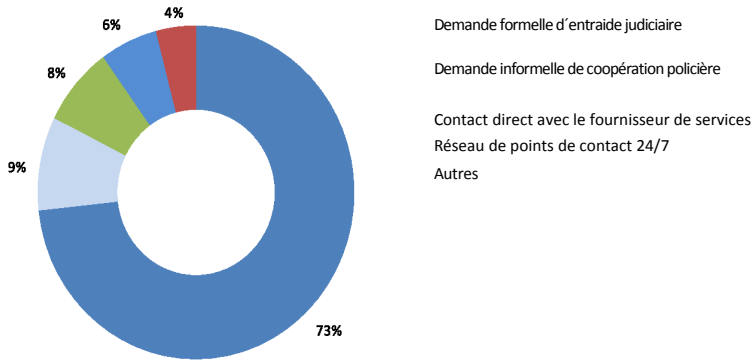
Au niveau des législations nationales, plus des deux tiers des pays d´Afrique, d´Asie, d´Océanie et d´Amérique ont signalé l´existence d´une législation nationale applicable à l´extradition et à l´entraide judiciaire dans des cas de cybercriminalité. Presque tous les pays d´Europe ont déclaré qu´une telle législation existait. La législation est généralement plus souvent appliquée pour l´extradition que pour l´entraide judiciaire.[109] L´analyse de la législation citée par les pays indique que la majorité de ces lois ne sont pas des lois spécifiques en matière de cybercriminalité, mais traitent l´extradition et l´entraide judiciaire dans des affaires pénales générales.[110] Il faut signaler que l´absence d´une législation nationale en matière d´extradition et d´entraide judiciaire n´est pas nécessairement un obstacle pour que les pays participent à la coopération internationale dans des affaires de cybercriminalité.

100 L´accord de la communauté des états indépendants, Art. 6 ; la Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 25, 27 ; la Convention de la Ligue des états arabes, Arts. 32, 34 ; le projet de loi type du COMESA, Arts. 43(a), 45.
101 Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 24(1), 25(5) ; Convention de la Ligue des états arabes, Arts. 32(5), 37(3) et (4) ; projet de loi type du COMESA, Arts. 42(a), 43(d).
102 Voir, par exemple, le projet de loi type du COMESA, Art. 45(c)(i).
103 Voir, par exemple, la Convention de la Ligue des états arabes, Art. 35.
104 Voir, par exemple, la Convention sur la cybercriminalité du Conseil de l´Europe, Art. 27(4)(b).
105 La Convention sur la cybercriminalité du Conseil de l´Europe, Art.25(3) ; la Convention de la Ligue des états arabes, Art. 32(3).
106 L´accord de la communauté des états indépendants, Art. 6(2).
107 La Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 29-31, 34 ; la Convention de la Ligue des états arabes, Arts. 37-39, 41, 42.
108 Il faut signaler que pour la collecte des données de trafic en temps réel et l´interception des données du contenu, l´assistance doit être fourni dans la mesure permise par le droit interne.
109 Questionnaire de l´étude sur la cybercriminalité Q193 et Q216.

110 *Ibid.*

Les affaires de coopération internationale peuvent être traitées en conformité avec des mécanismes nationaux comme les décrets ou les politiques administratives. L´utilisation de mécanismes formels de coopération dans des affaires de cybercriminalité transnationale prédomine sur d´autres formes de coopération. La figure 7.4 montre que plus de 70 % des autorités d´application de la loi ont déclaré que l´entraide judiciaire formelle était la plus souvent utilisée pour obtenir divers types de preuves d´autres juridictions.[111] Les mécanismes les moins utilisés incluaient la coopération policière informelle, le contact direct avec un fournisseur de services, et l´utilisation de points de contact 24/7.[112]

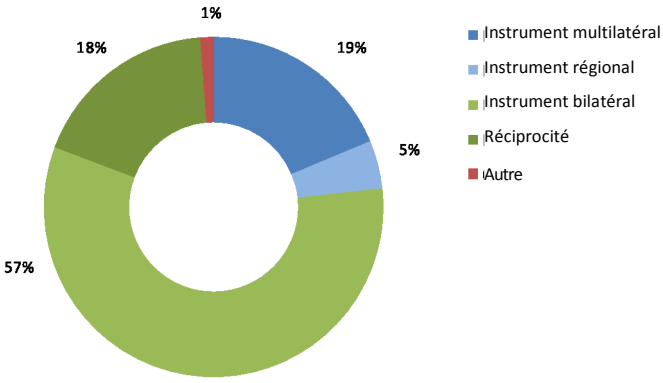
Figure 7.4 : moyens d´obtenir des preuves extraterritoriales



Source : questionnaire de l´étude sur la cybercriminalité Q105. (n=56, r=221)

Dans le cadre de la coopération formelle, l´utilisation d´instruments bilatéraux pour les affaires de cybercriminalité est la plus commune. Presque 60 % des pays ont signalé qu´ils utilisent les instruments bilatéraux comme base juridique pour l´extradition et l´entraide judiciaire dans des affaires de cybercriminalité,[113] et 20 % ont déclaré utiliser la réciprocité comme base juridique. Bien que dans le questionnaire de l´étude, environ 60 % des pays aient déclaré avoir signé ou ratifié un accord international ou régional contre la cybercriminalité contenant des dispositions sur la coopération,[114] seulement dans 25 % des cas les instruments régionaux ou internationaux furent cités comme une base juridique.[115]

Figure 7.5 : base juridique pour les demandes d´ extradition et d´entraide judiciaire dans les cas de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalitéQ202-207 et Q227-232. (n=21, r=50)

Le nombre de pays qui répondirent à la question sur la base juridique pour la coopération est comparativement faible, et les résultats devraient donc être interprétés avec prudence. L´utilisation prédominante de la réciprocité et d´instruments bilatéraux indiquent : (i) que tous les pays ne sont pas parties à des instruments multilatéraux ; et que (ii) les modalités traditionnelles de coopération internationale sont utilisées, même lorsque les pays sont parties à des instruments multilatéraux. À cet égard, aucun pays n´a signalé l´existence d´instruments bilatéraux spécifiques en matière de cybercriminalité, et aucun n´a été identifié au cours des recherches réalisées pour l´étude

111 Questionnaire de l´étude sur la cybercriminalitéQ105.
112 *Ibid.*
113 Questionnaire de l´étude sur la cybercriminalité. Q202-207 et Q227-232. La proportion des pays qui ont répondu à ces questions et qui ont signé ou ratifié un instrument régional ou international contre la cybercriminalité est la même que pour tous les pays répondants.
114 les états parties ou signataires de la Convention sur la cybercriminalité du Conseil de l´Europe (40 %), la Convention de la Ligue des états arabes (10 %), l´accord de la communauté des états indépendants (15 %), et l´accord de l´organisation de coopération de Shanghai (10 %). Ceci équivaut à plus de 60 % en raison de l´adhésion de certains pays à de multiples instruments.
115 Questionnaire de l´étude sur la cybercriminalité Q202-207 et Q227-Q232.

L´utilisation de modalités traditionnelles de coopération peut ne pas poser de problème lorsqu´elle utilisée entre des pays qui sont aussi parties à des instruments multilatéraux. Les pays seront probablement à même de demander des mesures d´enquêtes spécialisées dans des affaires de cybercriminalité – comme la conservation des données informatiques – si la législation nationale des deux pays prévoit les pouvoirs procéduraux pertinents. Cependant, l´utilisation des modalités traditionnelles lorsqu´aucun pays n´est partie à un instrument multilatéral peut poser des problèmes. C´est le cas pour la majorité des pays du monde. Au niveau mondial, plus de 60 % des pays ne sont pas parties à un instrument multilatéral contre la cybercriminalité – et par conséquent n´ont aucune obligation juridique *internationale* d´inclure des pouvoirs d´enquêtes spéciaux en matière de cybercriminalité dans le droit procédural national, ou de mener des enquêtes spécialisées à la suite de demandes de coopération.[116]

20 % des pas répondants ont, par exemple, déclaré que leur législation nationale ne prévoit pas la conservation rapide des données informatiques.[117] Comme on aurait pu s´y attendre, la majorité de ces pays (80 %) n´a ni signé ni ratifié d´instruments régionaux ou internationaux contraignants contre la cybercriminalité. Actuellement, les demandes de coopération internationale doivent être soumises à ces pays avec des modalités traditionnelles bilatérales et basées sur la réciprocité. Toutefois, si des mesures telles que la conservation rapide des données sont requises, la demande peut souffrir de : (i) un manque de clarté quant à savoir si ces mesures peuvent être requises en vertu de l´instrument ou de l´arrangement bilatéral pertinent, et/ou (ii) la non-existence de ces mesures dans la loi de procédure pénale nationale.

La double incrimination et d´autres dans la coopération en matière de cybercriminalité

L´utilisation de la coopération internationale pour enquêter sur des actes de cybercriminalité peut aussi poser des problèmes concernant l´équivalence de l´incrimination. Les demandes de coopération sont souvent soumises à diverses exigences de fond et procédurales – que l´état requérant doit satisfaire pour que l´état requis donne son consentement. Une exigence essentielle est la *double incrimination*. Le principe de la double incrimination exige que l´acte qui fait l´objet de la demande soit considéré comme un délit conformément au droit pénal de l´état requis et de l´état requérant.[118] La double incrimination figure dans les instruments régionaux et internationaux contre la cybercriminalité. Elle est nécessaire pour l´extradition et la Convention sur la cybercriminalité du Conseil de l´Europe ainsi que la Convention de la ligue des états arabes, par exemple, la requièrent pour certaines formes d´entraide judiciaire.[119]

Un facteur essentiel pour établir la double incrimination est la conduite sous-jacente de fond, plutôt que les définitions ou les termes techniques du délit dans les lois nationales.[120] La Convention sur la cybercriminalité du Conseil de l´Europe précise que l´exigence de double incrimination sera considérée comme satisfaite « *que le droit de l´état requis classe ou non cette infraction dans la même catégorie ou la décrive en utilisant la même terminologie que le droit de l´état requérant* » si « *le comportement sous-jacent à l´infraction* » pour laquelle l´assistance est requise « *est qualifié d´infraction pénale par son droit* ».[121] Conformément à cette approche, l´accent est mis sur la transposition des éléments de l´acte au droit de l´état requis afin de confirmer que l´acte est érigé en infraction pénale.[122]

116 Bien que, comme le mentionne le chapitre cinq (application de la loi et enquêtes), les pouvoirs d´enquêtes généraux existants peuvent être utilisés.

117 Questionnaire de l´étude sur la cybercriminalité Q49.

118 ONUDC, 2012. *Manuel sur l´entraide judiciaire et l´extradition*. La double incrimination n´est pas tant une règle du droit coutumier international qu´un traité et la considération d´un statut basés sur une politique et une opportunité (Williams, S.A., 1991. La règle de la double incrimination et l´extradition : une analyse comparative. *Nova Law review*, 15 :582).

119 On peut trouver des références à ce concept dans la Convention sur la cybercriminalité du Conseil de l´Europ, Arts. 24(1), 25(5), 29(3) et (4) ; la Convention de la ligue des états arabes, Arts. 32(5), 37(3) et (4).

120 L´article 43(2) de la Convention contre la Corruption des Nations Unies déclare, par exemple, que « *En matière de coopération internationale, chaque fois que la double incrimination est considérée comme une condition, celle-ci est réputée remplie, que la législation de l »État Partie requis qualifie ou désigne ou non l »infraction de la même manière que l »État Partie requérant, si l »acte constituant l »infraction pour laquelle l »assistance est demandée est une infraction pénale en vertu de la législation des deux États Parties* ».

121 Convention sur la cybercriminalité du Conseil de l´Europe, Art. 25(5).

122 Il existe deux approches à ce sujet : la double incrimination *in abstracto* et la double incrimination *in concreto*. « *In abstracto* » signifie que la considération du comportement en question se limite au fait de savoir si le comportement est punissable, indépendamment de sa qualification légale ou de l´existence de possibles raisons qui pourraient exclure la punissabilité. « *In concreto* » signifie que le comportement satisfait tous les critères de punissabilité, y compris l´absence d´une justification telle que l´excuse, l´autodéfense ou toute autre raison qui exclut la punissabilité. (voir le Comité européen pour les problèmes criminels du Conseil de l´Europe, 2012. *Note sur la double incrimination, in concreto ou in abstracto.* PC-OC (2012) 02 Final, 11 mai 2012.)

Certains actes de cybercriminalité peuvent être clairement incriminés dans un pays et non dans un autre – et ne satisfont donc pas le critère de double incrimination. La production, la distribution ou la possession d´outils informatiques malveillants, par exemple, n´est pas incriminé dans presque 20 % des pays qui répondirent au questionnaire de l´étude.[123] Les demandes concernant ce délit, soumises à ces pays auront donc un problème relatif à la double incrimination.

Pour ce qui concerne les actes généralement incriminés par les pays – comme les actes liés à l´informatique qui causent un préjudice personnel – les différences nuancées de la législation qui ont été examinées au chapitre quatre (incrimination) ne seront pas un obstacle pour établir la double incrimination. Néanmoins, en fonction de l´approche des autorités locales relative aux procédures de coopération – comme les audiences d´extradition – les différences concernant l´incrimination de certains actes de cybercriminalité peuvent être importantes. Dans certains pays, des caractéristiques telles que « l´utilisation de moyens techniques » pour commettre une infraction (dans le cas de l´interception illégale), ou de « seuils » d´insulte (dans le cas des infractions liées au contenu), peuvent être considérées comme des *éléments constitutifs* du délit – ceci signifie qu´il n´y a aucun délit si ces éléments ne sont pas présents. Dans ces circonstances, il peut donc surgir des problèmes de double incrimination. Un pays répondant a mentionné des problèmes de double incrimination dans une affaire de fraude informatique et d´infraction liée à l´informatique relative aux droits d´auteurs, et a signalé – en tant que pays requis– qu´il n´y avait aucun délit équivalant à celui qui faisait l´objet de la demande.[124]

De plus, la double incrimination peut avoir un rôle significatif pour les demandes d´entraide judiciaire [125] – y compris lorsque ces demandes d´assistance concernent la collecte de preuves électroniques pour « n´importe quelle infraction » (plutôt que des cyberdélits spécifiques ou des infractions « liées à l´informatique »). La Convention sur la cybercriminalité du Conseil de l´Europe, par exemple, permet aux états parties d´appliquer les exigences de double incrimination aux demandes de conservation des donnés.[126] Étant donné que les preuves électroniques géographiquement dispersées deviennent fondamentales pour les enquêtes de délits conventionnels, la mesure dans laquelle la double incrimination est requise deviendra un facteur essentiel.

Exemple d´une législation spécifique en matière de cybercriminalité sur la coopération internationale adoptée par un pays d´Afrique de l´ouest

Conservation et divulgation rapides des données informatiques dans le cadre de la coopération internationale

(1) La conservation rapide des données stockées dans un système informatique localisé dans [l´état] concernant les délits visés par la présente Loi, pourra être sollicitée à [l´état], en soumettant une demande d´assistance pour rechercher, saisir et divulguer ces données.

(2) …

(3) Lors de l´exécution de la demande soumise par une autorité étrangère conformément aux sections précédentes, le Procureur général de la Fédération peut ordonner à toute personne ayant ces données sous son contrôle ou y ayant accès, y compris un fournisseur de services, de les conserver.

à (6) …

(7) Une demande de conservation rapide de données informatiques peut être refusée s´il existe des motifs raisonnables de croire que l´exécution de la demande d´entraide judiciaire en vue de rechercher, saisir et divulguer ces données serait *rejetée en raison de l´absence de vérification de double incrimination.*

123 Questionnaire de l´étude sur la cybercriminalité Q28.

124 Questionnaire de l´étude sur la cybercriminalité Q215.

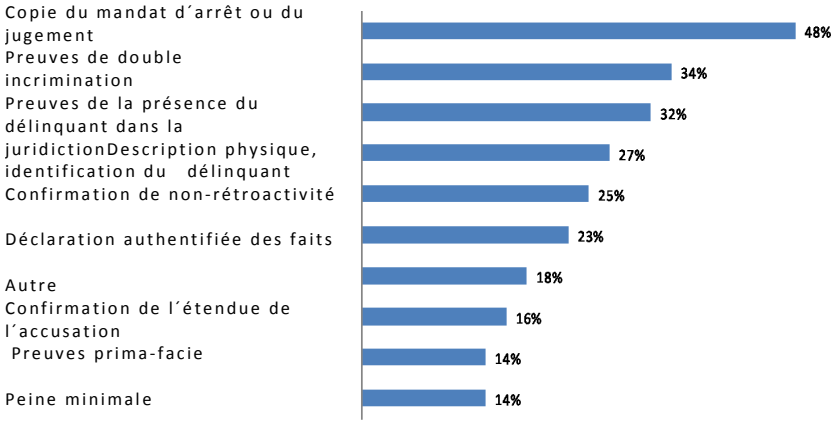
125 Pour ce qui concerne la coopération en matière pénale en général, la double incrimination pour l´entraide judiciaire peut ne pas être nécessaire du tout ou être exigée pour certains actes coercitifs d´entraide judiciaire, ou bien être requise pour tout type d´entraide judiciaire. (voir ONUDC, 2012. *Manuel sur l´entraide judiciaire et l´extradition*).

126 Convention sur la cybercriminalité du Conseil de l´Europe, Art. 28(4). Il faut noter que conformément à la Convention les demandes d´entraide judiciaire s´appliquent aux infractions pénales liées aux données et à l´informatique, ainsi qu´à la collecte de preuves électroniques pour tous types de délits.

D´une part, de nombreux pays ont signalé qu´ils exigent l´existence de la double incrimination lorsque les mesures requises sont « *particulièrement intrusives,* » comme la perquisition et la saisie, l´écoute ou la surveillance.[127] D´autre part, la double incrimination a un rôle important pour la protection de la souveraineté d´un état sur ses propres affaires de justice pénale et ses activités répressives. La protection de la double incrimination pourrait, par exemple, fournir une base juridique pour les pays pour refuser des demandes relatives à la fourniture de preuves électroniques concernant des infractions liées au contenu d´internet qui ne sont pas incriminées par le pays requis. Dans les cas concernant notamment l´entraide judiciaire et le contenu d´internet, des motifs additionnels de refus tels que les exceptions relatives aux infractions politiques, les exceptions relatives aux intérêts essentiels de l´état,[128] et même les obligations dérivées des droits de l´homme internationaux, peuvent être invoqués.[129] En effet, lorsqu´on leur demanda de préciser les raisons les plus fréquentes de refus de demandes d´entraide judiciaire dans des affaires de cybercriminalité, les pays répondants mentionnèrent spécifiquement « *l´atteinte aux obligations relatives aux droits de l´homme* » .[130]

Enfin, outre la question de l´*existence* d´une infraction pénale dans la législation de l´état requis, plusieurs instruments bilatéraux et multilatéraux établissent aussi des seuils de *gravité* pour les demandes de coopération internationale.[131] Ces seuils sont inclus, par exemple, dans la Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes – qui prévoient l´extradition pour les infractions établies en conformité avec la Convention « *punissables conformément aux lois des deux Parties* » (exigence de double incrimination) par « *la privation de liberté... d´au moins un an ou par une peine plus sévère* (seuil de référence).[132] Lors de la collecte des informations pour l´étude, les pays ont déclaré que les actes de cybercriminalité sont généralement considérés comme remplissant les critères des seuils de gravité – et constituent donc des infractions qui donnent lieu à l´extradition. Tous les pays répondants d´Europe et d´Amérique, et 90 % des pays d´Afrique, d´Asie et d´Océanie déclarèrent que les actes de cybercriminalité sont en général des infractions qui donnent lieu à l´extradition.[133] La contrainte de la double incrimination a été soulignée par les pays dans le contexte des conditions préalables pour les demandes de coopération en matière de cybercriminalité. On peut considérer que ces conditions ont un caractère de fond et procédural, et la manière dont de différentes conditions sont considérées varie en fonction des pays.[134]

Figure 7.6 : conditions préalables pour qu´une demande d´extradition dans une affaire de cybercriminalité soit considérée



Source : questionnaire de l´étude sur la cybercriminalitéQ198. (n=44, r=110)

127 Questionnaire de l´étude sur la cybercriminalité Q198.
128 Voir, par exemple, la Convention sur la cybercriminalité du Conseil de l´Europe, Art. 29(4).
129 Voir, par exemple, Currie, R.J., 2000. Les droits de l´homme et l´entraide judiciaire internationale : Résoudre la tension .*Forum de droit |pénal*, 11(2) :143-181.
130 Questionnaire de l´étude sur la cybercriminalité. Q239.
131 Voir, par exemple, la Convention sur la criminalité organisée, Arts. 2, 3, et 16.
132 Convention sur la cybercriminalité du Conseil de l´Europe, Art. 24.
133 Questionnaire de l´étude sur la cybercriminalité. Q194.
134 Pour l´extradition, une copie du mandat d´arrêt et la description physique du suspect peuvent, par exemple, être considérés des éléments procéduraux soumis à un contrôle initial de régularité. L´existence de la double incrimination peut être soumise à un

examen approfondi lors de l´audience d´extradition devant une autorité judiciaire (Réponse des experts régionaux nommés par WEOG aux résultats préliminaires de l´étude).

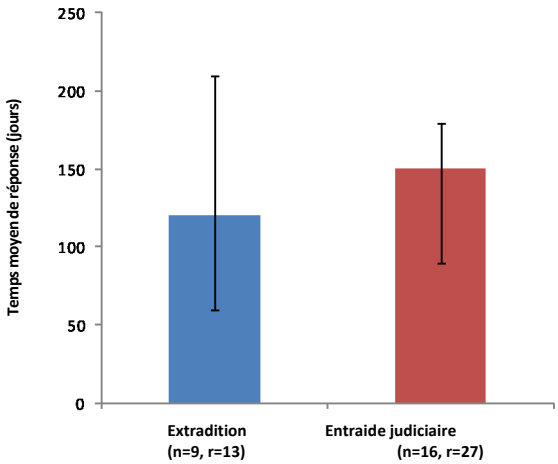
Bien que les pays mentionnent des éléments de fond et des éléments procéduraux, la double incrimination est néanmoins une exigence pour l´extradition et l´entraide judiciaire.[135] Dans le cas de l´extradition, les pays mentionnent aussi fréquemment des exigences procédurales escomptées comme une copie du jugement ou du mandat d´arrêt et des preuves attestant que le suspect se trouvait dans la juridiction.[136] Dans le cas de l´entraide judiciaire les pays mentionnèrent des conditions comme la suffisance de la preuve requise et une déclaration authentifiée des faits.[137]

Bien que de nombreux pays aient déclaré n´avoir jamais rejeté une demande d´assistance ou d´extradition dans une affaire de cybercriminalité jusqu´à présent, ils soulignèrent le fait de ne pas satisfaire les exigences de fond et les exigences procédurales lorsqu´on leur demanda de préciser les motifs fréquents de refus des demandes.[138] Les pays signalaient le plus souvent des irrégularités procédurales et des preuves insuffisantes – et cela met en évidence la nécessité de préparer soigneusement les demandes de coopération.[139] Les raisons substantielles fournies concernaient la double incrimination et les obligations dérivées des lois internationales sur les droits de l´homme.[140] Un pays a notamment mentionné le problème pratique de la « *volatilité des données informatiques* » comme un motif de refus de demandes d´entraide judiciaire[141] – ceci indique peut-être les demandes qui n´ont pas pu être satisfaites car les preuves électroniques pertinentes avaient déjà été éliminées. Ceci est étroitement lié au temps nécessaire de réponse pour les modalités formelles de coopération – une question traitée ci-après.

L´extradition et l´entraide judiciaire dans la pratique

Les statistiques disponibles citées dans le questionnaire de l´étude montrent que l´extradition et l´entraide judiciaire sont utilisées par les pays à des degrés divers. Environ la moitié des pays répondants a déclaré avoir envoyé ou reçu moins de 10 cas d´extradition ou d´entraide judiciaire en matière de cybercriminalité par an .[142] Le nombre moyen de cas fut de 8 par an, et trois quarts de tous les cas signalés se situaient entre 3 à 45 cas par an. Les pays avec le plus grand nombre de cas étaient généralement des pays plus grands situés en Europe ou en Amérique du nord.

Figure 7.7 : temps moyen de réponse (jours) pour les demandes d´extradition et d´entraide judiciaire en matière de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité

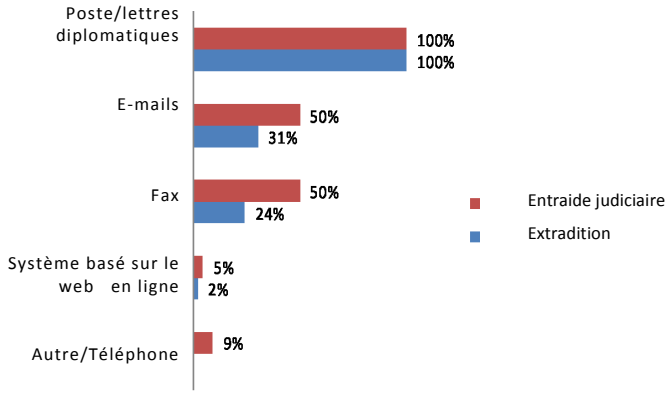
La répartition des infractions de cybercriminalité qui font l´objet de demandes d´entraides judiciaire et d´extradition est similaire au volume de cas traités par les services répressifs en général – et représentent environ un tiers des actes commis contre la confidentialité, l´intégrité et la disponibilité des données ou des systèmes informatiques, des actes causant des préjudices, et les actes liés au contenu.[143] Les mesures les plus fréquemment mentionnées accessibles aux états requérants pour enquêter sur ces actes, incluaient la fourniture de données de trafic ou du contenu stockées, ou la perquisition et la saisie de matériel ou de données informatiques.[144]

135 Questionnaire de l´étude sur la cybercriminalité Q198 et Q220.
136 *Ibid.* (Q198).
137 *Ibid.* (Q220).
138 Questionnaire de l´étude sur la cybercriminalité Q214 and Q239.
139 *Ibid.*
140 *Ibid.* (Q239).
141 *Ibid.* (Q239).
142 Questionnaire de l´étude sur la cybercriminalité. Q202-206 et Q227-231.
143 Questionnaire de l´étude sur la cybercriminalité Q208-211 et Q233-236.
144 Questionnaire de l´étude sur la cybercriminalité Q221.

Conformément au fait que les lois nationales de certains pays ne prévoient pas de pouvoirs d´enquêtes spéciaux, tels que la conservation des données informatiques ou la collecte des données du trafic ou du contenu en temps réel, seulement 35 % et 45 % des pays, respectivement, ont déclaré que ces mesures pouvaient être requises par l´entremise de l´entraide judiciaire.[145]

Alors que la gamme d´infractions couvertes et des pouvoirs d´enquêtes accessibles par le biais de la coopération internationale est expansive, dans la pratique le mécanisme est freiné par les longs délais de réponse. Les pays ont mentionné un délai moyen de réponse de 120 jours pour les demandes d´extradition et de 150 jours pour les demandes d´entraide judiciaire, reçues et envoyées.[146] Ces données devraient être considérées avec prudence, en raison du nombre relativement réduit de pays qui ont répondu à la question et à la possibilité que les pays appliquent diverses définitions d´échelles de temps lorsqu´ils répondent à cette question,par exemple, de la « réception de la demande » à la « réponse initiale », ou de la « réception de la demande » à la « résolution de fond ». Toutefois, étant donné que 75 % de tous les délais de réponse signalés figurent dans les barres d´erreur,[147] il est clair que les délais lors de l´utilisation de mécanismes formels de coopération sont de l´ordre de plusieurs mois et non de plusieurs jours. Les longs délais de la coopération internationale pourraient être dus au fait de recourir aux voies traditionnelles formelles de communication qui requièrent généralement la participation de multiples autorités dans la chaîne de communication. Par exemple, tous les pays ont signalé qu´ils utilisaient la poste ou les lettres diplomatiques pour soumettre des demandes d´extradition ou d´entraide judiciaire en matière de cybercriminalité.[148] De nombreux pays ont précisé que les modalités de transmission des demandes sont régies par les dispositions des conventions multilatérales ou des traités bilatéraux pertinents, qui dans certains cas incluent des exigences en matière de modalités formelles de communication.[149]

Figure 7.8 : formes de communication dans les affaires de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité Q197 et Q219. (n=44,47, r=77,94)

Les mécanismes de coopération formelle exigent généralement la désignation d´autorités centrales – et ces autorités gèrent l´envoi et la réception des demandes par poste ou par lettres diplomatiques. L´Accord de la Communauté des états indépendants exige, par exemple, que les états parties établissent une « *liste des autorités compétentes* ».[150] La Convention sur la cybercriminalité du Conseil de l´Europe requiert que les parties désignent des autorités centrales pour l´extradition et pour l´entraide judiciaire.[151] Étant donné que les cas de cybercriminalité sont traités de la même manière que d´autres cas de criminalité, les pays ont indiqué que dans les cas de coopération en matière de cybercriminalité, les autorités centrales sont les institutions qui ont généralement un rôle d´autorité centrale., [152] comme le bureau du garde des sceaux ou du procureur général et le ministère de la Justice.[153]

145 *Ibid.*
146 Questionnaire de l´étude sur la cybercriminalité Q213 et Q238.
147 Les barres d´erreur de la figure représentent les quartiles inférieurs et supérieurs
148 Questionnaire de l´étude sur la cybercriminalité Q197 et Q219.
149 *Ibid.*
150 Accord de la communauté des états indépendants, Art 4.
151 Convention sur la cybercriminalité du Conseil de l´Europe, Arts. 24 et 27. Les autorités compétentes notifiées conformément à ces articles sont énumérées sur :http ://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp
152 Questionnaire de l´étude sur la cybercriminalité Q195 et Q217.
153 *Ibid.*

Certains pays ont déclaré qu´en fonction de l´étape des procédures, le rôle d´autorités centrales était assigné à différentes autorités.[154] Alors qu´une autorité centrale déterminée est chargée de coordonner les requêtes, la décision finale relative à une demande revient souvent à une autorité nationale différente.[155] Pour les pays d´Europe, par exemple, l´autorisation des demandes n´est pas traitée de manière uniforme – avec des décisions rendues par un tribunal national d´instance inférieure et des décisions prises par l´organe exécutif du gouvernement.[156] Dans d´autres régions, les procureurs ou les magistrats ont également un rôle important. Les interactions (souvent nécessaires) entre diverses institutions gouvernementales peuvent, dans certains cas, contribuer aux longs délais de réponses mentionnés.

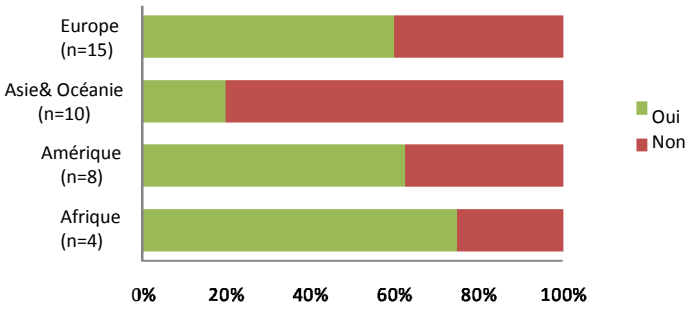
Comme le mentionnait le chapitre cinq (preuves électroniques et justice pénale), les preuves électroniques sont volatiles et peuvent n´exister que durant de courtes périodes de temps – dans certains cas, des périodes de temps beaucoup plus courtes que celles mentionnées précédemment par les états. De nombreux pays répondants ont, par exemple, déclaré que : « *les mécanismes formels de coopération internationale tels que l´entraide judiciaire peuvent exiger beaucoup de temps et entraîner des retards dans l´enquête et la poursuite des cyberdélits* ».[157] Les lois nationales qui régissent l´entraide judiciaire comprennent très rarement des dispositions spécifiques en matière de cybercriminalité qui reflètent cette réalité.[158] Néanmoins, certains instruments bilatéraux et multilatéraux ainsi que des lois nationales autorisent parfois des formes rapides de communication, comme les courriels, les fax, ou les systèmes en ligne.[159] La Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes stipulent, par exemple, que « *dans des circonstances urgentes* » les parties peuvent présenter des demandes d´entraide judiciaire par le biais de moyens rapide de communication, y compris par fax ou par courriel, avec une confirmation formelle postérieure.[160] Les instruments non contraignants prévoient aussi l´utilisation des « *moyens les plus efficaces, [...] à condition que des niveaux appropriés d´authentification et de sécurité soient utilisés et que la demande ou la réponse soit suivie d´une confirmation formelle* ».[161]

Lors de la collecte d´informations pour l´étude, environ la moitié des pays répondants a mentionné l´utilisation de courriels ou de fax pour les demandes d´entraide judiciaire. Une proportion beaucoup plus restreinte– 5 % – a signalé l´utilisation de systèmes en ligne. Comme cela était prévisible compte tenu du rôle de l´entraide judiciaire durant la phase d´enquête, l´utilisation de formes rapides de communication a été plus élevée pour les demandes d´entraide judiciaire que pour les demandes d´extradition.[162] Conformément aux exigences des instruments régionaux et internationaux contre la cybercriminalité, plusieurs pays ont déclaré que ces communications étaient suivies par l´utilisation de la poste et de lettres diplomatiques.[163] Un pays d´Amérique du sud a déclaré avoir utilisé des courriels et des fax pour suivre un processus d´extradition, et des pays d´Asie de l´ouest ont déclaré n´avoir recours aux communications électroniques que dans des cas urgents.[164] En concordance avec les niveaux d´utilisation signalés de courriels, de fax et de téléphone, plus de 60 % des pays d´Afrique, d´Amérique et d´Europe ont mentionné l´existence de voies pour les demandes urgentes d´entraide judiciaire. Toutefois, seulement 20 % des pays d´Asie et d´Océanie ont mentionné l´existence de ces voies. Plus d´un tiers des pays répondants a cité des mécanismes spécifiques pour les demandes urgentes comme les bureaux centraux nationaux d´INTERPOL et les réseaux 24/7 du G8 et du Conseil de l´Europe.[165]

154 *Ibid.*
155 Questionnaire de l´étude sur la cybercriminalitéQ218.
156 *Ibid.*
157 Questionnaire de l´étude sur la cybercriminalité Q141.
158 Questionnaire de l´étude sur la cybercriminalité Q193 et Q216.
159 *Ibid.*
160 La Convention sur la cybercriminalité du Conseil de l´Europe, Art. 25(3), et la Convention de la Ligue des états arabes, Art. 32(3).
161 Le projet de loi type du COMESA, Art. 43(b).
162 Questionnaire de l´étude sur la cybercriminalité Q197 et Q219.
163 *Ibid.*
164 Questionnaire de l´étude sur la cybercriminalité Q222.
165 *Ibid.*

Être partie à un instrument régional ou international des voies urgentes pour les demandes d´entraide judiciaire semble avoir un effet modéré – 55 % des pays répondants qui n´étaient pas parties à des instruments multilatéraux contre la cybercriminalité n´avaient pas de voies pour les demandes urgentes, contre 40 % des pays qui étaient parties à un instrument multilatéral contre la cybercriminalité.[166]

Figure 7.9 : voies pour les demandes urgentes d´entraide judiciaire



Source : questionnaire de l´étude sur la cybercriminalitéQ222. (n=37)

L´utilisation de mécanismes rapides pour les demandes d´entraide judiciaire en matière de cybercriminalité passe en partie par la gestion des problèmes causés par la volatilité des preuves électroniques, mais seulement la moitié des pays répondants a mentionné l´utilisation de ces mécanismes. De plus, si les délais de réponse des demandes formelles d´assistance cités dans le questionnaire de l´étude incluent les demandes traitées sur la base d´une urgence, les délais moyens des réponses – et la *distribution* prédominante des délais de réponse – sont encore évalués en mois et non en jours. Comme cela a été mentionné précédemment, la situation est différente quand il s´agit de modalités informelles de coopération. Étant donné que la coopération informelle offre une gamme plus réduite d´assistance, les délais de réponse sont généralement plus rapide.

7.4 Coopération internationale II – coopération informelle

Principaux résultats :

- les modalités de coopération informelle sont possibles pour environ les deux tiers des pays répondants bien que peu de pays aient une politique relative à l´utilisation de ces mécanismes ;
- il existe de nombreux réseaux de coopération informelle dans le domaine de la cybercriminalité, y compris les réseaux 24/7 du G8 et du Conseil de l´Europe ;
- les initiatives concernant la coopération informelle et visant à faciliter la coopération formelle, comme les réseaux 24/7, offrent un potentiel important pour des délais de réponse plus rapides, de l´ordre de quelques jours ;
- ces initiatives sont cependant peu utilisées, et le nombre de cas traités par le biais des réseaux 24/7 représente environ trois % du nombre total de cas de cybercriminalité traités par les autorités répressives du groupe de pays déclarants ;
- on estime avec l´analyse de la situation actuelle en matière de coopération internationale que les mécanismes de coopération formelle et informelle sont insuffisants. Globalement, les divergences concernant la portée des dispositions sur la coopération dans les instruments bilatéraux et multilatéraux ; un manque d´obligation de délai de réponse ; les multiples réseaux informels des services répressifs ; et la variance des garanties de coopération représentent des difficultés significatives pour une coopération internationale efficace pour ce qui concerne les preuves électroniques dans des affaires pénales.

166 *Ibid.*

Perspectives régionales et internationales

Outre les formes de coopération internationale formelle, les mesures relatives au processus d´enquête extraterritoriale des services répressifs peuvent être prises par le biais de la communication informelle entre les polices ou les organismes. Cette communication peut être utilisée avant qu´une demande formelle d´entraide judiciaire ne soit présentée à une autorité compétente, ou pour faciliter une demande formelle. La Convention sur la cybercriminalité du Conseil de l´Europe et la Convention de la Ligue des états arabes prévoient notamment des modalités informelles de coopération. Alors que la coopération peut être établie par la communication directe entre les polices ou par le biais de réseaux internationaux comme celui d´INTERPOL, ces deux instruments exigent que les états parties désignent un point de contact spécialisé. Le point de contact est chargé d´assurer la fourniture rapide d´assistance dans des enquêtes pénales liées aux données et aux systèmes informatiques pour collecter les preuves électroniques d´un délit pénal.[167] Conformément à la Convention sur la cybercriminalité du Conseil de l´Europe, les points de contact « 24/7 » devront faciliter, ou si la pratique et le droit national le permettent, directement : (i) fournir des avis techniques ; (ii) conserver les données (iii) rassembler les preuves, fournir des informations juridiques et localiser des suspects.[168] De manière plus générale, la Convention sur la criminalité organisée requiert que les états parties envisagent de conclure des arrangements relatifs à « *une coopération directe entre leurs organismes d´application de la loi* » .[169] Il existe au niveau international de nombreux réseaux de coopération informels en matière de cybercriminalité. Outre les réseaux 24/7 des états parties à la Convention sur la cybercriminalité du Conseil de l´Europe,[170] le sous-groupe du G8 sur le crime en haute technologie a établi un réseau 24/7 qui vise à renforcer et à compléter les méthodes traditionnelles utilisées pour obtenir une assistance dans des affaires qui impliquent des communications en réseau et d´autres technologies connexes.[171] Comme le montre la carte, le réseau du G8 inclut des pays qui sont parties à divers instruments régionaux et internationaux – et cela offre des opportunités de coopération informelle et d´un accès plus rapide à la coopération formelle à des pays qui n´auraient autrement pas été en mesure de recourir à des instruments juridiques multilatéraux partagés en matière de cybercriminalité .[172]

Figure.7.10 : membres du réseau 24/7 du G8 (2007)

Source : énoncé du protocol G8 24/7

« **La coopération informelle** est utilisée [...] 80 pour cent du temps, **car elle est plus rapide, particulièrement lors de la progression de l´enquête**. Il n´y a pas de **temps perdu** avec la présentation des demandes formelles, ce qui pourrait entraver l´enquête»...

Source : questionnaire de l´étude sur la cybercriminalité Q223 (réponse d´un pays d´Afrique de l´ouest).

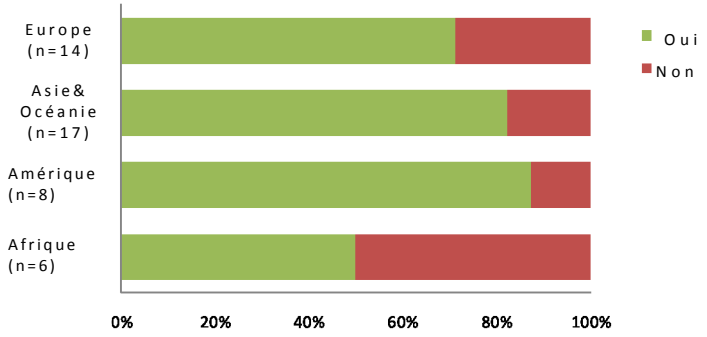
Les réseaux 24/7 offrent l´avantage d´être un point de départ connu et facilement accessible pour les demandes de coopération. L´évolution de multiples réseaux risque toutefois de nuire à l´atout de ce système qui est le « point de contact unique ».

167 Convention sur la cybercriminalité du Conseil de l´Europe, Art. 35 ; Convention de la Ligue des états arabes, Art. 43.
168 *Ibid.* (Convention sur la cybercriminalité du Conseil de l´Europe).
169 Convention sur la criminalité organisée, Art. 27(2).
170 Les points de contact 24/7 désignés conformément à l´art.35 de la Convention sur la cybercriminalité du Conseil de l´Europe, sont disponibles sur :http ://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp
171 Conseil de l´Europe, 2008. *L´efficacité de la coopération internationale contre la cybercriminalité : exemples d´une bonne pratique.* p.13.
172 Les membres du réseau 24/7 du G8 en décembre 2007. Voir http ://www.oas.org/juridico/english/cyb_pry_G8_network.pdf

Lors de la collecte des informations pour l´étude, un pays a, par exemple, mentionné que le point de contact national du réseau du G8 se trouvait dans un organisme d´application de la loi alors que le point de contact national du réseau 24/7 établi en conformité avec la Convention sur la cybercriminalité du Conseil de l´Europe, se trouvait dans le bureau du procureur attaché au tribunal supérieur.[173] Il peut être difficile pour d´autres pays de savoir de quel point de contact s´approcher quand il existe de multiples points de contact dans un pays. Ceci peut également entraîner des retards dans les réponses lorsque les pays requis doivent vérifier la validité ou l´identité du point de contact d´un organisme avec lequel il n´avait pas eu de communication préalable.

Approches nationales de la coopération informelle

Figure 7.11 : est-ce que l´assistance peut être fournie de manière informelle, aussi bien que par le biais d´une demande formelle d´entraide judiciaire ?



Source : questionnaire de l´étude sur la cybercriminalité Q223. (n=45)

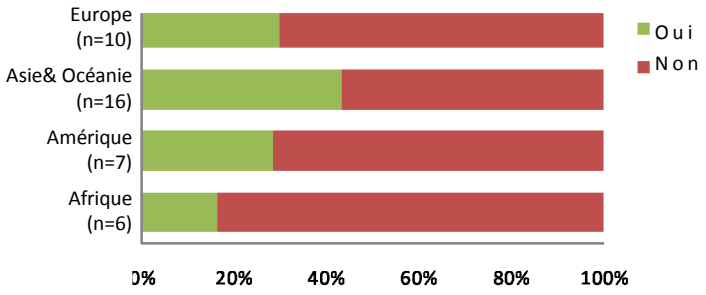
La majorité des pays répondants ont déclaré que l´assistance pouvait être fournie de manière informelle, aussi bien que par le biais d´une demande formelle d´entraide judiciaire.[174] La proportion de pays qui étaient à même de fournir une assistance informelle était notablement plus élevée en Europe, en Asie, en Océanie et en Amérique (entre 70 et 90 %) qu´en Afrique (environ 50 %).[175]

Les pays qui utilisaient la coopération informelle signalèrent que ces mécanismes dépendaient de l´existence d´homologues étrangers compétents et bien organisés et ils commentèrent que ceci était le cas lorsque la coopération informelle des services répressifs était régie par une forme quelconque d´accord. De nombreux pays déclarèrent que la coopération informelle est par conséquent mise en place sur la base d´accords régionaux et bilatéraux, par l´entremise de réseaux établis par des institutions et des organisations internationales et régionales ; avec l´assistance des ambassades et des consulats ; et par le biais de réseaux privés entre les officiers des services répressifs.[176] Certains pays ont mentionné la coopération directe entre les polices et d´autres pays ont essentiellement parlé de la coopération informelle par le biais des voies établies par INTERPOL.[177] Un pays a signalé que cela concordait avec la réalité de la coopération juridique internationale, dans la mesure où les moyens informels de communication –aussi flexibles et utiles qu´ils puissent être – n´existent souvent qu´entre les états qui ont développé des relations de travail à long terme.[178] L´échange d´informations sur des affaires internationales par le biais de canaux policiers internationaux établis, est reconnue comme une étape nécessaire pour des enquêtes fructueuses. Même si les modalités informelles de coopération sont vraisemblablement plus efficaces quand elles se basent sur un accord clair, la majorité des pays ont signalé que l´utilisation de la coopération informelle, au lieu de l´entraide judiciaire formelle, n´était pas soumise à une politique définie.[179]De nombreux pays mentionnèrent toutefois l´existence de directives et de protocoles, ainsi que de règles « non écrites »

173 Réponse des experts régionaux nommés par WEOG aux résultats préliminaires de l´étude.
174 questionnaire de l´étude sur la cybercriminalité Q223.
175 *Ibid.*
176 *Ibid.*
177 Questionnaire de l´étude sur la cybercriminalité Q106 and Q223.
178 Réponse des experts régionaux nommés par le Groupe asiatique aux résultats préliminaires de l´étude.
179 Questionnaire de l´étude sur la cybercriminalité Q224.

Quand des règles existent, elles sont incluses dans la législation nationale, par exemple, dans des lois sur l´entraide judiciaire en matière pénale.[180] Les pratiques varient, notamment pour désigner la personne qui autorise l´assistance informelle. Les options vont du surintendant local ou de l´agent enquêteur supérieur au chef de la division contre la cybercriminalité, ou bien du procureur ou d´une autorité judiciaire au ministère de la Justice.[181] La majorité des pays tendent à autoriser des décisions au niveau de l´enquête – le procureur ou la police locale, parfois de concert avec les chefs respectifs de leurs organismes.[182] Un pays d´Asie du sud-est a, par exemple, mentionné que bien que le bureau du procureur général soit concerné par les demandes formelles, son implication n´est pas obligatoire pour l´assistance fournie par le biais de la coopération informelle.[183]

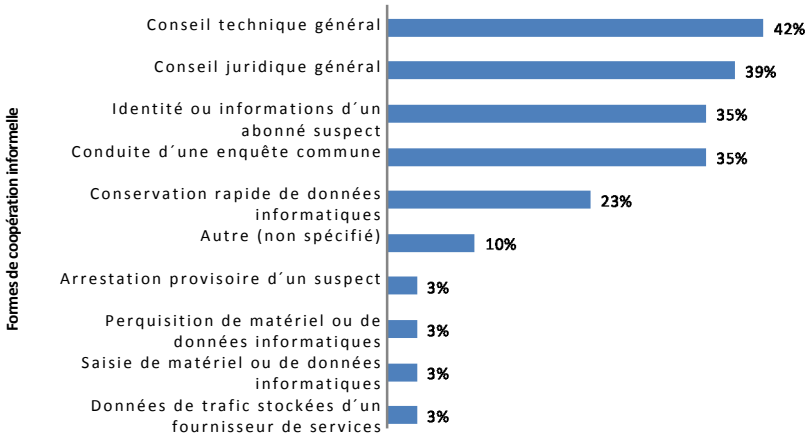
Figure 7.12 : politique pour l´utilisation de la coopération informelle au lieu de l´entraide judiciaire



Source : questionnaire de l´étude sur la cybercriminalité Q 224. (n=39)

Un manque général de politiques n´a cependant pas été un obstacle pour que les pays indiquent clairement les types d´assistance qui peuvent être fournis par le biais de la coopération informelle – avec toutefois certaines variations.

Figure 7.13 : formes de coopération informelle avec les services répressifs



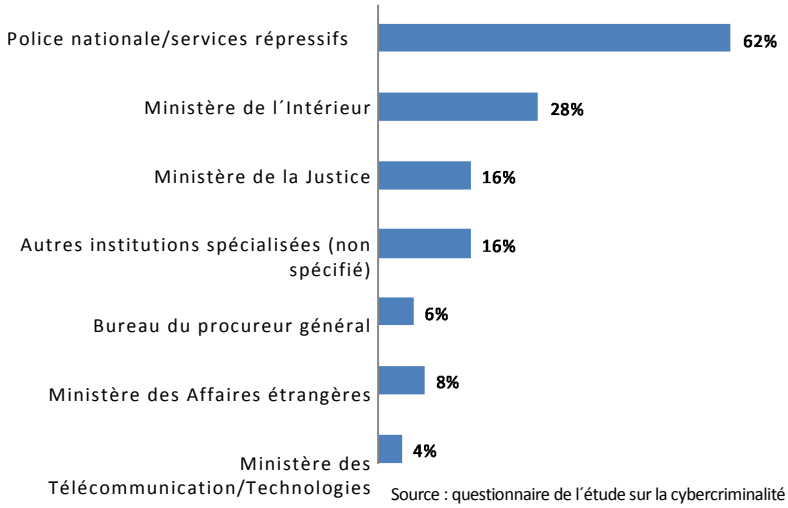
Source : questionnaire de l´étude sur la cybercriminalité Q106. (n=31, r=61)

Les pays ont déclaré qu´ils échangent des conseils techniques et juridiques généraux avec leurs homologues des services répressifs étrangers presque quotidiennement. La majorité de ces informations concerne les enquêtes communes ou des renseignements généraux opérationnels.[184] Presque tous les pays répondants sont à même de fournir ces informations de manière informelle, et seulement 10 % des pays ont déclaré que « *toutes les demandes informelles sont transmises à l´autorité chargée de l´entraide judiciaire* ».[185] Certains pays ont indiqué qu´ils partageaient même certaines données personnelles (y compris les titulaires des numéros de téléphone et de boîte postale, des informations des registres d´hôtel, et les détenteurs d´adresses IP sans recourir à des mesures de contrainte), et qu´avec la coopération directe des services répressifs, la surveillance, les antécédents judiciaires et les dépositions volontaires, des témoins pouvaient être fournis.[186]

180 *Ibid.*
181 Questionnaire de l´étude sur la cybercriminalité Q106, Q223 et |Q224.
182 Questionnaire de l´étude sur la cybercriminalité Q106.
183 Questionnaire de l´étude sur la cybercriminalité Q223.
184 Questionnaire de l´étude sur la cybercriminalité Q106.
185 Questionnaire de l´étude sur la cybercriminalité Q223.
186 Questionnaire de l´étude sur la cybercriminalité Q106.

Cependant, en général, les demandes de mesures d´enquête spécifiques, comme la conservation rapide des données, l´arrestation provisoire d´un suspect, ou la perquisition et la saisie de matériel et de données informatiques exigent une demande formelle d´entraide judiciaire, ou qu´une demande formelle ultérieure soit présentée dans un court délai.[187] Un pays d´Amérique du nord a, par exemple, déclaré que la coopération entre les polices « *ne permet pas d´utiliser des ordonnances obligatoires de collecte de preuves, comme l´émission d´ordonnances de production ou les citations à comparaître, l´exécution de mandats de perquisition ou d´autres mandats du Code pénal* ».[188] Un seul pays a déclaré que tous les types d´assistance formelle pouvaient aussi être obtenus par le biais de la coopération informelle. La situation la plus commune (plus des deux tiers des pays répondants) était que « *certains types d´assistance* » pouvaient être fournis de manière informelle.[189] Ceci coïncide avec le fait que la majorité des pays recourent à des moyens formels pour obtenir des preuves extraterritoriales lors des enquêtes sur des cyberdélits .[190]

Figure 7.14 : institution servant de point de contact 24/7



Source : questionnaire de l´étude sur la cybercriminalité Q107. (n=50, r=70)

Points de contact 24/7 – conformément aux initiatives au niveau régional et international, comme le réseau 24/7 du G8, plus de 70 % de tous les pays répondants ont mentionné l´existence d´une institution servant de point de contact 24/7.[191] Il est cependant probable que cette proportion soit très exagérée par rapport à l´existence des points de contact 24/7 au niveau global – en se basant sur la portée actuelle des réseaux 24/7 régionaux et internationaux et le nombre comparativement faible de pays répondants de régions telles que l´Afrique. Néanmoins, de nombreux pays répondants ont souligné l´importance des réseaux 24/7. Un pays a, par exemple, déclaré que « *Il est impératif d´avoir un point de contact (bureau HQ) pour avoir accès à la liste de contact 24/7 d´INTERPOL ainsi qu´aux points de contact 24/7 d´urgence du G8* »[192] En général les points de contact 24/7 sont établis dans les organismes de la police nationale et des services répressifs, ainsi que dans les ministères de l´Intérieur et de la Justice.[193] Comme cela a été mentionné précédemment les points de contact 24/7 peuvent faciliter et, s´ils y sont autorisés, agir directement en matière de coopération formelle et informelle. Les demandes les plus fréquentes reçues par les points de contact 24/7 concernaient l´identité ou des informations sur un abonné, des demandes de conservation rapide des données et la fourniture de données de trafic stockées.[194] Ceci est en conformité avec les fonctions prévues des points de contact 24/7 par la Convention sur la cybercriminalité du Conseil de l´Europe.[195]

187 Questionnaire de l´étude sur la cybercriminalité Q106 et Q223.
188 *Ibid.* (Q223).
189 *Ibid.* (Q223).
190 Questionnaire de l´étude sur la cybercriminalité Q105.
191 Questionnaire de l´étude sur la cybercriminalité. Q107.
192 Questionnaire de l´étude sur la cybercriminalité Q99.
193 *Ibid.*
194 *Ibid.*
195 Convention sur la cybercriminalité du Conseil de l´Europe, Art. 35.

Pour ce qui concerne les types de délits les plus fréquents, les pays ont déclaré que les demandes d´assistance concernaient le plus souvent la production, la distribution ou la possession de pornographie infantile liées à l´informatique, et, la sollicitation et la prédation sexuelles des enfants. Il y avait ensuite des demandes relatives à la contrefaçon et la fraude informatique.[196] La proportion des cas concernant la pornographie infantile traités par les points de contact 24/7 est légèrement plus élevée que tous les cyberdélits traités par les services répressifs en général.[197] Ceci peut refléter un degré plus élevé de dispersion internationale des victimes et des auteurs de ce délit. Par contre, un pays d´Amérique du sud a mentionné que ses points de contact 24/7 traitaient le plus souvent des infractions concernant les attaques aux systèmes informatiques du gouvernement, la dégradation des sites internet, les attaques de botnets et l´hameçonnage .[198]

Exemple d´une législation spécifique en matière de cybercriminalité sur les 24/7 d´un pays d´Afrique de l´ouest

Désignation d´un point de contact pour les réseaux 24/7

(1) Afin d´assurer une assistance immédiate à des fins de coopération internationale en conformité avec la présente loi, le Conseiller à la sécurité nationale désignera et maintiendra un point de contact disponible vingt-quatre heures sur vingt-quatre les sept jours de la semaine.

(2) Les autres points de contact pourront joindre ce point de contact en conformité avec les accords, les traités ou les conventions auxquels [cet état] est lié ou en conformité avec les protocoles de coopération des organismes judiciaires ou des services répressifs internationaux.

(3) Une assistance immédiate fournie par le point de contact inclut :

a) des conseils techniques à d´autres points de contact ;

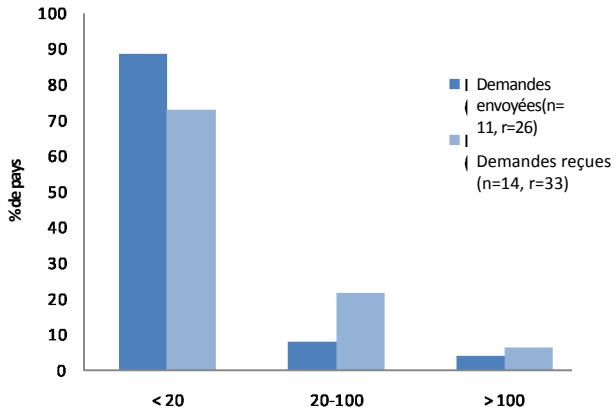
b) la conservation rapide des données dans les cas d´urgence ou de danger ;

c) la collecte des preuves sur lesquelles il y a une juridiction légale dans les cas d´urgence ou de danger ;

d) la détection des suspects et la fourniture d´informations juridiques dans les cas d´urgence ou de danger ;

e) la transmission immédiate des demandes concernant les mesures mentionnées à ... de cette section, en vue de leur mise en œuvre rapide.

Figure 7.15 : nombre de demandes envoyées et reçues par an par les points de contact



Source : questionnaire de l´étude sur la cybercriminalitéQ107. (n=11,14, r=26,33)

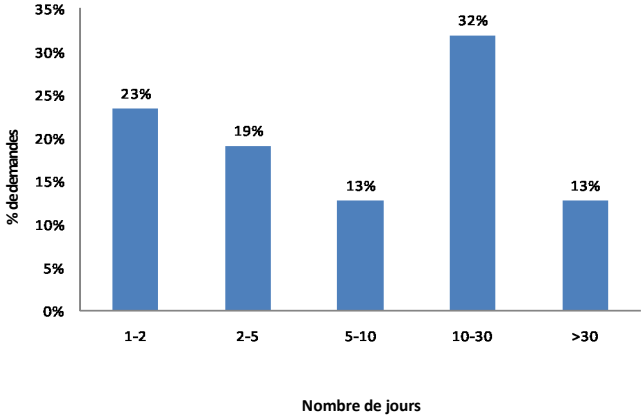
Seul un petit nombre de pays (avec une vaste répartition géographique) furent à même de fournir des statistiques relatives au nombre de demandes envoyées et reçues par les points de contact 24/7 chaque année. Les données fournies pour le questionnaire de l´étude montrent que plus de 70 % des pays traitaient moins de demandes (envoyées ou reçues) par an par le biais des points de contact. Seuls deux pays répondants traitaient plus de 100 demandes par an.[199]En comparaison, les services répressifs de ces mêmes pays déclarèrent qu´ils traitaient généralement une moyenne d´environ 1000 cas de cybercriminalité par an.[200] Pour ce groupe de pays, le nombre total de demandes traitées par les points de contact 24/7 par an, représentait 3 % du nombre total de cas de cybercriminalité traités par les services répressifs par an.[201]

196 Questionnaire de l´étude sur la cybercriminalité Q107.
197 voir le chapitre deux (la perspective d´ensemble), Section 2.2 la situation globale de la cybercriminalité, répartition des actes de cybercriminalité.
198 Questionnaire de l´étude sur la cybercriminalité Q107.
199 *Ibid.*
200 Questionnaire de l´étude sur la cybercriminalité Q54-71.
201 Calcul basé sur le questionnaire de l´étude sur la cybercriminalité. Q107 et Q54-71 pour tous les pays qui ont répondu aux deux séries de questions.

Tous les cas de cybercriminalité qui sont signalés aux services répressifs ne nécessitent pas l´implication des réseaux 24/7 – des enquêtes fructueuses peuvent être menées au niveau national. Néanmoins, le groupe de pays qui a fourni des données sur l´utilisation des points de contact 24/7 a aussi déclaré, qu´en moyenne, 60 % des cas impliquaient une dimension transnationale,[202] et il pourrait être possible d´utiliser plus amplement ce mécanisme.

La faible utilisation des réseaux 24/7 risque d´entraîner la perte des gains de temps potentiels dans les délais de réponse. Les pays qui ont répondu au questionnaire de l´étude ont signalé que presque 90 % des demandes traitées par les points de contact 24/7 recevaient une réponse dans un délai d´un mois.[203] Plus de 20 % des demandes reçurent une réponse dans un délai de un à deux jours. Un délai de réponse plus rapide, pour les demandes traitées par les points de contact 24/7 que pour les demandes d´entraide judiciaire, est prévisible, non seulement en raison de la nature du système des points de contact « 24/7 », mais aussi en raison du fait que – comme il s´agit d´une forme de coopération informelle – la gamme des actions qui peuvent être mises en œuvre par les points de contact 24/7 est plus limitée que dans le cas de l´entraide judiciaire formelle.

Figure 7.16 : temps moyen de réponse pour les demandes envoyées et reçues par les points de contact pour la coopération dans des affaires de cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité. Q107. (n=25, r=47)

Les délais de réponse signalés correspondent donc à un panel différent d´actions d´assistance de celles offertes par l´entraide judiciaire formelle – et les deux figures relatives aux délais de réponse ne sont donc pas directement comparables. Comme cela a été mentionné précédemment, un mécanisme informel tels que les points de contact 24/7, sont vraisemblablement habilités à fournir des conseils juridiques et techniques généraux, et à faciliter d´autres actions formelles mais non à collecter des preuves eux-mêmes.[204] Néanmoins, le fait que les points de 24/7 fournissent souvent une réponse dans un délai de quelques jours représente une ouverture importante des voies de communication qui facilitent une coopération en temps opportun, et éventuellement des actions qui requièrent une demande formelle.

La coopération est-elle suffisante ?

Ce chapitre soulignait, précédemment, que les bases actuelles de juridiction étaient vraisemblablement suffisantes pour éviter des lacunes juridictionnelles dans les enquêtes et pour lutter contre les actes de cybercriminalité. D´autre part, l´analyse des mécanismes de coopération formelle et informelle conclut que la situation globale actuelle est insuffisante pour faire face aux difficultés en matière d´enquête et de poursuite des cyberdélits. Bien qu´il existe de nombreuses options – y compris l´utilisation de la coopération informelle, directement ou pour faciliter la coopération formelle – plus de 70 % des pays ont déclaré qu´ils utilisaient généralement des demandes d´entraide judiciaire formelle pour obtenir des preuves électroniques localisées dans une autre juridiction. Dans le domaine de l´entraide judiciaire formelle, les instruments bilatéraux sont prédominants – et établissent des méthodes traditionnelles de communication comme la poste et les lettres diplomatiques qui entraînent des délais de réponses de l´ordre de mois et non de jours.

202 Questionnaire de l´étude sur la cybercriminalité. Q83. Données seulement pour les pays qui ont aussi répondu à Q107.
203 Questionnaire de l´étude sur la cybercriminalité. Q107.
204 Voir la Section 7.4 coopération internationale II – coopération informelle, approches nationales de la coopération informelle.

Comme l´ont mentionné les pays, de longs délais de réponse en matière de coopération créent des problèmes significatifs étant donné la volatilité des preuves électroniques. Bien que la coopération informelle dans des affaires de cybercriminalité offre des délais plus courts, le panel des mesures d´enquête pouvant être fournies varie considérablement ainsi que l´existence de politiques claires relatives à son utilisation. Plusieurs pays reconnaissent que les preuves obtenues par le biais de la coopération informelle ne sont pas considérées recevables lors d´un procès. En raison, peut être, de la diversité des approches, la coopération informelle pourrait même être considérée, dans certains cas, comme un mécanisme encombrant.[205] Alors que les réseaux « 24/7 » sont prometteurs pour rationaliser la coopération informelle et faciliter la coopération formelle, ils sont généralement peu utilisés par rapport à la masse d´affaires transnationales de cybercriminalité dont prennent connaissance les services répressifs.

Nombre de ces problèmes émanent des différences entre les instruments régionaux et internationaux, ceci est notable dans les différences relatives à la disponibilité de voies urgentes pour l´entraide judiciaire, à la capacité d´offrir des mesures spécialisées comme la conservation des données, en réponse aux demandes de coopération. La situation actuelle de la coopération internationale est exposée à l´émergence de groupements de pays ayant les procédures et les pouvoirs nécessaires pour coopérer entre eux, mais limités, pour tous les autres pays, aux modalités « traditionnelles » de coopération internationale qui ne tiennent pas compte des spécificités des preuves électroniques. Ceci est particulièrement vrai pour la coopération dans le cadre des mesures d´enquêtes. L´absence d´une approche commune, y compris parmi les instruments multilatéraux sur la cybercriminalité, signifie que les demandes de mesures, comme, par exemple, la rapide conservation des données, hormis les pays soumis à des obligations internationales de garantir ce service et de les mettre à disposition sur demande, peuvent ne pas être facilement satisfaites. L´inclusion de ce pouvoir dans le projet de Convention sur la cybersécurité de l´Union Africaine pourrait contribuer à combler cette lacune. Globalement, les divergences sur la portée des dispositions relatives à la coopération dans les instruments bilatéraux et multilatéraux, une absence d´obligation en matière de délai de réponse, une absence d´accords relatifs à l´accès direct autorisé aux données extraterritoriales, les multiples réseaux informels des services d´application de la loi et les variations de garanties en matière de coopération représentent des difficultés non négligeables pour une coopération internationale efficace pour ce qui concerne les preuves électroniques dans des affaires pénales.

205 Réponse des experts régionaux nommés par WEOG aux résultats préliminaires de l´étude.

7.5 Preuves extraterritoriales des fournisseurs de services et des nuages

Principaux résultats :

- en raison du développement de l´informatique en nuage, la « localisation » des données, bien qu´il soit techniquement possible de la connaître, devient de plus en plus artificielle, dans la mesure où même les demandes traditionnelles d´entraide judiciaire sont souvent adressées au pays où se trouve le siège du fournisseur de services, plutôt qu´au pays où se trouve physiquement le centre de données ;
- avec l´utilisation de la connexion en direct existante du dispositif d´un suspect ou les identifiants d´accès, les enquêteurs ont de plus en plus accès – sciemment ou non – aux données extraterritoriales lors de la collecte des preuves sans le consentement de l´état où ces données sont physiquement situées ;
- les enquêteurs des services répressifs peuvent parfois obtenir des données des fournisseurs de services extraterritoriaux par le biais d´une demande directe informelle, bien que les fournisseurs de services requièrent généralement une procédure légale en bonne et due forme ;
- les dispositions pertinentes existantes sur l´accès « transfrontalier » incluses dans la Convention sur la Cybercriminalité du Conseil de l´Europe et la Convention sur la lutte contre les infractions portant sur les technologies de l´information de la Ligue des états arabes ne couvrent pas ces situations de manière adéquate, car elles se basent sur le « consentement » de la personne qui est légalement autorisée à divulguer ces données et sur la connaissance présumée de la localisation des données au moment de l´accès ou de la réception.
- ces difficultés exigent de : (i) redéfinir la mesure dans laquelle la localisation des données peut continuer à être utilisée comme un principe directeur ; et (ii) développer des garanties et des normes communes relatives aux circonstances dans lesquelles les services répressifs peuvent avoir un accès direct aux données extraterritoriales

Les difficultés

Comme ce chapitre l´a exposé, les méthodes actuelles de coopération internationale en matière de cybercriminalité font face à des difficultés significatives – qui incluent les longs délais de réponse en matière d´entraide judiciaire, et la non-uniformité des mesures d´enquête nationale pour obtenir des données informatiques comme éléments de preuve. Une troisième difficulté – à laquelle il a été fait allusion dans la section sur la juridiction mais qui n´a pas été examinée – est de déterminer la juridiction pertinente à laquelle une demande de coopération pour l´obtention de preuves électroniques, devrait être adressée en premier lieu. Ce problème devient de plus en plus aigu car les services informatiques se sont déplacés vers des serveurs et des centres de données dispersés géographiquement et connus collectivement comme l´informatique en nuage.

Les services d´informatique en nuage se caractérisent par une « infrastructure sous forme de service, » un « logiciel sous forme de service, » et une « plateforme sous forme de service » couvrant la disposition relative aux machines virtuelles sur internet, la disposition relative aux applications logicielles, et la disposition relative au réseau, au système du serveur, au système d´exploitation et au stockage respectivement.[206] À cet égard, « le nuage » est un nouveau terme pour une ancienne idée – exploiter l´expertise et l´infrastructure d´une autre organisation pour fournir des ressources informatiques comme un service internet.

206 Voir, par exemple, la Direction générale des politiques internes, des droits des citoyens et des affaires constitutionnelles du Parlement européen, 2012.*Lutter contre la cybercriminalité et protéger la confidentialité dans le nuage.*

Le matériel informatique physique des services dans le nuage se trouve dans des centres de données situés à des points stratégiques conçus pour minimiser les retards dans la prestation des services et les frais d´électricité et de refroidissement de l´équipement. Les utilisateurs des services Google peuvent, par exemple, avoir accès à des données stockées ou traitées en Amérique du nord, en Asie du sud-est ou en Europe du nord ou de l´ouest.[207]

On dit souvent qu´il n´est pas possible de savoir où sont stockées les données dans le nuage et que les données peuvent être fragmentées dans plusieurs emplacements. Il est vrai que les bases de données peuvent être hébergées dans de multiples centres de données, y compris dans différents pays qui contiennent de multiples copies des mêmes données.[208] Ceci peut impliquer un placement de données dynamique automatisé des services en nuage dans des centres de données physiquement répartis dans divers pays.[209] Il est également vrai que les accords contractuels entre les fournisseurs de services informatiques en nuage et les utilisateurs ne révèlent pas toujours l´emplacement des centres de données, ou n´incluent pas toujours des déclarations ou des conditions relatives à l´emplacement géographique des données.[210] D´autre part, certains fournisseurs de services dans les nuages permettent à l´utilisateur d´indiquer la région physique où se trouveront les serveurs et leurs données et s´engagent à ne pas déplacer le contenu de la région sélectionnée sans le notifier à l´utilisateur.[211] De plus, les protocoles de géolocalisation pour l´identification à distance de l´origine de la source de données sont actuellement mis au point – et permettent une vérification indépendante de la géolocalisation des données dans le nuage.[212] En général, les exigences croissantes de conformité, les demandes des clients et la technologie de gestion de données tendent vers une localisation précise des données dans le nuage.

Il n´en demeure pas moins que – même lorsqu´il y a une géolocalisation des données dans le nuage – cela révèle un patron de données dispersées et parfois transitoires, qui inclut des copies dans de multiples juridictions. Quand les données dans le nuage sont des éléments de preuves d´une enquêtesur un cyberdélit, ce seront des preuves extraterritoriales (dans de multiples pays) par rapport au pays qui mène l´enquête. Cependant, dans certains cas, même le fait basique de l´extraterritorialité ne peut être reconnu avec certitude par les enquêteurs des services répressifs.[213] Souvent, le point de départ est seulement le nom du fournisseur de services dans les nuages – comme Amazon ou Google. Bien que la possibilité technique existe, il est improbable qu´un enquêteur des services répressifs puisse savoir – dès le début d´une enquête – dans quel pays les données dans le nuage sont physiquement localisées (même si elles n´ont pas déjà été déplacées). Si le siège du fournisseur de services dans les nuages ne se trouve pas dans le pays qui mène l´enquête, une approche traditionnelle d´entraide judiciaire exigerait une communication envoyée à l´autorité centrale de la juridiction de résidence du fournisseur de services, avec une demande de conservation et /ou de production des données informatiques. Il faut noter que conformément à cette approche, la demande d´entraide judiciaire peut ne pas être envoyée au pays *dans lequel les données sont réellement localisées*. Facebook, par exemple, héberge les données de nombreux utilisateurs dans un centre de données dans un pays d´Europe du nord,[214] mais spécifie qu´il divulgue les registres en conformité avec les lois en vigueur d´un pays d´Amérique du nord.[215]

207 Voir http ://www.google.com/about/datacenters/inside/locations/index.html

208 Voir, par exemple, http ://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf, qui fait référence au contrôle des opérations de multiples centres de données dans de multiples zones géographiques, par, entre autres, eBay et Netflix.

209 Voir, par exemple, Peterson, Z.N.J., Gondree, M., Beverly, R., 2011. *Un exposé de position sur la souveraineté des données :l´importance de la géolocalisation des données dans le nuage.* Pour un exemple de technologie de placement automatisé de données dans des centres de données géo distribués, voir Agarwal, S., *et al.*, 2010. *Volley : placement automatisé de données pour des services de nuage géodistribués*.

210 Benson, K., Dowsley, R., Shacham, H., 2011. Savez vous où sont vos fichiers dans les nuages ? *Procédures du 3ème atelier d´ACM sur la sécurité de l´informatique dans le nuage*, pp.73-82.

211 Voir, par exemple, Amazon Web Services, 2012. *Risques et conformité. Novembre 2012.* Disponible sur : http ://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

212 *Ibid.* Démonstration de l´identification réussie des géolocalisations approximatives des données dans le nuage d´Amazon. Voir aussi, Albeshri, A., Boyd, C. et Gonzalez Nieto, J., 2012. Géolocalisation : des preuves de la localisation géographique pour l´environnement de l´informatique en nuage. *Procédures de la 32ieme conférence internationale sur les ateliers des systèmes informatiques distribués 2012*, IEEE, Macao, Chine, pp.506-514.

213 Bien que cela puisse être inféré en se basant sur une vaste connaissance des localisations des centres de données des fournisseurs de services en nuages.

214 Voir https ://www.facebook.com/luleaDataCenter

215 Voir http ://www.facebook.com/safety/groups/law/guidelines/

À l´intention des services répressifs étrangers, les directives de Facebook indiquent qu´une demande d´entraide judiciaire ou une commission rogatoire adressée à ce pays d´Amérique du nord peut être nécessaire pour que les contenus d´un compte Facebook[216] soient divulgués. En effet, les intérêts de l´état où sont stockées les données dans les nuages perdent leur pertinence par rapport aux intérêts de l´état où sont contrôlées les données.[217]

Ces difficultés ont été mentionnées par les pays lors de la collecte des informations pour l´étude. Lorsqu´on leur demanda de donner des détails sur l´obtention de preuves électroniques des fournisseurs de services localisés dans d´autres juridictions, de nombreux pays commentèrent que le processus d´obtention de données extraterritoriales était long et qu´il était difficile de localiser « *des autorités étrangères ayant l´autorité juridique et l´expertise technique requises dans les lieux où les preuves numériques étaient physiquement localisées* ».[218]

Les approches régionales et internationales

La difficulté relative à l´obtention de preuves extraterritoriales détenues par des tierces parties a été reconnue depuis longtemps. Lors de l´élaboration de la Convention sur la cybercriminalité du Conseil de l´Europe, l´Article 32 a été inclus, afin de permettre aux parties, sans l´autorisation d´une autre partie, de : (a) accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou(b) accéder à, ou recevoir au moyen d »un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, 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.[219] Un article a également été inclus, dans des termes presque identiques, dans la Convention de la Ligue des états arabes.[220]

Étant donné que l´obtention de données extraterritoriales est particulièrement importante pour les enquêtes des services répressifs, cette analyse est axée sur les mesures décrites par l´article 32(b) de la Convention sur la cybercriminalité du Conseil de l´Europe (accès aux données stockées avec le consentement préalable). Ces mesures sont communément nommées « accès transfrontalier ».

L´Article 32(b) est rédigé en termes permissifs car il prévoit que les états partiesà la Convention sur la cybercriminalité du Conseil de l´Europe *peuvent* prendre ces mesures. Il n´interdit pas directement aux états parties d´empêcher d´autres états parties d´accéder aux données stockées sur leur territoire – mais si un état partie le fait, cela serait considéré incompatible avec l´esprit de l´Article. L´accès « *sans autorisation* » d´un autre état partie est interprété comme « *un accès unilatéral aux données informatiques stockées dans un autre état partie sans solliciter une entraide* ».[221] L´Article est silencieux sur la notification à l´autre état partie – sans l´interdire ni la requérir. Il faut aussi signaler que l´Article 32(b) concerne l´accès à, ou la réception de « données informatiques » stockées en général, et ne se limite pas au contexte des enquêtes sur la cybercriminalité. À cet égard, l´Article 32(b) constitue une règle permettant l´exercice du pouvoir de l´état sur le territoire d´un autre état avec les exceptions prévues par les lois internationales.[222] Par ailleurs, un tel accès est incompatible avec le principe de souveraineté et de non-ingérence, s´il est réalisé sans le consentement de l´état sur le territoire duquel les données sont stockées.[223] Un troisième point de vue est que ces mesures ne répondent pas au critère d´ »ingérence » dans les affaires internes ou externes de l´état sur le territoire duquel les données sont stockées.[224]

---

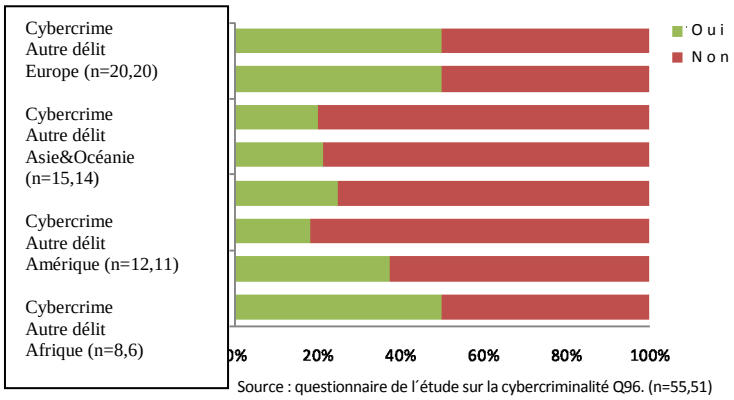
216 *Ibid.*
217 Sieber, U., 2012. *Straftaten und Strafverfolgung im internet. Gutachten C zum 69. Deutschen Juristentag.* Munich : C.H. Beck.
218 Questionnaire de l´étude sur la cybercriminalité Q105.
219 Voir la Convention sur la cybercriminalité du Conseil de l´Europe, Art. 32.
220 Voir la Convention de la Ligue des états arabes, Art. 40.
221 Comité de la Convention sur la cybercriminalité du Conseil de l´Europe (T-CY), sous-groupe ad-hoc sur la juridiction et l´accès transfrontalier aux données, 2012. *L´accès transfrontalier et la juridiction : quelles sont les options ?* T-CY (2012)3. 6 décembre, p.21.
222 *Ibid.* At p.27, cite « *une règle permissive dérivée d´une convention ou d´une coutume internationale* » incluse dans l´affaire *Lotus*, PCIJ Séries A., n°.10, à 18 (1927).
223 Sieber, U., 2012. *Straftaten und Strafverfolgung im internet. Gutachten C zum 69. Deutschen Juristentag.* Munich : C.H. Beck.
224 Comité de la Convention sur la cybercriminalité du Conseil de l´Europe (T-CY), sous-groupe ad-hoc sur la juridiction et l´accès transfrontalier aux données, 2012. *L´accès transfrontalier et la juridiction : quelles sont les options ?* T-CY (2012)3. 6 décembre, p.27.

L´informatique en nuage n´était certainement pas aussi développée au moment de l´élaboration de l´Article 32 de la Convention sur la cybercriminalité du Conseil de l´Europe. Néanmoins, les rédacteurs ont spécifiquement prévu l´application de l´Article 32(b) à, entre autres, une situation où « *les courriels d´une personne peuvent être stockés par le fournisseur de services dans un autre pays* ».[225] L´Article 32(b) est donc applicable à un vaste panel de circonstances, qui incluent l´accès à, ou la réception de données informatiques de personnes, d´organisations du secteur privé, de fournisseurs de services et d´opérateurs de services informatiques en nuage localisés hors du pays. Un avantage potentiel de l´Article 32(b) pour les services répressifs est que, s´il y a un consentement volontaire et légal, les enquêteurs n´ont pas à suivre les procédures d´entraide judiciaire qui sont trop lentes pour capturer les données transitoires.

Pratique nationale

Lors de la collecte des informations pour l´ étude, on demanda aux pays si « l´accès transfrontalier à des données ou un système informatiques » était utilisé comme une mesure d´enquête,[226] et si « l´accès transfrontalier à un système ou des données informatiques dans le pays par des services répressifs étrangers était autorisé.[227]

Figure 7.17 : utilisation de l´accès transfrontalier par la police pour des enquêtes en matière de cybercriminalité et sur d´autres délits



Source : questionnaire de l´étude sur la cybercriminalité Q96. (n=55,51)

Pour ce qui concerne l´utilisation de l´accès transfrontalier par les services répressifs, environ 20 % des pays d´Amérique, d´Asie et d´Océanie ont signalé que ces mesures étaient utilisées lors des enquêtes en matière de cybercriminalité ou sur d´autres délits. Ceci s´élève à environ 40 % des pays répondants en Afrique, et 50 % en Europe.[228] Le pourcentage plus élevé en Europe pourrait refléter l´influence de l´Article 32(b) de la Convention sur la cybercriminalité du Conseil de l´Europe.

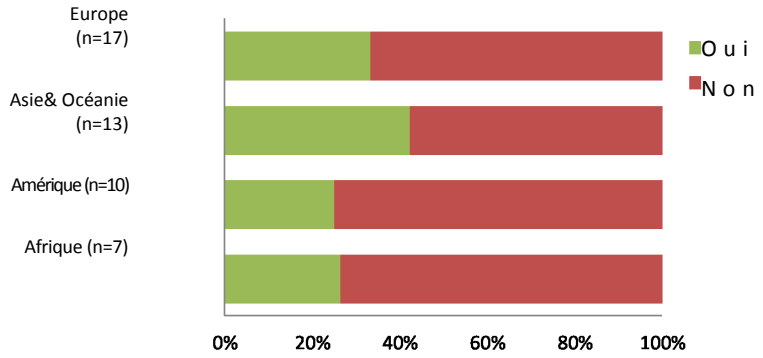
Lorsqu´ils répondirent au questionnaire, les pays attribuèrent une signification large au terme accès « transfrontalier » – y compris le cas où il y eut un accès direct à des données extraterritoriales mais seulement après que les autorités étrangères aient donné leur approbation.[229] De nombreux pays mentionnèrent des restrictions spécifiques dans la pratique, comme la nécessité d´obtenir le consentement du propriétaire, les conditions de notification et l´obligation de s´assurer que les données sont vraiment stockées à l´étranger. La principale raison citée pour ne pas utiliser cette pratique est le manque d´un cadre juridique. Certains pays ont notamment indiqué qu´ils étaient tenus de présenter une demande d´entraide judiciaire ou une commission rogatoire pour collecter des preuves à l´étranger.[230]

Pour ce qui concerne l´interception passive des sites où un pays surveille les communications sans fil d´un pays étranger, voir aussi la demande n°. 54934/00. 29 de la ECtHR. de juin 2006, où la cour jugea que le pays répondant n´avait pas agi d´une manière qui représentait une ingérence avec la souveraineté territoriale d´états étrangers protégée par le droit public international.

225 Conseil de l´Europe, 2001. *Rapport explicatif sur la Convention sur la cybercriminalité.*
226 Questionnaire de l´étude sur la cybercriminalité Q96.
227Qquestionnaire de l´étude sur la cybercriminalité Q108.
228 *Ibid.*
229 *Ibid.*
230 *Ibid.*

Pour ce qui concerne le fait de savoir si l´accès aux systèmes et aux données informatiques est permis pour les services répressifs étrangers, environ deux tiers des pays de toutes les régions du monde ont déclaré que cela n´était pas permis.[231] Un pays d´Océanie a, par exemple, déclaré que les services répressifs nationaux pourraient « *accéder aux systèmes et aux données informatiques au nom du pays étranger par le biais d´un processus formel d´entraide judiciaire*, » et l´étendue de l´assistance « *est limitée aux situations où est exécuté un mandat de perquisition dans des installations [nationales] [...],* » et les autorités nationales ne peuvent pas « *accéder aux communications stockées au nom d´un pays étranger* ».[232] D´autres pays considéraient que cette pratique était incompatible avec le principe de souveraineté des états. Bien que les pays autorisent l´accès transfrontalier aux systèmes et aux données informatiques sur leur territoire, ilsont souvent déclaré que ce n´était que pour les fins prévues par la Convention sur la cybercriminalité du Conseil de l´Europe. Un pays a déclaré que la pratique était autorisée sur la base de la réciprocité. Dans d´autres cas, comme pour un pays d´Amérique du sud, la pratique est autorisée « *dans les cas urgents qui concernent un délit grave qui menace la vie ou l´intégrité d´une personne* ».[233] D´autres pays ont signalé que l´accès transfrontalier était autorisé « *si l´affaire menaçait la sécurité nationale* ». Un pays d´Europe du nord a déclaré qu´il autoriserait l´accès « *s´il était impossible de savoir* [*dans quel pays*] *se trouvaient réellement les données* ».[234]

Figure 7.18 : permissibilité d´un accès transfrontalier des services répressifs étrangers aux systèmes ou aux données informatiques



Source : questionnaire de l´étude sur la cybercriminalité Q108. (n=47)

Dans la pratique, il semble que pour obtenir des données extraterritoriales la majorité des pays répondants ont recours à des voies formelles – et ont besoin de demandes d´entraide judiciaire.[235] En général, moins de 10 % ont déclaré prendre contact directement avec les fournisseurs de services extraterritoriaux « la plupart du temps » pour obtenir des preuves comme les données relatives à l´abonné, au trafic ou au contenu.[236] Un pays en Asie de l´ouest a observé que la prise de contact avec des fournisseurs de services extraterritoriaux devait être informelle et, si le fournisseur de services refusait de coopérer, les autorités d´application de la loi devaient recourir aux voies formelles, afin d´obtenir les permissions nécessaires et les données requises.[237]

Conceptualiser l´accès direct aux données extraterritoriales

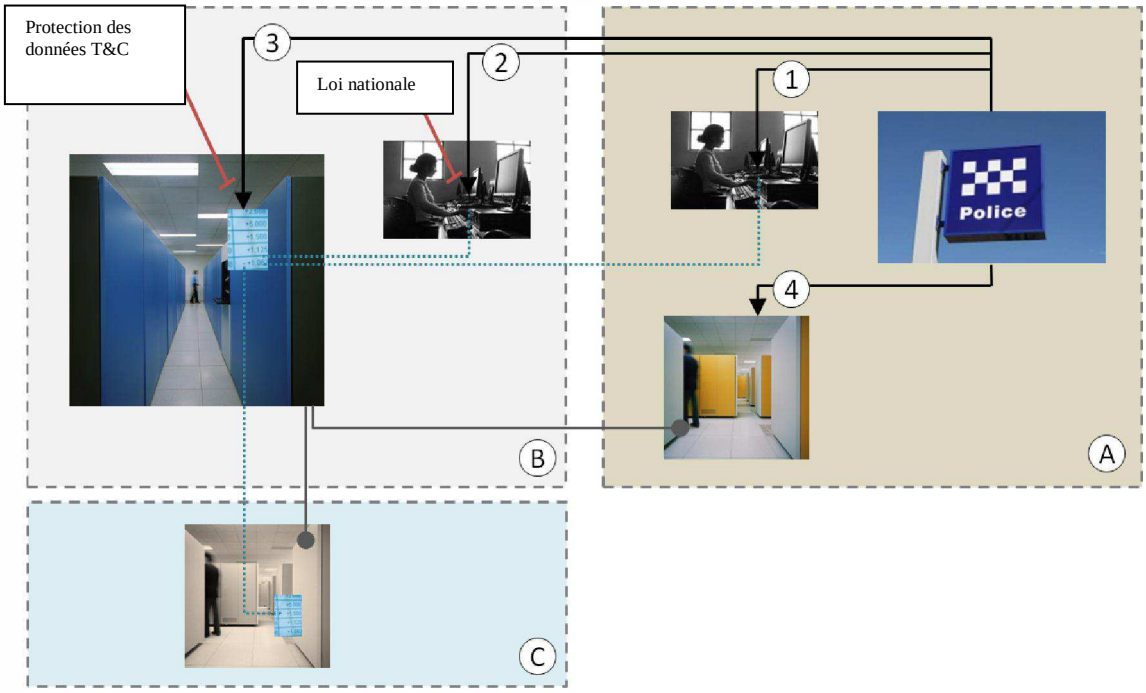
Pour conceptualiser les considérations impliquées dans l´accès aux données extraterritoriales sans une demande formelle d´entraide judiciaire, ou une coopération informelle entre les polices, la figure ci-dessous démontre quatre scénarios possibles dans le contexte de l´informatique en nuage.

L´exemple est basé sur un fournisseur de services informatiques en nuage dont le siège et les centres de données se trouvent dans le pays B, mais qui possède des centres de données additionnels dans le pays C et des bureaux dans le pays A. Les services répressifs du pays A ont accès ou reçoivent des données dans le nuage que l´on croit stockées dans le pays B, via :

231 Questionnaire de l´étude sur la cybercriminalité Q108.
232 *Ibid.*
233 *Ibid.*
234 *Ibid.*
235 Questionnaire de l´étude sur la cybercriminalité Q105.
236 *Ibid.*
237 *Ibid.*

(1) Un individu localisé dans le pays A qui contrôle les données dans le nuage. L´accès peut être obtenu si (i) l´individu y consent ou (ii) les autorités utilisent une connexion en direct existante du dispositif de l´individu.
(2) Un individu localisé dans le pays B qui contrôle les données dans le nuage. L´accès peut être obtenu si l´individu y consent.
(3) Le fournisseur de services informatiques en nuage est localisé dans le pays B. L´accès peut être obtenu si (i) le fournisseur de services informatiques en nuage y consent ou (ii) les identifiants d´accès aux données ont été obtenus par les services répressifs.
(4) Les bureaux du fournisseur de services informatiques en nuage se trouvent dans le pays A. L´accès peut être obtenu par le biais d´arrangements informels locaux entre les services répressifs et le fournisseur de services informatiques en nuage.

Dans toutes ces situations, alors que les services répressifs croient que le fournisseur de services informatiques en nuage détient ces données dans ses centres de données du pays B, il est également possible que les données, ou une copie des données, se trouvent physiquement dans le pays C. Dans d´autres exemples possibles, les services répressifs du pays A pourraient n´avoir aucune information initiale sur la localisation des données– y compris si elles sont physiquement localisées hors du pays ou non.[238]



Le panel de possibilités démontre la complexité de l´accès aux données extraterritoriales pour les services répressifs. Dans l´exemple, il existe aussi d´autres nuances comme : (i) l´effet des conditions générales du client utilisées par le fournisseur de services sur les demandes des services répressifs étrangers ; (ii) dans le pays B, la légalité des interactions entre les services répressifs étrangers, et les individus et les personnes morales sur le territoire et (iii) dans le pays A, la légalité de la manière dont les identifiants d´accès ont été obtenus par les services répressifs.

La considération d´une gamme de scénarios similaires dans un rapport récent du Conseil de l´Europe révéla de nombreuses différences dans les approches des états.

238 Lors de l´accès direct à un dispositif du suspect, il n´est pas clair si les données sont stockées (ou « cachées ») localement sur le dispositif ou si on y a accès par le biais d´une connexion réseau à un serveur sur le territoire, ou par le biais d´une connexion réseau à un serveur hors du territoire.

Ces considérations se référaient à : s´il était évident pour les enquêteurs que les données soient stockées dans différentes juridictions ; si les enquêteurs étaient autorisés à obtenir l´accès à distance avec des logiciels tels que les enregistreurs de clés et les renifleurs ; si la personne qui a fourni l´accès était légalement habilitée à divulguer les données conformément au droit du pays où les données étaient stockées ; et si le fait que la personne qui fournit l´accès se trouve physiquement dans le pays requérant ou si elle est localisée dans un autre pays, marque une différence.[239]

Considérations essentielles

L´exemple conceptuel examiné précédemment ainsi que les réponses fournies par les pays au questionnaire de l´étude, mettent l´accent sur de nombreuses considérations essentielles.

Il semble tout d´abord que les services répressifs peuvent, dans la pratique, avoir un accès direct à des données extraterritoriales *sans le consentement* d´une personne ou du fournisseur de services. Ceci pourrait avoir lieu lorsque les enquêteurs utilisent une connexion en direct existante d´un dispositif du suspect ou lorsque les enquêteurs utilisent des identifiants d´accès aux données obtenus légalement pour accéder aux données en nuage.

D´autre part, les services répressifs qui prennent ces mesures ne savent pas toujours *si* l´accès aux données est vraiment extraterritorial ou, lorsque c´est le cas, le ou les pays dans *lesquels* les données sont physiquement localisées. Ceci peut arriver lorsque, par exemple, des fournisseurs de services informatiques dans le nuage stockent des données dans de multiples copies dans des centres de données de divers pays et utilisent une gestion dynamique des données entre ces centres de données.

Ces deux points sont importants pour les approches régionales et internationales existantes, comme les dispositions de l´Article 32(b) de la Convention sur la cybercriminalité du Conseil de l´Europe et l´Article 40(2) de la Convention de la Ligue des états arabes – qui requièrent le *consentement* d´une personne légalement habilitée à divulguer les données, et se limitent à prévoir l´accès aux données *localisées dans un autre état partie*. Ces dispositions ne couvrent pas le cas où le consentement n´est pas obtenu et où les données sont physiquement localisées dans un pays qui n´est pas partie à un instrument pertinent. En ce qui concerne notamment la question du *consentement* et des fournisseurs de services informatiques en nuage – plusieurs pays répondants ont indiqué que les fournisseurs de services qui opèrent dans leur juridiction sont tenus de divulguer les données seulement sur la signification d´une ordonnance du tribunal, d´une citation à comparaître ou d´un mandat.[240] Ces obligations s´appliquent également –si ce n´est davantage – aux demandes des services répressifs étrangers. De nombreux fournisseurs de services qui ont répondu au questionnaire de l´étude ont déclaré qu´ils ne considéraient pas que les demandes informelles des services répressifs étrangers créaient des obligations de divulgation des données.[241] Dans l´ensemble, les entreprises qui ont répondu au questionnaire de l´étude ont déclaré qu´ils préféraient recevoir des demandes formelles basées sur des traités d´entraide judiciaire. L´examen des directives des fournisseurs de services en ligne illustre aussi cette approche. Par exemple, les directives de Twitter stipulent que *« ...la loi autorise Twitter à répondre aux demandes de renseignements relatives aux usagers émanant d´organismes étrangers d´application de la loi envoyées par ...le tribunal ou par le biais d´un traité d´entraide judiciaire ou d´une commission rogatoire* ».[242] Ainsi, il peut être difficile pour les services répressifs étrangers d´obtenir des données avec le consentement direct d´un fournisseur de services extraterritorial. Un autre point à ajouter à un équilibre complexe est que des arguments relatifs à la souveraineté et à la vie privée suggèrent que l´accès à des données informatiques extraterritoriales est approprié seulement dans le cadre de procédures d´entraide judiciaire – qui entraînent un examen formel de ces questions au cas par cas.[243]

239 Comité de la Convention sur la cybercriminalité du Conseil de l´Europe (T-CY), sous-groupe ad-hoc sur la juridiction et l´accès transfrontalier aux données, 2012. *L´accès transfrontalier et la juridiction : quelles sont les options ?* T-CY (2012)3. 6 décembre 2012. p.29-31.

240 Questionnaire de l´étude sur la cybercriminalité Q21.

241 Questionnaire de l´étude sur la cybercriminalité (secteur privé). Q28.

242 voirhttp ://support.twitter.com/articles/41949-guidelines-for-law-enforcement#

243 Cette recommandation a été faite par l´Initiative mondiale des réseaux, 2012. *La liberté numérique dans le droit international : des mesures pratiques pour protéger les droits de l´homme en ligne.*

D´autre part, la réalité montre que, *dans la pratique*, par de nombreux moyens, les services répressifs ont un accès direct aux données extraterritoriales lors des enquêtes – que les enquêteurs en aient connaissance ou pas. Ceci est motivé par les longs délais requis par les procédures de coopération formelle ; les situations où l´on trouve des dispositifs avec des connexions en direct et où les identifiants d´accès sont révélés au cours de l´enquête.

Les approches actuelles régionales et internationales présentent de nombreuses limitations car elles se basent sur le « consentement » et la connaissance présumée de la « localisation » des données. En réalité, la véritable localisation des données est rarement connue au début d´une enquête ou au moment où l´accès aux données peut être requis. Même si des demandes formelles d´entraide judiciaire sont utilisées, celles–ci peuvent être adressées à la juridiction dont relève le siège du fournisseur de services informatiques en nuage, plutôt que la juridiction correspondant au centre de données physique.[244]

Du point de vue de la justice pénale et de la prévention des délits, il existe de nombreuses circonstances dans lesquelles un accès urgent à des données en nuage peut être requis – comme lorsqu´il existe une menace imminente de préjudices. Atteindre un consensus sur la manière la plus efficace d´atteindre les objectifs tout en veillant au respect des droits de l´homme[245] requiert les actions suivantes : (i) redéfinir la mesure dans laquelle la localisation des données peut continuer à être utilisée comme un principe directeur ; et (ii) développer des garanties et des normes communes relatives aux circonstances dans lesquelles les services répressifs peuvent avoir un accès direct aux données extraterritoriales

244 Les accords entre les opérateurs des centres de données appartenant à des entreprises mondiales et les pays hôtes pourraient probablement traiter ce point.

245 Voir le chapitre cinq (application de la loi et enquêtes), Section 5.3vie privée et mesures d´enquêtes.

Page intentionnellement laissée vierge

CHAPITRE HUIT : PRÉVENTION

Ce chapitre procède à un examen global de la prévention de la cybercriminalité à partir des points de vue des gouvernements, du secteur privé et du milieu universitaire. Il expose des liens importants entre ces intervenants et met l´accent sur diverses interactions entre eux qui peuvent mettre en œuvre des mesures efficaces pour la prévention de la cybercriminalité.

8.1 Les stratégies nationales et la prévention de la cybercriminalité

PRINCIPAUX RÉSULTATS :

- près de 40 % des pays qui ont répondu ont signalé l´existence de politiques ou de lois nationales sur la prévention de la cybercriminalité. Des mesures sont en cours dans près de 20 % des pays ;
- les bonnes pratiques en matière de prévention de la cybercriminalité incluent la promulgation de la législation, un leadership efficace, le développement de la capacité d´application de la loi et de justice pénale, l´éducation et la sensibilisation, le développement d´une solide base de connaissance, et la coopération entre le gouvernement, les communautés, le secteur privé et au niveau international ;
- près de 70 % de tous les pays ont mentionné des stratégies nationales qui incluaient des éléments de sensibilisation, de coopération internationale et de capacité d´application de la loi ;
- plus de 50 % des pays répondants ont mentionné avoir établi des partenariats public-privé pour prévenir et lutter contre la cybercriminalité.

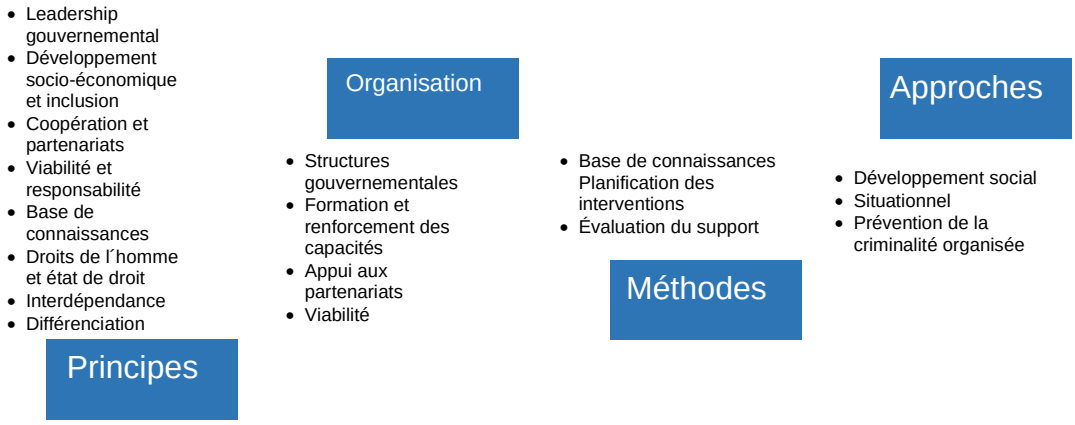
Introduction à la prévention de la criminalité

La prévention de la criminalité fait référence aux mesures et aux stratégies qui visent à réduire le risque de commettre des délits, et leurs potentiels effets nocifs sur les individus et la société, par le biais d´interventions qui influent sur les multiples causes de criminalité.[1]Les principes directeurs applicables à la prévention du crime des Nations Unies soulignent le fait que le leadership du gouvernement joue un rôle important dans la prévention de la criminalité, ainsi que la coopération et le partenariat entre les ministères et les autorités, les organisations communautaires, les organisations non-gouvernementales, le milieu des affaires et les citoyens.[2]Une bonne pratique en matière de prévention de la criminalité commence avec des principes basiques (comme le leadership, la coopération, et l´état de droit), suggère des formes d´organisation (comme des plans de prévention de la criminalité), et met en œuvre des méthodes (comme le développement d´une base de connaissances solide) et des approches (qui incluent la réduction des opportunités criminelles et le durcissement des cibles).

1 *Principes directeurs pour la prévention du crime*, annexe à la Résolution2002/13 du Conseil économique et social des Nations sur *les actions pour promouvoir une prévention efficace de la criminalité* ,24 juillet 2002, para. 3.

2 *Ibid.* Arts. 7 and 9.

Figure 8.1 : principes de la prévention de la criminalité, organisation, méthodes et approches

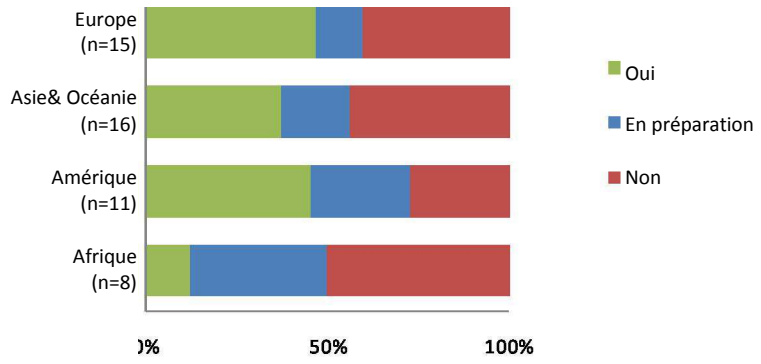


La cybercriminalité présente des difficultés particulières en matière de prévention des délits. Ceci inclut l´omniprésence et la disponibilité croissantes des dispositifs en ligne qui donnent lieu à un grand nombre de potentielles victimes ; la disposition des personnes à assumer des risques en ligne ; la possibilité d´anonymat et les techniques d´obfuscation utilisées par les délinquants ; le caractère transnational de divers actes de cybercriminalitéet le rythme rapide des innovations criminelles. Chacune de ces difficultés a des implications pour l´organisation, les méthodes et les approches adoptées pour prévenir la cybercriminalité. Les structures organisationnelles devront, par exemple, refléter le besoin de coopération régionale et internationale en matière de prévention de la cybercriminalité. Les méthodes devront veiller à être constamment actualisées dans le domaine des menaces de la cybercriminalité, et les approches devront impliquer de nombreux intervenants – en particulier des organisations du secteur privé qui détiennent et opèrent des services et des infrastructures d´internet.

Approches nationales de la prévention de la cybercriminalité

L´établissement d´un plan de prévention de la criminalité avec des priorités et des cibles claires fait partie intégrante de l´aspect organisationnel de la prévention de la criminalité.[3] Les directives pour la prévention de la criminalité stipulent que les gouvernements devraient inclure la prévention comme une partie permanente de leurs structures et leurs programmes de contrôle de la criminalité, et s´assurer qu´il existe au sein du gouvernement des responsabilités et des objectifs clairs pour organiser la prévention de la criminalité.[4]

Figure 8.2 : législation ou politique nationale pour la prévention de la cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité Q8. (n=50)

3 *Principes directeurs pour laprévention du crime*, annexe àla résolution 2002/13 du Conseil économique et social des Nations Unies sur les *Actions pour promouvoir une prévention efficace de* la criminalité, 24 juillet 2002, para. 17.

4 *Ibid.*

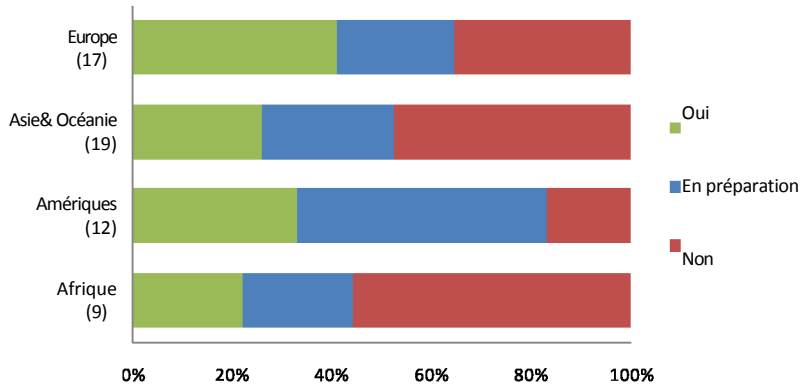
Lors de la collecte des informations pour l´étude, environ 40 % des pays répondants indiquèrent l´existence d´une législation ou d´une politique nationale sur la prévention de la cybercriminalité,[5] et 20 % des pays indiquèrent que cette loi ou cette politique était en cours de développement. Les pays qui mentionnèrent l´existence d´une loi ou d´une politique sur la prévention étaient le plus souvent des pays d´Europe et d´Amérique. Quelques pays d´Afrique mentionnèrent l´existence d´une loi ou d´une politique sur la prévention, et environ 40 % des pays répondants d´Afrique déclarèrent que cet instrument était en cours d´élaboration. Cependant, le fait que plus de la moitié de tous les pays répondants déclara qu´il n´y avait aucune loi ni politique en matière de prévention de la cybercriminalité, indique un potentiel significatif pour consolider les mesures dans ce domaine. Les pays qui disposent de lois ou de politique en matière de prévention de la cybercriminalité, ont déclaré que ces lois ou ces politiques étaient généralement conçues pour « *organiser et coordonner l´environnement juridique, pour établir des systèmes institutionnels efficaces et coordonnés, pour assigner des responsabilités relatives à divers aspects de la cybercriminalité et pour préparer des programmes de sensibilisation destinés aux utilisateurs, au personnel technique et aux décideurs.*[6] D´autres pays mentionnèrent aussi que les lois sur la prévention avaient fixé les rôles et les responsabilités des institutions publiques, des fournisseurs de services et des organisations non-gouvernementales dans les programmes de prévention de la cybercriminalité. De nombreux pays – développés et en voie de développement – ont mentionné les activités spécifiques de sensibilisation ou de la prévention de la cybercriminalité qu´ils ont réalisées, en incluant les activités entreprises par le biais des services répressifs et d´autres institutions gouvernementales, et des organisations du secteur privé et du milieu universitaire. Un pays d´Amérique du sud a, par exemple, mentionné le travail réalisé avec des fournisseurs de services internet et des cafés internet sur la conformité aux règlements, ainsi que des activités de réduction de risques dans des communautés spécifiques avec la création de comités pour la prévention de la criminalité visant à promouvoir la prévention des cyberdélits.[7] D´autres pays mentionnèrent le travail réalisé avec des institutions bancaires pour renforcer la sécurité sur internet, le développement de formations sur la cybersécurité dans le cadre de partenariats avec des organisations non-gouvernementales dans les écoles et la participation des services répressifs à des conférences et des forums sur la cybercriminalité.[8] Les pays ont aussi mentionné l´importance de désigner un point de contact facilement accessible pour que les entreprises et les citoyens puissent signaler des actes de cybercriminalité et recevoir des conseils pour la prévention. Les activités de sensibilisation en matière de cybercriminalité sont examinées postérieurement dans ce chapitre de manière plus détaillée.

Stratégies de cybercriminalité

Plusieurs pays formulèrent des réponses liées à la prévention de la cybercriminalité dans le contexte général du besoin d´une stratégie nationale contre la cybercriminalité.[9]

Plusieurs pays ont aussi souligné les liens étroits entre les stratégies sur la cybersécurité et contre la cybercriminalité.

Figure 8.3 : existence d´une stratégie nationale contre la cybercriminalité



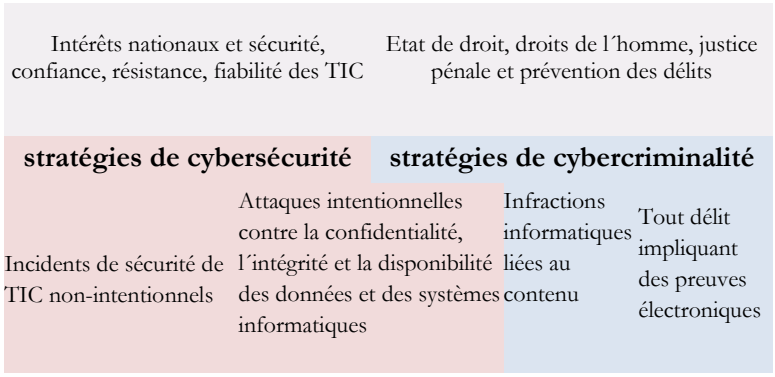
Source : questionnaire de l´étude sur la cybercriminalité

5 Questionnaire de l´étude sur la cybercriminalité Q8.
6 Questionnaire de l´étude sur la cybercriminalité Q8.
7 Questionnaire de l´étude sur la cybercriminalité Q9.
8 *Ibid.*
9 Questionnaire de l´étude sur la cybercriminalité Q1 et Q8.

Aux questions concernant l´existence d´une stratégie nationale (ou son équivalent) contre la cybercriminalité, les pays mentionnèrent des « cyber » stratégies, des stratégies en « cybersécurité », des stratégies sur la « sécurité de l´information », des stratégies sur le « cyberespace » et des stratégies sur la « cybercriminalité ».[10] Ce panel de réponses souligne la croissante interdépendance entre la sécurité des citoyens et la vulnérabilité face à la cybercriminalité, et la sécurité des infrastructures informatiques nationales et celle des entreprises transnationales. Bien qu´il existe un chevauchement important entre les approches de la cybersécurité et de la cybercriminalité, il existe toutefois des différences entre ces deux domaines. Ceux-ci sont résumés dans l´encadré suivant.

Dans la mesure où les pays répondants ont signalé un panel de stratégies pertinentes pour la cybercriminalité, l´analyse dans ce chapitre ne se limite pas à une « stricte » définition d´une stratégie contre la cybercriminalité mais vise à refléter les informations fournies pour le questionnaire de l´étude, en incluant tous les types de stratégies signalés.

Stratégies contre la cybercriminalité et stratégies sur la cybersécurité



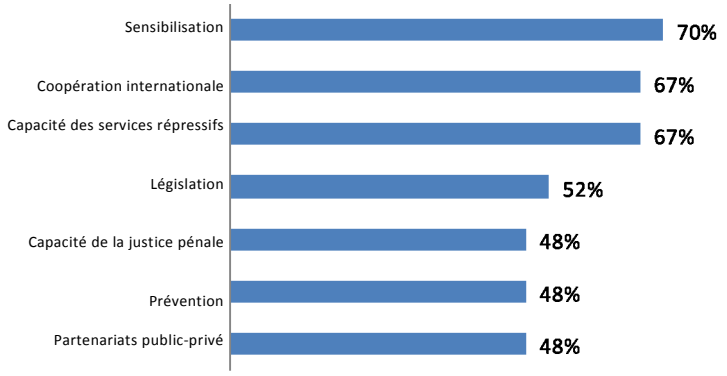
Adapté de Seger, A., 2011. *Stratégies de cybercriminalité, conférence Octopus 2011.*

Environ 30 % des pays répondants ont indiqué l´existence d´une stratégie nationale contre la cybercriminalité (dans le sens le plus large). Selon la région, de 20 à 50 % des pays ont déclaré que ce type de stratégie était en cours d´élaboration. Des pays d´Afrique, d´Asie et d´ Océanie ont mentionné des niveaux plus bas de stratégies contre la cybercriminalité – et 50 % ou plus des pays ont déclaré qu´il n´existait aucun instrument de ce type. Les stratégies contre la cybercriminalité sont importantes pour s´assurer que les ripostes de la justice pénale et des services répressifs nationaux tiennent compte des difficultés particulières propres de la cybercriminalité et des preuves électroniques comme des éléments de tous les délits. Le développement d´une stratégie contre la cybercriminalité représente une première mesure essentielle pour déterminer les priorités opérationnelles et stratégiques avant de s´impliquer dans des processus comme une réforme législative. Comme le démontre la gamme de réponses fournies par les pays, les stratégies contre la cybercriminalité peuvent être préparées comme des documents autonomes ou être incorporées à des stratégies sur la cybersécurité. Lors de la collecte des informations pour l´étude, on demanda aux pays quels étaient les domaines couverts par les stratégies nationales contre la cybercriminalité. Les domaines mentionnés couvraient presque tous ceux qui étaient mentionnés dans l´étude – y compris la prévention de la cybercriminalité et la sensibilisation, la capacité de la justice pénale et des services répressifs, les partenariats public-privé, la législation et la coopération internationale. Pour presque 30 stratégies nationales sur lesquelles des informations avaient été fournies, la prévention des délits était un élément clé. En général, la prévention de la cybercriminalité était incluse dans presque la moitié de toutes les stratégies nationales signalées. De plus, parmi les domaines couverts par ces stratégies, le plus fréquemment cité était l´activité de prévention relative à la « sensibilisation » – et 70 % des stratégies mentionnées incluaient ce thème.[11] La prochaine section de ce chapitre examine ce domaine de manière plus détaillée.

10 Questionnaire de l´étude sur la cybercriminalité Q1.
11 Questionnaire de l´étude sur la cybercriminalité Q1.

Parmi les stratégies nationales contre la cybercriminalité les plus fréquemment citées, venait ensuite la « coopération internationale ». L´importance stratégique de ce domaine, y compris du point de vue de la prévention de la criminalité, a été mentionnée par de nombreux pays. Un pays signalait que : « *la coopération internationale se situe au cœur même* « *des défis exceptionnels que pose une cybercriminalité transnationale, à grande vitesse, sophistiquée et omniprésente à tous les états membres qui doivent équilibrer la nécessité de mesures répressives et de mesures d´enquêtes rapides et efficaces avec la protection de la souveraineté nationale, le respect de la courtoisie et des droits de l´homme dans leur juridiction* ».[12] La coopération internationale en matière pénale concernant la cybercriminalité est analysée de manière détaillée au chapitre sept de cette étude (coopération internationale).La même proportion de pays (presque 70 %) a aussi inclus « la capacité des services répressifs » dans les domaines clés de leur stratégie nationale contre la cybercriminalité. Les difficultés mentionnées liées à la capacité des services répressifs ont été brièvement décrites par un pays comme « *l´équipement, la capacité et les ressources humaines* ».[13] Le chapitre cinq (application des lois et enquêtes) de cette étude examine ce domaine de manière plus détaillée. Parmi d´autres domaines inclus dans les stratégies nationales contre la cybercriminalité figurent la législation sur la cybercriminalité et la capacité de la justice pénale. Il existe une action concertée pour renforcer la capacité et la formation des procureurs, des magistrats et des juges. Quelques pays ont mentionné des plans et des objectifs spécifiques comme désigner « *au moins un procureur public chargé uniquement de traiter les affaires de cybercriminalité dans tous les districts judiciaires d´ici à 2015* »[14] ou de « *créer une équipe d´experts judiciaires du secteur public et du secteur privé pour partager leur expertise et leurs connaissances* ».[15] Le chapitre six (preuves électroniques et justice pénale) examine ce domaine. Un autre thème fréquemment mentionné parmi les priorités de la prévention de la cybercriminalité était l´importance de protéger les infrastructures nationales essentielles. Ceci a été signalé avec le « *développement des informations, des connaissances et des normes de cybersécurité, ainsi que des mécanismes pour identifier et réduire les menaces de la cybercriminalité* ».[16] À cet égard, la coopération entre le gouvernement local et fédéral est décrite comme étant fondamentale « *faciliter le partage des informations relatives aux meilleures pratiques, les informations sur les enquêtes, la coordination des réponses aux incidents, de la gestion des incidents, des procédures et des processus* »[17].

Figure 8.4 : domaines de stratégies nationales contre la cybercriminalité



Source : questionnaire de l´étude sur la cybercriminalité Q1. (n=27, r=108)

Leadership en matière de cybercriminalité

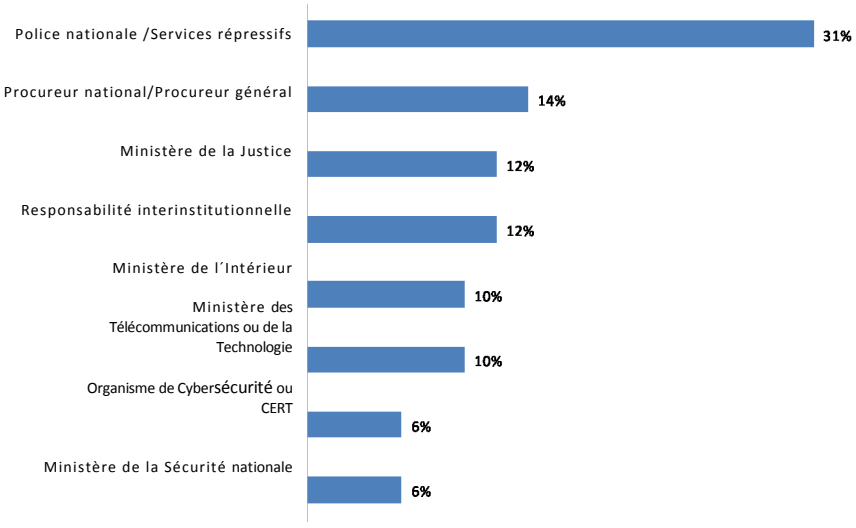
Les pays répondants ont reconnu que plusieurs institutions et organismes gouvernementaux sont requis pour soutenir la prévention de la criminalité et les ripostes de la justice pénale en matière. Cependant, plusieurs pays ont signalé que la prévention de la cybercriminalité requiert un leadership centralisé et des ressources plus importantes pour coordonner les initiatives de prévention de la cybercriminalité du gouvernement.[18]

12 Questionnaire de l´étude sur la cybercriminalité Q4.
13 Questionnaire de l´étude sur la cybercriminalité Q5.
14 *Ibid.*
15 *Ibid.*
16 *Ibid.*
17 *Ibid.*
18 *Ibid.*

Environ 75 % des pays répondants ont déclaré avoir désigné une institution principale gouvernementale chargée de coordonner la prévention et la lutte contre la cybercriminalité.[19] L´institution la plus fréquemment mentionnée (environ 30 % des pays répondants) était la police nationale ou les services répressifs. D´autres institutions principales fréquemment mentionnées étaient le bureau du procureur ou du procureur général et les ministres de la justice. Dans un peu plus de 10 % des pays fut mentionnée une coordination principale interinstitutionnelle.[20]
Pour une faible proportion de pays (10 % ou moins) le rôle de la coordination principale en matière de cybercriminalité reposait sur les ministères des télécommunications, des organismes de cybersécurité ou des équipes d'intervention d'urgence en matière de sécurité informatique (CERT), plutôt que des institutions de justice pénale et de prévention de la criminalité.[21] Les CERT ont un rôle clé pour identifier et réduire les vulnérabilités des systèmes informatiques et pour répondre aux incidents de sécurité informatique.[22] Par conséquent ils possèdent des connaissances importantes sur les tendances actuelles de la cybercriminalité. L´utilisation des ministères des télécommunications et des CERT comme coordination principale en matière de cybercriminalité souligne la nature multidisciplinaire des ripostes à la cybercriminalité.

Il faut cependant noter que, dans l´ensemble, la coordination principale reflète la conception de la cybercriminalité comme un défi dans le domaine d´application de la loi et de la justice pénale, plutôt qu´un défi en matière detechnologie et de communications. Néanmoins, la cybercriminalité possède des éléments de ces deux domaines, et de récents travaux en Europe suggèrent que la coopération entre les CERT et les services répressifs est importante en ce qui concerne les réponses aux incidents et le partage d´informations.[23] Cet aspect a aussi été mentionné par les pays qui ont répondu au questionnaire de l´étude. Les pays ont souvent réitéré l´importance d´une approche de collaboration en raison de la complexité des menaces de la cybercriminalité, y compris envers les infrastructures économiques et essentielles. À cet égard, les difficultés pour coordonner de manière efficace les activités de prévention de la cybercriminalité incluaient le manque de statistiques officielles et de données fiables sur l´étendue de la cybercriminalité, le manque d´une législation pertinente, et le « *manque de partage d´informations, de coordination et de coopération entre les intervenants ainsi que le chevauchement de fonctions des organes gouvernementaux des TI* ».[24]

Figure 8.5 : principales institution pour coordonner les ripostes à la cybercriminalité



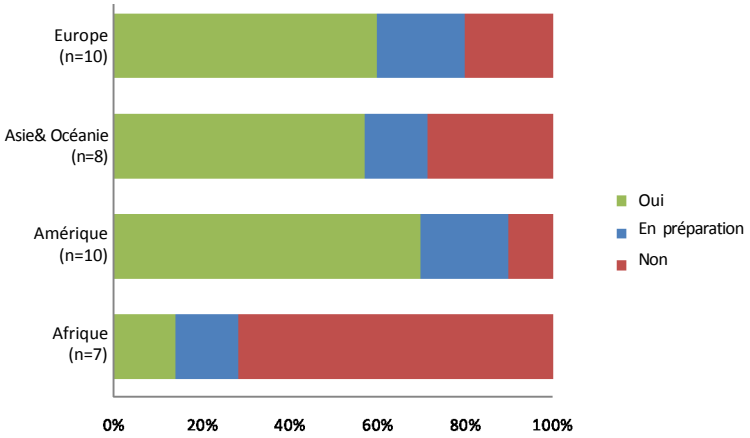
Source : questionnaire de l´étude sur la cybercriminalité Q2. (n=51)

19 Questionnaire de l´étude sur la cybercriminalité Q2.
20 *Ibid.*
21 *Ibid.*
22 Assemblée mondiale de normalisation des télécommunications, 2012. *Résolution 58* - Encourager la création d´une équipe nationale de réponse en cas d´incident informatique, particulièrement pour les pays en voie de développement
23 ENISA, 2012. *La lutte contre la cybercriminalité : la coopération entre les CERT et les organismes d´application de la loi pour la lutte contre la cybercriminalité. Un premier recueil de pratiques*
24. Questionnaire de l´étude sur la cybercriminalité Q5
24 Questionnaire de l´étude sur la cybercriminalité Q5.

Partenariats public-privé

Outre le partenariat et la coordination *au sein* du gouvernement, les pays répondants des différentes régions ont souligné l´importance des partenariats *public-privé*. Plus de 50 % des pays répondants ont mentionné avoir établi des partenariats public-privé pour prévenir et lutter contre la cybercriminalité. Un peu moins de 20 % des pays répondants déclarèrent que ces partenariats étaient en cours de préparation. Environ 30 % des pays répondants déclarèrent qu´il n´y avait aucun partenariat public-privé.[25]

Figure 8.6 : existence de partenariats public-privé



Source : questionnaire de l´étude sur la cybercriminalité Q6. (n=41)

La majorité des pays qui déclarèrent qu´il n´y avait aucun partenariat public-privé étaient localisés en Afrique, en Asie et en Océanie. Plus de 60 % des pays répondants d´Afrique signalèrent l´absence de partenariats public-privé. Cette situation était inversée pour les pays d´Europe et d´Amérique puisque 60 % ou plus des pays répondants signalèrent l´existence de partenariats pertinents.

Les pays mentionnèrent de nombreux facteurs de motivation pour établir des partenariats, y compris la nécessité de comprendre un univers de menaces en constante évolution et d´établir des relations étroites avec les propriétaires et les opérateurs des infrastructures numériques du secteur privé.[26] Lors de la collecte des informations pour l´étude, on interrogea les organisations du secteur privé sur l´existence de partenariats public-privé visant à prévenir et à lutter contre la cybercriminalité. Un peu plus de la moitié des entreprises déclara avoir participé à ces initiatives.[27] Il s´agissait généralement de partenariats avec des organisations internationales, des institutions académiques, des ministères de la justice, des autorités des services répressifs, des ministères de la sécurité nationale et des ministères des télécommunications.[28]

Modèles de partenariats public-privé contre la cybercriminalité

Les cadres juridiques, la confiance, les incitations ainsi que d´autres facteurs sont déterminants pour que de solides modèles de partenariats public-privé pour la cybersécurité prospèrent. Un point de mire approprié est l´analyse du meilleur modèle pour un partenariat fructueux dans un contexte qui puisse minimiser les difficultés et offrir le maximum d´avantages. Cinq grands modèles ont émergé :

- partage des informations à but non lucratif au niveau mondial ;
– partage des informations distribuées au niveau communautaire ;
- partage des informations centralisées au niveau communautaire ;
–au sein du gouvernement ;
- collaboration informelle de l´industrie.

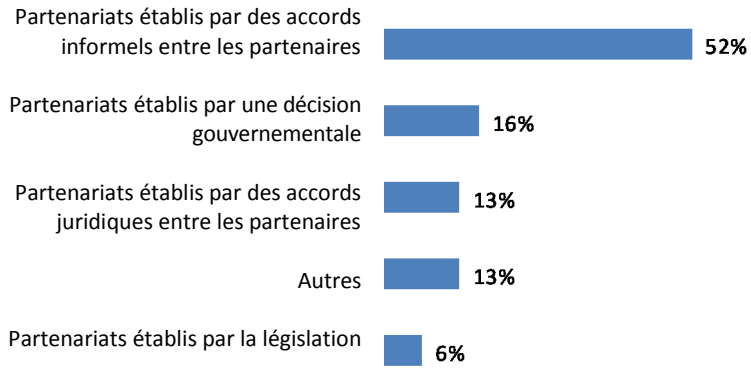
Les caractéristiques principales d´un partenariat fructueux incluent la neutralité pour ce qui concerne la plateforme, l´autorité, des règles relatives au partage des informations, la confiance, une adhésion non ouverte à tous, l´encouragement des bénéfices et de la réactivité.

Source : 17 ECLR 1936, 31 Dec 2012

25 Questionnaire de l´étude sur la cybercriminalité Q6.
26 Questionnaire de l´étude sur la cybercriminalité Q6.
27 Questionnaire de l´étude sur la cybercriminalité (secteur privé). Q40-45.

Les entreprises ont mentionné des expériences positives de partenariats, ainsi que des possibilités d´échanger des informations sur les menaces et les tendances de la cybercriminalité et les considèrent comme une bonne pratique en matière de prévention de la cybercriminalité.[29] Plusieurs entreprises ont aussi mentionné les difficultés relatives à l´établissement et la maintenance des partenariats. Certaines entreprises ont, par exemple, mentionné d´éventuels « *objectifs divergents* » entre le secteur privé et les autorités du gouvernement, et ont expliqué que les partenariats devaient garantir que le « *partage des informations était valable dans les deux sens* ».[30] À cet égard, de nombreuses organisations multinationales du secteur privé ont souligné que les partenariats devaient se concentrer sur des « *solutions mutuelles* » , y compris dans le domaine de la règlementation et de la prévention de la criminalité.[31]

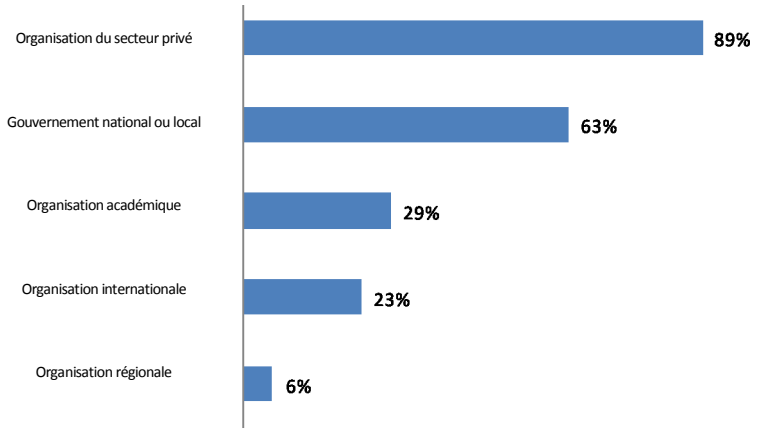
Figure 8.7 : bases des partenariats public-privé



Source : questionnaire de l´étude sur la cybercriminalité Q6. (n=31)

Plus de la moitié des pays répondants a indiqué que les partenariats public-privé sont créés par des accords informels entre les partenaires, et cela indique la nature non contraignante de plusieurs de ces arrangements. Les partenariats établis par le biais d´une décision formelle du gouvernement tendent souvent à concerner des entreprises dont les infrastructures sont essentielles, comme les services publics et les télécommunications.[32] Les autres partenariats mentionnés étaient basés sur des accords juridiques entre les partenaires, ou sur d´autres mécanismes comme des protocoles d´accord et l´adhésion à des « groupes de travail ». La législation était la base la moins fréquemment mentionnée (un peu plus de cinq %) pour l´organisation et le développement des activités de partenariats. Ceci correspond à une utilisation des partenariats public-privé comme une réponse dynamique basée sur des intérêts mutuels, des besoins opérationnels et la nécessité d´une riposte face à l´évolution des tendances de la cybercriminalité.

Figure 8.8 : partenaires des partenariats



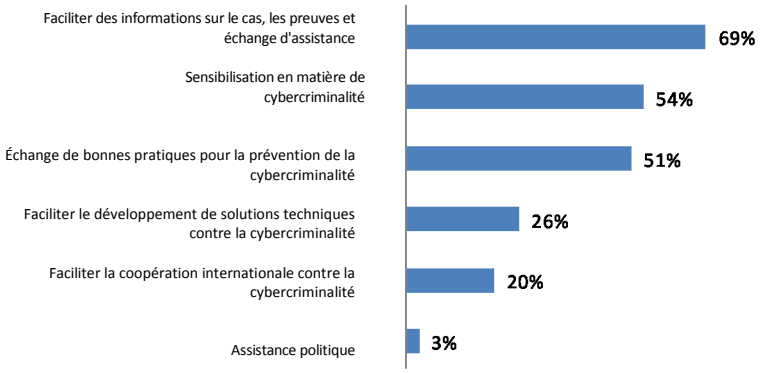
Source : questionnaire de l´étude sur la cybercriminalité. Q6 (n=35, r=73)

28 *Ibid.*
29 *Ibid.*
30 Entretiens de l´étude sur la cybercriminalité (secteur privé).
31 *Ibid.*
32 Questionnaire de l´étude sur la cybercriminalité Q6.

En conformité avec les informations fournies par les organisations du secteur privé, les pays répondants ont déclaré que les entreprises étaient les participants les plus fréquents des partenariats. Environ 90 % de tous les partenariats mentionnés impliquaient le secteur privé, et des organisations académiques, internationales et régionales furent mentionnées par de nombreux pays.

Les objectifs des partenariats reflètent une gamme d´activités. Presque 70 % des partenariats mentionnés par les pays incluaient l´échange d´informations sur la cybercriminalité. Les pays signalèrent, par exemple, que les partenariats étaient utilisés pour « *faciliter la collecte des preuves* et pour la « *détermination concertée de normes et de protocoles de travail* », et pour « *établir des points de contact uniques* ».[33] À la question sur la nature de l´échange d´informations dans ces partenariats, la plupart des pays répondirt qu´il s´agissait d´informations relatives aux menaces et aux tendances de la cybercriminalité ou d´informations générales sur les types de cas de cybercriminalité. La moitié des pays répondants indiqua aussi que les informations échangées incluaient des informations sur des cas *spécifiques* d´actes de cybercriminalité. Comme le mentionnait le chapitre cinq (application des lois et enquêtes), des relations durables et efficaces entre les services répressifs et les fournisseurs de services peuvent être d´une grande utilité pour des enquêtes efficaces en matière de cybercriminalité. Cependant, si ces arrangements impliquent des échanges informels de données personnelles, il est essentiel qu´ils soient aussi en conformité avec l´état de droit et les normes internationales sur les droits de l´homme pour ce qui concerne la certitude juridique et les garanties contre les abus.[34]

Figure 8.9 : portée des partenariats public-privé



Source : de l´étude sur la cybercriminalitéQ6 (n=35, r=78)

D´autres activités communes de partenariats qui furent mentionnées incluaient la sensibilisation en matière de cybercriminalité, l´échange de bonnes pratiques pour la prévention de la cybercriminalité, et faciliter le développement de solutions techniques contre la cybercriminalité.[35] « *Partager les méthodes de bonnes pratiques* », a, par exemple, été cité comme une activité de partenariat par la moitié des pays répondants. Seul un petit pourcentage des états membres a indiqué que les partenariats facilitaient l´assistance pour le développement des politiques. Etant donné les intérêts du secteur privé relatifs au développement mutuel de ripostes contre la cybercriminalité, ceci représente un domaine dans lequel les partenariats public-privé peuvent se développer davantage.

33 Questionnaire de l´étude sur la cybercriminalité Q6.
34 Voir le chapitre cinq, section 5.3 vie privée et mesures d´enquêtes.
35 Questionnaire de l´étude sur la cybercriminalité Q6.

8.2 Sensibilisation à la cybercriminalité

Principaux résultats :

- les sondages, y compris dans les pays en voie de développement, montrent que la plupart des utilisateurs d´internet prend actuellement des précautions basiques en matière de sécurité ;
- tous les intervenants soulignent l´importance constante des campagnes de sensibilisation publiques, y compris celles qui abordent les menaces émergentes et celles qui visent des audiences spécifiques, comme, par exemple, les enfants ;
- l´éducation fournie aux utilisateurs est plus efficace si elle est combinée à des systèmes qui aident les utilisateurs à accomplir leurs objectifs de manière sûre.

La sensibilisation

Les directives des Nations Unies pour la prévention de la criminalité soulignent l´importance de la sensibilisation et de l´éducation du public.[36] Accroître la sensibilisation aux risques de victimisation et aux mesures de protection pouvant être prises représente une stratégie importante pour prévenir tout type de délit.[37] Lors de la collecte des informations pour l´étude, non seulement les gouvernements, mais aussi les organisations du secteur privé soulignèrent l´importance de la sensibilisation en matière de cybercriminalité pour le public et les entreprises. Une grande entreprise de télécommunications a, par exemple, déclaré que : « *nous devons éduquer les gens sur la sécurité basique. Les propriétaires de machines qui n´ont pas de sécurité basique, de correctifs ou de mises à jour laissent leur porte grande ouverte. Cette campagne devrait faire aussi partie du rôle du gouvernement ; nous devons constamment transmettre aux gens le message qu´ils sont leur meilleure protection* ».[38]

Plusieurs pays ont mentionné des initiatives de sensibilisation. Un pays répondant d´Amérique a, par exemple, mentionné l´importance de « *promouvoir les campagnes dans les médias, mettre en œuvre des portails interactifs 24/7 de discussion en ligne,* [*et*] *de renforcer les sites web et les réseaux sociaux* ».[39] De nombreux pays d´Amérique et d´Europe ont aussi mentionné qu´ils avaient développé des stratégies de sensibilisation par le biais de périodes consacrées aux campagnes comme « *le mois de sensibilisation en matière de cybersécurité* » et « *la journée de la sécurité sur internet* ».

Un pays a également déclaré avoir « *créé une page sur Facebook, qui publie... des conseils en ligne sur la cybersécurité et qui a des liens vers un portail pour notifier des plaintes. Il y a aussi le numéro de téléphone 1800-CRIME pour signaler des incidents de cybercriminalité* ». Un pays d´Europe a mentionné que « *les mesures pour améliorer le signalement de cyber délits ont été développées davantage en 2007 avec la création d´un site web spécialisé... le site sert de plateforme d´information à double sens, où une personne peut recevoir des informations relatives aux dangers existants dans l´espace internet mais également signaler le fait de commettre un délit. Les rapports sont directement transmis aux officiers de* [*police*]*... jusqu´à présent environ 150 rapports mensuels sont reçus par le biais de ce site... Après le lancement d´une campagne pour promouvoir le site, il est probable que les visites du site et le nombre de rapports soumis augmenteront* ».[40] Le tableau suivant résume les détails de quatre campagnes de sensibilisation mentionnées lors de la collecte des informations pour l´étude.

36 Principes directeurs des Nations Unies pour la prévention du crime, annexe à la Résolution 2002/13 du Conseil économique et social. Para.6et 25.
37 Voir, par exemple, ONUDC. 2010. Manuel sur les principes directeurs en matière de prévention du crime.
38 Entretien de l´étude sur la cybercriminalité (secteur privé). Juin 2012.
39 *Ibid.*
40 *Ibid.*

Caractéristiques de campagnes de sensibilisation

	Campagne n°1	*Campagne n°2*	*Campagne n°3*	*Campagne n°4*
Fondée et coordonnée par	Gouvernement d´un pays d´Europe du nord	Gouvernement d´un pays d´Océanie	Gouvernement d´un pays d´Amérique du nord	Gouvernement d´un pays d´Amérique du sud
Principales caractéristiques				
Utilisation sûre, vol de ID, escroqueries	☐	☐	☐	☐
Protection des enfants, cyberintimidation	☐	☐	☐	
Contenu préjudiciable (violence, pornographie, racisme)	Sans la protection des enfants	☐		
Secteur privé – campagnes ciblées, y compris le secteur financier (hameçonnage, sécurité, etc.)				
Portée d´internet				
Service public Annonces, films	☐	Campagne du service public		☐
Pages web ciblées	☐	☐	☐	
Jeux interactifs		☐	Navigation sûre en ligne	
Alertes	RSS, Facebook, Twitter	Service de messagerie personnalisé		
Informations des victimes	☐			
Portails dédiés aux signalements	Portail sur les fraudes	Portail Web		Portail Web
Conférences, séances d´information, diffusion				
Pour les citoyens, le public en général	Activité annuelle d´une semaine, campagne de médias	Semaine annuelle de sensibilisation	Mois national de sensibilisation en cybersécurité	Conférence de deux jours
Groupes spéciaux – étudiants, professeurs, professionnels, universitaires, services répressifs et judiciaires	Conférences, forums, meetings		Mois national de sensibilisation en cybersécurité	Sensibilisation scolaire. Formation basique de six semaines sur l´utilisation sécuritaire des TI pour les spécialistes en TI et les étudiants

En 2011 l´examen international des initiatives en matière d´éducation et de sensibilisation sur la cybersécurité a évalué 68 de ces campagnes, qui toutes utilisaient l´internet comme moyen de communication. Plus d´un tiers des campagnes ont produit des publications, et 30 % incluaient des mois, des semaines ou des jours dédiés à la sensibilisation, ainsi que des manuels et des séminaires de formation. Un quart utilisait des vidéos, des jeux ou des quiz. La plupart des campagnes était organisée par des organismes gouvernementaux, et faisaient aussi souvent partie d´un consortium du secteur privé et de partenaires à but non lucratif.[41]

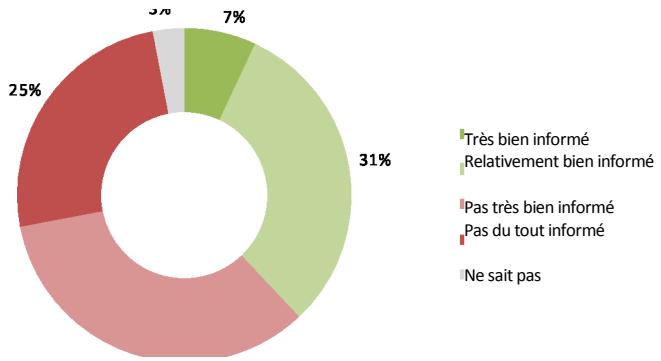
41 Voir http ://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf

Bien que de nombreuses campagnes de sensibilisation soient organisées au niveau national, il existe aussi un petit nombre d´exemples régionaux. Le système européen de partage d´alertes et d´informations a, par exemple, été créé en 2006. Cette campagne a réuni des informations et du matériel éducatif des équipes d´intervention en cas d´urgence informatique et d´autres organismes de sécurité de divers pays d´Europe. Le matériel a ensuite été adapté pour les différents groupes de citoyens et les petites et moyennes entreprises de chaque pays participant. Le matériel fut diffusé par le biais des médias sociaux, des sites web et des listes de diffusion. Le projet pilote à grande échelle qui était axé sur la sensibilisation en matière de botnets, de vol d´identité et de menaces de l´ingénierie sociale atteignit environ 1500 personnes.[42]

Les entreprises de technologie et les groupes sans but lucratif ont également développé leurs propres campagnes de sensibilisation. La campagne « Good to Know » de Google a, par exemple, circulé dans environ 40 langues depuis 2011. Des annonces sur les journaux, les magazines, en ligne et dans les transports publics donnent des conseils de sécurité et expliquent certaines caractéristiques basiques comme les témoins de connexion et les adresses IP.[43] Le FOSI (l´institut pour la sécurité de la famille en ligne) a également travaillé avec des entreprises de technologies pour ajouter des ressources éducatives destinées aux parents, aux enfants et aux enseignants, sur leur plateforme des bons sites web.[44] Kyivstar, un opérateur de télécommunications de l´Europe de l´est, a lancé la campagne « parlez à vos enfants de la sécurité sur internet » en avril 2012, avec des annonces dans la presse écrite, en ligne, sur des véhicules et avec des volontaires qui fournissaient des sessions d´information dans les écoles.[45] Pour une audience plus jeune, Disney a lancé une campagne de sécurité avec la TV, des sites web et des magazines en 2012 destinée à 100 millions d´enfants et leurs parents en Europe, dans le moyen orient et en Afrique.[46] Malgré le nombre croissant de ces campagnes, de nombreux pays considèrent que « *il faudra du temps pour que les campagnes de sensibilisation publique développent la confiance du public pour signaler les actes les actes de cybercriminalité.*[47] L´examen international des campagnes en 2011 a conclu que peu de campagnes incluaient un élément d´évaluation. Il souligna les difficultés relatives au développement de campagnes appropriées et rentables, et signala que le fait de fournir des informations aux utilisateurs sans formation additionnelle et sans activité d´acquisition de compétences avait une incidence limitée sur leur comportement en ligne. L´examen concluait que de simples campagnes axées sur un groupe ciblé spécifique semblaient être les plus rentables.[48]

Il existe donc le besoin de comprendre le comportement sous-jacent à risque des usagers, et les perceptions de risque. Ces informations sont importantes pour concevoir et appliquer des activités de sensibilisation en matière de cybercriminalité, et pour la prévention de la cybercriminalité en général. La section suivante de ce chapitre examine les informations de la population et les sondages des-entreprises dans ce domaine.

Figure 8.10 : vous considérez vous bien informé en matière de risques de cybercriminalité ?



Source : Commission européenne, 2012 , Eurobaromètre spécial390, juillet (p. 37)

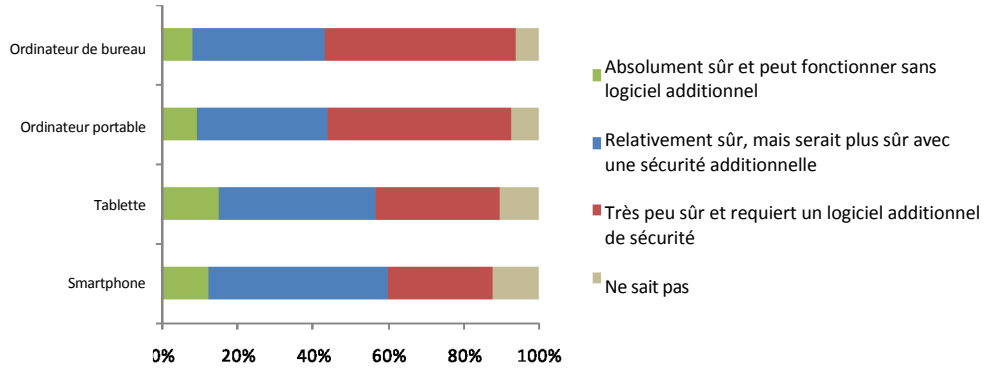
42 Degenhardt, W. 2012. *EISAS projet pilote à grande échelle : sensibilisation concertée pour les citoyens de l´UE & SMEs*, ENISA.
43 Voir http ://www.google.com/goodtoknow/
44 Voir http ://aplatformforgood.org/
45 Voir http ://en.csrukraine.org.ua/?p=367
46 Voir http ://www.guardian.co.uk/technology/appsblog/2012/jul/04/disney-club-penguin-child-safety
47 Questionnaire de l´étude sur la cybercriminalité Q82.
48 Galexia. 2011. Un aperçu de la cybersécurité internationale *Initiatives éducatives et de sensibilisation.* ACMA

Comprendre les comportements à risque des usagers

Les enquêtes de population montrent que de nombreux utilisateurs d´internet, du moins dans les pays les plus développés, sont conscients du risque que représente la cybercriminalité. Un sondage dans les pays européens a, par exemple, révélé que plus de 70 % des personnes avaient entendu ou vu des informations sur la cybercriminalité durant l´année antérieure, qui provenaient généralement de la télévision, de journaux, d´internet, de la radio ou d´amis, de membres de la famille ou de collègues.[49] Néanmoins, recevoir des informations sur la cybercriminalité ne se traduisait pas nécessairement par le fait de « se sentir informé » en matière de cybercriminalité. Seulement 7 % des personnes qui répondirent à cette enquête déclarèrent « se sentir très bien informées » en matière de cybercriminalité. Plus de la moitié déclara « ne pas être du tout informée » ou « ne pas être très bien informée ».

Cependant, les enquêtes suggèrent que la plupart des utilisateurs d´ordinateurs, y compris dans les pays en développement, prend au moins des précautions basiques de sécurité. Lors d´une enquête qui porta sur plus de 13 000 utilisateurs d´internet dans 24 pays, presque 90 % des personnes qui répondirent déclarèrent éliminer les courriels suspects provenant d´expéditeurs inconnus. Environ 80 % déclarèrent utiliser au moins un logiciel antivirus basique, et ne pas ouvrir les fichiers attachés ou les liens des textes ou des courriels non sollicités.[50] Seulement la moitié des personnes qui répondirent utilisaient les paramètres de confidentialité des réseaux sociaux pour contrôler les informations partagées, et environ 35 % avaient accepté des « demandes d´amis » de personnes qu´elles ne connaissaient pas. Faisant écho à ce patron, une autre enquête internationale portant sur presque 4000 utilisateurs d´internet de six pays d´Amérique du nord et d´Europe révéla qu´environ 10 % des utilisateurs de courriels avaient cliqué sur des liens potentiellement risqués de messages non sollicités, et un peu moins de 10 % avait ouvert un fichier attaché d´un message suspect non sollicité.[51] Les enquêtes portant sur des générations plus jeunes de pays moins développés révélèrent des niveaux très élevés de risques de victimisation en matière de cybercriminalité. Une enquête portant sur environ 25 000 enfants en âge scolaire de sept pays d´Amérique centrale et d´Amérique du sud révéla que, sur environ 45 % des enfants qui disposaient d´une connexion à domicile, seulement 10 % des adolescents (10 à 18 ans) mentionnèrent avoir un logiciel de sécurité installé (filtrage du web ou anti-virus) et 20 % ne savaient pas si un logiciel de sécurité était ou non installé.[52] Les comportements à risque et les problèmes de sécurité ne concernent pas les ordinateurs de bureau. Comme le mentionnait le chapitre 1 (connectivité globale), les utilisateurs ont davantage accès à l´internet en utilisant un dispositif mobile plutôt qu´avec des lignes fixes à haut débit. Même si les menaces électroniques sont en recrudescence pour les dispositifs mobiles,[53] la perception des utilisateurs est que les dispositifs mobiles et les tablettes sont plus sûrs que les ordinateurs de bureau.

Figure 8.11 : perception de la sécurité du dispositif



Source : Kaspersky Lab, 2012. Perception et connaissance des menaces de TI (p. 2)

49 Commission européenne. 2012 *Eurobaromètre spécial 390.*
50 Symantec. 2012. *Rapport Norton sur la cybercriminalité 2012.*
51 Groupes de travail contre l´utilisation abusive des messageries (MAAWG), *2010, rapport sur l´utilisation et la sensibilisation sur la sécurité des courriels* New York : Ipsos Public Affairs.Cette enquête a été pondérée pour être représentative de la population en ligne de chaque pays.
52 Fundación Telefónica. 2008. *La generación interactiva en Iboamérica : Niños y adolescentes ante las pantallas.*
53 Voir, par exemple, Symantec. 2012. *Rapport sur les menaces à la sécurité sur internet*, Volume 17.

Une enquête portant sur 11 000 utilisateurs d´internet d´Amérique du nord et d´Amérique latine, d´Europe, du Moyen orient, d´Asie et d´Afrique révéla que 60 % des utilisateurs pensaient qu´ils étaient « sûrs » ou « relativement sûrs » d´utiliser un smartphone sans logiciel additionnel de sécurité alors qu´environ 45 % pensaient la même chose des ordinateurs portables ou des ordinateurs de bureau.[54]

Limites de l´éducation des utilisateurs

Les conseils aux individus concernant la réduction des risques de la cybercriminalité est un élément important de la stratégie générale qui vise à réduire la cybercriminalité. La mesure dans laquelle les utilisateurs pourraient apprendre de complexes mécanismes de sécurité, se souvenir de divers mots de passe pour chaque service en ligne pour lesquels ils se sont enregistrés, et prendre d´autres précautions qui, souvent, affectent directement la tâche à accomplir, a ses limites.[55] Il n´est pas surprenant que de nombreux utilisateurs ne suivent pas les conseils de sécurité car cela représente une charge beaucoup plus lourde que les conséquences probables d´une défaillance de la sécurité. Les chercheurs en matière de sécurité signalent, par exemple, que « *si les utilisateurs consacraient une minute par jour à lire les URL pour éviter l´hameçonnage, le coût (en termes de temps de l´usager) serait de deux ordres de grandeur supérieurs à toutes les pertes causées par l´hameçonnage ».*[56] La compréhension de toutes les différentes manières dont un site d´hameçonnage peut usurper un domaine exigerait un investissement d´éducation et de temps, que la plupart des usagers refuserait logiquement de faire.[57] L´éducation des usagers sera probablement plus efficace si elle est associée à des systèmes qui les aident à atteindre leurs objectifs de manière sécurisée. Ceci devra requérir une confirmation expresse lorsque les usagers tentent d´exécuter des actions qui peuvent compromettre gravement la sécurité de leur système – en installant, par exemple, un logiciel d´origine inconnue. Les coûts des mesures de sécurité pour l´usager devront toutefois être proportionnels aux bénéfices qu´ils apportent – par exemple, les règles de mots de passe complexes requièrent un investissement de la part de l´usager pour se souvenir de mots de passe compliqués, mais pourraient facilement être contournés par des enregistreurs de frappe ou des attaques d´hameçonnage. Quand le coût est plus élevé que les bénéfices directs pour l´utilisateur, les personnes sont fortement incitées à ignorer les mesures de sécurité.[58] Dans les organisations et les entreprises du secteur privé, les processus organisationnels qui promeuvent un comportement de prise de conscience des risques de sécurité chez les employés et les clients sont donc essentiels – en aidant, par exemple, les usagers à choisir au moment opportun des mots de passe sécurisés mais mémorisables, et en réitérant que ces mots de passe ne seront jamais sollicités lors d´un appel téléphonique ou par courriel, ou après avoir cliqué un lien d´un courriel. La culture sociale et organisationnelle devrait éviter d´encourager le point de vue selon lequel une conduite prudente en matière de sécurité est « paranoïaque » ou « pointilleuse » et entrave la productivité. La culture organisationnelle devrait en fait aider à promouvoir et à récompenser les comportements sécuritaires.[59] La section suivante de ce chapitre examine les pratiques de cybersécurité adoptées par les organisations du secteur privé.

54 Kaspersky Lab. 2012. *Perception et connaissance des menaces des TI : le point de vue du consommateur*, p.2.
55 Sasse, M.A., Brostoff, S. et Weirich, D., 2001. Transformer le point faible – une approche de l´interaction homme/ordinateur pour une sécurité efficace et accessible. *Revue de technologie BT*, 19(3) :122-131.
56 Herley, C., 2009. A la prochaine et non merci pour les externalités : le rejet rationel des conseils de sécurité de la part des usagers. Atelier sur les nouveaux paradigmes de sécurité, Oxford.
57 *Ibid.*
58 *Ibid.*
59 Sasse, M.A., S Brostoff et D Weirich (2001) Transformer le point faible – une approche de l´interaction homme/ordinateur pour une sécurité efficace et accessible *revue de technologie BT*, 19(3) :122-131.

8.3 Prévention de la cybercriminalité, le secteur privé et le milieu universitaire

PRINCIPAUX RÉSULTATS :

- les répondants du secteur privé ont mentionné la sensibilisation et diverses actions en matière de cybersécurité. Deux tiers des répondants du secteur privé ont effectué des évaluations de risques en matière de cybercriminalité et la plupart a signalé l´utilisation de techniques de cybersécurité ;
- ils ont cependant mentionné qu´il était préoccupant que les petites et moyennes entreprises ne prennent pas suffisamment de mesures pour protéger les systèmes, en supposant de manière erronée qu´elles ne seront pas une cible ;
- certaines entreprises, dont des fournisseurs de services et des entreprises de technologie, ont pris des mesures proactives pour lutter contre les actes de cybercriminalité, y compris par le biais de mesures juridiques ;
- les fournisseurs de services internet et les fournisseurs d´hébergement peuvent jouer un rôle essentiel dans la prévention de la cybercriminalité. Ils peuvent conserver des journaux qui pourront être utilisés pour enquêter sur des activités criminelles ; aider des usagers à identifier des ordinateurs compromis ; bloquer certains types de contenus illégaux comme le spamet, en général, assurer un environnement de communications sécurisé pour leurs usagers ;
- les institutions académiques sont des partenaires importants dans la prévention de la cybercriminalité, avec le partage et le développement de connaissances, le développement de lois et de politiques ; le développement de normes technologiques et techniques ; la fourniture d´assistance technique et la coopération avec les services répressifs.

Cette section examine trois aspects des relations entre le secteur privé, le milieu universitaire et la cybercriminalité : (i) les approches de cybersécurité adoptées par les organisations du secteur privé ; (ii) les mesures que peuvent prendre les fournisseurs de services internet pour prévenir la cybercriminalité et (iii) le rôle des organisations intergouvernementales et du milieu universitaire dans la prévention de la cybercriminalité.

Les pratiques en matière de cybersécurité des organisations du secteur privé

Lors de la collecte des informations pour l´étude, on interrogea les organisations du secteur privé sur les pratiques de cybersécurité adoptées en vue de prévenir la victimisation de la cybercriminalité. Les informations fournies par les entreprises sont présentées ici avec la référence aux principes directeurs de l´OCDE sur la sécurité des systèmes d´information et des réseaux.[60]Les principes directeurs de l´OCDE ont été reflétés dans une résolution de l´Assemblé générale concernant la création d´une culture mondiale de la cybersécurité,[61] ainsi que dans des instruments régionaux [62]. Ils ont également été utilisés par la Chambre internationale de commerce pour produire un petit guide sur l'« *assurance de la sécurité de l´information pour les dirigeants*, » qui signale que « *toutes les parties ont un rôle à jouer pour ce qui concerne la culture de la sécurité, mais les entreprises, en tant que principal innovateur, développeur, utilisateur et fournisseur des technologies de l´information et la communication (TIC), ont un rôle plus étendu que la plupart* ».[63]

60 Recommandation du Conseil concernant les principes directeurs sur la sécurité des réseaux et des systèmes d´informations – Vers une culture de la sécurité, OCDE, 25 juillet 2002 - C(2002)131/FINAL.

61 Résolution 57/239 de l´Assemblée générale des Nations Unies, 31 janvier2003.

62 Voir, par exemple, Conseil de l´Europe :Résolution du Conseil sur une approche européenne axée sur une culture de la sécurité des réseaux et de l´information, 15723/02, 28 Jan 2003 et la stratégie de l´APEC pour assurer un environnement en ligne fiable, sûr et durable, approuvée par les responsables en Nnovembre 2005.

63 Voir http ://intgovforum.org/Substantive_1st_IGF/Information.security%20assurance.pdf

Les principes directeurs de l´OCDE mentionnent trois groupes de principes de cybersécurité, (i) les principes de base (ii) les principes sociaux et (iii) les principes de cycle de vie de la sécurité. Ceci représente la base de l´organisation des approches en matière de prévention de la cybercriminalité mentionnées par les entreprises du secteur privé.

Les principes de base – les principes de base en matière de cybersécurité concernent l´importance de la sensibilisation organisationnelle aux risques ; la responsabilité d´agir en conformité avec cette sensibilisation et les processus de coordination et d´apprentissage pour prendre des mesures en cas d´incidents.

Lors de la collecte des informations pour l´étude, les répondants du secteur privé mentionnèrent l´importance d´une approche holistique de la sécurité dans l´entreprise. Un dirigeant d´entreprise commenta : « *beaucoup d´assureurs demandent des choses très spécifiques, comme « avez-vous des pare-feu, avez-vous un cryptage ou avez-vous un logiciel antivirus », mais ce que nous cherchons vraiment à savoir est si la sécurité fait partie intégrante des décisions commerciales prises par une entreprise potentiellement assurée, et ceci est très difficile à évaluer, car de nombreuses entreprises font le minimum nécessaire pour protéger les données, mais la protection des données n´est pas vraiment une priorité pour elles... lorsqu´on considère la sécurité et la confidentialité comme des fonctions séparées de tout le reste et autonomes, cela n´est pas efficace* ».[64] Un fabricant d´équipement ajouta : « *les entreprises ont besoin d´un programme de gestion des risques et de mettre en place des pratiques et des politiques pour gérer les risques de manière transparente...la capacité de vérifier la conformité en temps réel rend la fonction d´audit moins coûteuse* ».[65]

Les répondants ont aussi souligné le besoin de leadership au niveau du conseil. Un fabricant d´équipement déclara : « *je ne pense pas que, qui que ce soit, ait réellement établi les exigences de diligence raisonnable que nous devons suivre. Pour ce qui concerne le conseil d´administration, vous devez savoir ce dont vous devez vous soucier, vous devez savoir si votre entreprise suit ou non les pratiques recommandées qui constituent des diligences raisonnables dans votre pays. [...] ils n´exerceront donc pas seulement le contrôle financier mais ils vérifieront aussi les systèmes d´informations afin de s´assurer d´être en conformité avec les meilleures pratiques* ».[66] Une entreprise de services de technologies de taille moyenne déclara : « *la plupart des institutions dispose de quelques personnes qui sont conscientes des menaces et des personnes qui sont conscientes des données que l´institution collecte, le problème est que très peu de personnes ont conscience des deux* ».[67]

La plupart des intervenants du secteur privé qui répondirent au questionnaire de l´étude dit qu´ils traitaient la question de la sensibilisation aux risques par le biais de la formation des employés, avec des politiques et en supervisant l´utilisation et l´accès des employés, des clients et des tierces parties. Ces mesures étaient développées universellement au niveau interne et les coûts d´application variaient en fonction de la taille de l´organisation. Elles incluaient des éléments comme la diffusion des informations relatives aux plus récentes menaces et aux limites des solutions techniques.[68]

Plusieurs répondants commentèrent que dans de nombreuses entreprises la formation n´était pas suffisamment efficace, bien qu´une entreprise internationale de services signala que « *les fondements de la pratique [de sécurité et de confidentialité de l´information] sont de plus en plus enracinés* ».[69] Le responsable de la sécurité d´une entreprise de technologie de taille moyenne déclara que : « *la plupart des menaces provient, en réalité, des erreurs humaine et de l´ingénierie sociale. Des utilisateurs peu sophistiqués peuvent être ciblés pour obtenir un accès à l´entreprise. C´est l´un des principaux problèmes sur lesquels nous travaillons.*

Si les institutions bénéficiaient d´une formation adéquate et si des politiques étaient en place, cela

n´arriverait pas. La prévention est donc essentielle ».[70] Une entreprise internationale de télécommunications considérait que : « *la principale difficulté est que tous les employés suivent les règles basiques d´utilisation* ».[71]

Bien que la sensibilisation aux risques ait augmenté, certains répondants ont déclaré que cela n »entraînera pas un changement immédiat dans les comportements. Un fabricant d´équipement commenta : « *je pense qu´il y a beaucoup de publicité sur les menaces, mais les gens doivent associer les menaces avec leur responsabilité personnelle et la responsabilité de l´entreprise* ».[72] Une entreprise de services déclara : « *je pense qu´il existe une sensibilisation parmi les gens de l´industrie qu´il n´y avait pas antérieurement, mais de nombreuses personnes n´ont pas ces connaissances.*

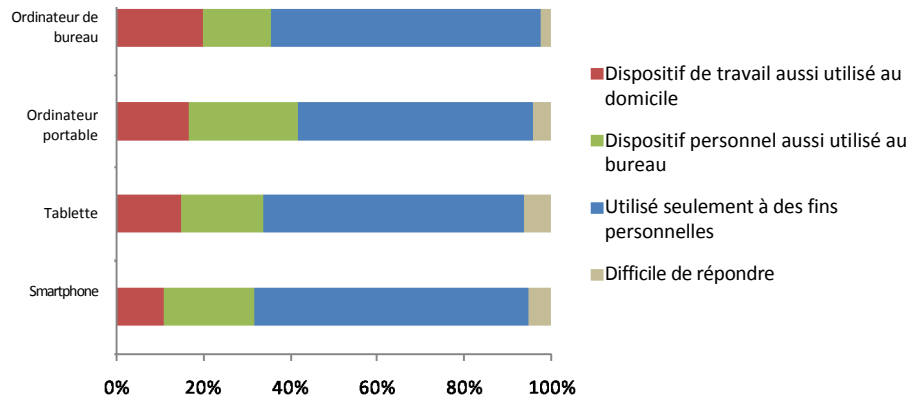
64 Entretien de l´étude sur la cybercriminalité (secteur privé).
65 Entretien de l´étude sur la cybercriminalité (secteur privé).
66 Entretien de l´étude sur la cybercriminalité (secteur privé).
67 Entretien de l´étude sur la cybercriminalité (secteur privé).
68 Questionnaire de l´étude sur la cybercriminalité (secteur privé).Q64-67.
69 Entretien de l´étude sur la cybercriminalité (secteur privé).
70 Entretien de l´étude sur la cybercriminalité (secteur privé).
71 Entretien de l´étude sur la cybercriminalité (secteur privé).
72 Entretien de l´étude sur la cybercriminalité (secteur privé).

Si vous allez pirater une entreprise, vous n´allez pas entrer en empruntant la porte d´entrée. Vous allez entrer en envoyant un PDF trafiqué au directeur des comptes lorsque le directeur est en vacances et vous allez infecter son ordinateur avec ce PDF ; puis vous allez prendre le contrôle de son ordinateur portable et vous introduire dans son réseau, accéder aux comptes et aux systèmes de paiements. Il s´agit de constamment accroître la sensibilisation aux risques et la mise à jour. Il n´y a pas de solution miraculeuse pour cela ».[73]

Il y a des proportions presque similaires entre les répondants du secteur privé qui avaient une unité centrale spécialisée pour traiter les problèmes de cybercriminalité, ceux qui avaient plusieurs unités spécialisées (pour la liaison avec les services répressifs et la sécurité des TI) et les répondants qui avaient du personnel spécialisé dans divers domaines de travail. Le nombre total de personnel assigné augmentait lentement en fonction de la taille de l´entreprise et variait de 0 à 38 (avec un cas extrême de 120).

Le personnel s´occupait généralement de la conservation des données et des enquêtes avancées sur internet, de la surveillance des tendances et des menaces émergentes en matière de cybercriminalité, de la coopération avec les services répressifs, et de l´analyse des approches relatives à la sécurité des systèmes informatiques. Le personnel était essentiellement formé en interne et recevait des formations additionnelles fournies par le secteur privé, le milieu universitaire et les organisations non gouvernementales. Environ un tiers des répondants fournissaient des formations sur ces thèmes à d´autres organisations, y compris à des entreprises, des institutions gouvernementales et dans certains cas à des organisations internationales et à des organisations non gouvernementales.[74]

Figure 8.12 : utilisation des dispositifs : personnels ou professionnels



Source : Kaspersky Lab, 2012. Perception et connaissance des menaces de TI (p.2)

Deux récents changements technologiques fondamentaux qui affectent l´environnement de risques de sécurité de l´information, sont la croissance rapide de l´utilisation des services informatiques en nuage, et l´utilisation que font les employés de leurs propres dispositifs informatiques (en particulier les smartphones et les tablettes) pour accéder au système de l´entreprise. Un sondage réalisé par une entreprise internationale de sécurité portant sur 11 000 utilisateurs d´internet en Amérique du nord et en Amérique latine, en Europe, au Moyen-Orient, en Asie et en Afrique révéla qu´entre 15 à 25 % des répondants utilisaient plusieurs dispositifs informatiques personnels au bureau.[75] Des répondants du secteur privé mentionnèrent aussi l´ impact croissant des services informatiques en nuage sur les considérations de sécurité. Un consultant en technologie déclara, par exemple : « *pour les petites entreprises l´utilisation du nuage est probablement plus sûre du point de vue informatique que d´essayer de le faire soi-même. Il n´y a pas suffisamment d´experts en cybersécurité pour que chaque entreprise en ait un et cela serait beaucoup trop coûteux. Et donc les concentrer sur Amazon est tout à fait logique pour ce qui concerne la protection et la riposte. Cela crée évidemment des cibles d´opportunités car il est beaucoup plus amusant de violer les défenses d´un grand fournisseur de services que de violer les défenses du magasin du coin* ».[76]

73 Entretien de l´étude sur la cybercriminalité (secteur privé).
74 Questionnaire de l´étude sur la cybercriminalité (secteur privé).Q68-73.

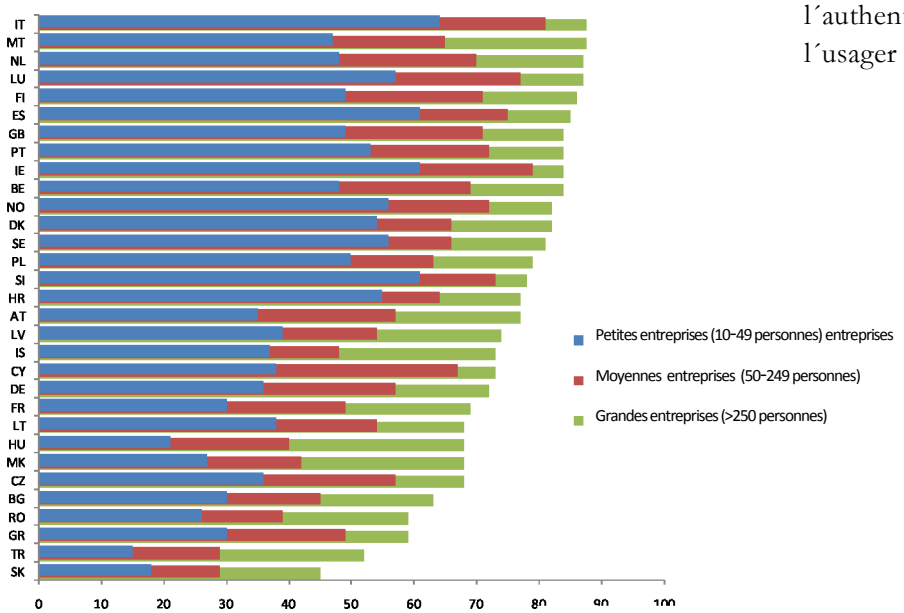
75 Kaspersky Lab. 2012. *Perception et connaissance des menaces des TI : le point de vue du consommateur*,.
76 Entretien de l´étude sur la cybercriminalité (secteur privé).

D´autres répondants mentionnèrent l´utilisation que faisaient les employés de leurs propres dispositifs. Un cabinet de conseil en technologie déclara : « *je pense que l´accumulation de risques provient du fait d´amener des dispositifs personnels. Lorsque les personnes qui amènent des dispositifs adaptés les connectent à des réseaux sans fil, ils mélangent les médias sociaux et les courriels du travail et de la vie privée. Je pense donc que la menace principale provient d´une absence d´appropriation culturelle du problème* ».[77]

Principes sociaux – les principes sociaux de l´OCDE concernent la conduite démocratique et éthique des participants de la société de l´information. Ceci inclut la sensibilisation à l´impact de la violation de la sécurité sur d´autres parties, la règlementation et la législation pertinentes, et le fait que la conduite des employés soit à la hauteur des valeurs de l´entreprise. Ceci est également lié à la compatibilité des pratiques de sécurité avec des valeurs sociétales telles que la liberté d´expression, le respect de la vie privée, l´ouverture et la transparence. Les intervenants du secteur privé qui ont répondu à l´étude étaient essentiellement chargés des décisions commerciales et techniques liées à la sécurité et à la cybercriminalité, plutôt que des responsabilités sociales ou juridiques des entreprises. Pour ce qui concerne les principes sociaux, un seul répondant commenta : « *ces dernières années le concept de « plus il y a de données mieux c´est » a été la philosophie de la plupart des entreprises. Il fallait collecter le plus de données possibles car il était ensuite possible d´explorer les données, de les utiliser et de faire des modélisations prévues en pensant très peu au préjudice* ».[78] Le répondant mentionna également que cette forme de comportement pouvait affecter l´évaluation des risques car certaines entreprises tendaient à sous-estimer l´importance des données personnelles qu´elles détenaient et les risques que cela pouvait entraîner.

Principes du cycle de vie de la sécurité – les répondants du secteur privé se basaient sur une portée plus vaste des principes du cycle de vie de la sécurité de l´OCDE qui sont de nature plus fonctionnelle. Ces principes sont axés sur l´évaluation des risques ; les systèmes conçus pour réduire les risques identifiés ; le développement de politiques, de processus et de procédures pour gérer ces systèmes ; et une évaluation continue des progrès technologiques. Des enquêtes réalisées par des entreprises internationales montrent la mesure dans laquelle ces principes sont mis en œuvre. La figure 8.13 montre, par exemple, le pourcentage d´entreprises européennes qui utilisent des jetons matériels pour protéger l´authentification de l´usager .[79]

Figure 8.13 : authentification forte du mot de passe et/ou authentification et identification de l´usager avec des jetons matériels par taille



% des entreprises qui utilisent une des mesures de sécurité suivantes : une authentification forte du mot de passe et ou l´identification/authentification avec des jetons matériels, 2010
Source : enquête communautaire d´Eurostat sur l´usage des TIC et le commerce électronique dans les entreprises

77 Entretien de l´étude sur la cybercriminalité (secteur privé).
78 Entretien de l´étude sur la cybercriminalité (secteur privé).
79 Enquête communautaire d´Eurostat sur l´usage des TIC et le commerce électronique dans les entreprises.

La figure illustre les différences relatives à la mesure dans laquelle les petites, moyennes ou grandes entreprises utilisent de bonnes pratiques en matière de cybersécurité – les plus petites entreprises utilisent généralement des pratiques moins sûres que les moyennes et grandes entreprises. Deux tiers des intervenants du secteur privé qui ont répondu au questionnaire de l´étude ont déclaré que leurs organisations avaient appliqué des évaluations de risques en matière de cybercriminalité. Un grand cabinet de conseil déclara que : « *deux fois par an la direction exécutive de l´entreprise doit valider les risques de sécurité relatifs aux informations prioritaires dans le cadre du point de vue de la direction sur l´organisation de la sécurité de l´information. La liste des risques examinés inclut, sans s´y limiter, les actes criminels ». Un fabricant d´équipement déclara que les méthodes d´évaluation incluaient des « entretiens, des tests d´intrusion [et] des tests de produits* ».[80]

Plusieurs répondants mentionnèrent des disparités entre les petites, moyennes et grandes entreprises en matière d´évaluation de risques. Une entreprise de taille moyenne de conseils en technologie déclara que : *« [les petites et moyennes entreprises pensent]* « *nous ne sommes pas visibles et ils ne nous attaqueront pas, » et cela est faux. La perception « nous n´avons pas une valeur élevée et ils ne nous attaqueront pas* » *est fausse et provient de* « *nous ne savons pas quoi faire » – ce qui est vrai ».*[81] Une entreprise internationale de conseil ajouta : « *en ce qui concerne les activités criminelles, les banques et les grandes entreprises sont relativement bien protégées. Les marchés intermédiaires n´ont pas les mêmes capacités ; ils ont du mal à réagir et à savoir quoi faire ».*[82] Une petite entreprise de technologie déclara : « *nous fournissons beaucoup d´éducation gratuite en ligne et nous avons toujours eu une extraordinaire participation des petites et moyennes entreprises. Les grandes entreprises participeront aussi, mais la majorité est composée de petites et moyennes entreprises qui viennent pour l´éducation gratuite, ils ont définitivement besoin d´information* ».[83]

Plusieurs répondants signalèrent que certaines petites entreprises ne prenaient pas des mesures simples pour protéger leurs systèmes. Une entreprise de services commenta : « *les petites et moyennes entreprises ont des pertes de données causées par des moyens très simples et non des moyens de haute technologie (lorsque quelqu´un oublie de changer de mot de passe – des choses de ce genre)... la plupart des entreprises ne sécurise probablement pas les données au repos, seulement les données en transit ».*[84] Une entreprise de conseil en technologie ajouta : « *les conseils que nous donnons essentiellement aux personnes sont : assurez vous que votre système soit corrigé, totalement mis à jour ; veiller à mettre à jour régulièrement l´équipement et les logiciels antivirus ; si vous n´utilisez pas les produits Java, Adobe – retirez-les ; ayez un ordinateur autonome, isolé que vous utiliserez seulement pour les opérations bancaires en ligne. Mais vous ne pouvez pas vous défendre d´une attaque au jour zéro* ».[85] Un fournisseur international de services de technologie a déclaré que même dans le cas des grandes entreprises : « *diverses infractions étaient et sont évitables – et elles sont toutes liées aux configurations basiques* ».[86]

La plupart des répondants du secteur prive a mentionné qu´ils utilisaient des solutions techniques pour prévenir la cybercriminalité, comme les pare-feu, la conservation des preuves électroniques, et des restrictions sur des connexions d´adresses IP spécifiques. Plusieurs utilisent également l´identification de certains types de contenus, des mesures pour éviter les infractions aux droits d´auteurs /marques déposées, le décryptage du matériel encodé et des mesures contre l´utilisation abusive de l´informatique. Les principaux éléments de ces solutions incluent la surveillance du système, la détection des intrusions et des logiciels antivirus. Les systèmes étaient principalement développés par le secteur privé, et certains en interne, et avaient un coût annuel d´application significatif, particulièrement pour les entreprises internationales.[87] Les intervenants étaient en désaccord sur les menaces représentées par les « initiés » (des employés ou d´autres personnes avec un accès autorisé au système). Deux entreprises internationales soulignèrent que le groupe de potentiels « initiés » était devenu extrêmement vaste dans leurs cas : une avait « *30 0000 employés dans le monde entier, plus des contractuels* »[88] et l´autre avait « *20 0000 employés et 50-60 000 vendeurs ou contractuels ».*[89] Un fabricant était préoccupé par la « *collusion entre les initiés et les criminels externes* [*avec*] *des initiés qui interrompent les processus de fabrication et les systèmes internes* ».[90]

80 Entretien de l´étude sur la cybercriminalité (secteur privé).Q49.
81 Entretien de l´étude sur la cybercriminalité (secteur privé).
82 Entretien de l´étude sur la cybercriminalité (secteur privé).
83 *Ibid.*
84 Entretien de l´étude sur la cybercriminalité (secteur privé).
85 *Ibid.*

86 *Ibid.*
87 Entretien de l´étude sur la cybercriminalité (secteur privé).Q60-63.
88 Entretien de l´étude sur la cybercriminalité (secteur privé).
89 Entretien de l´étude sur la cybercriminalité (secteur privé).
90 Entretien de l´étude sur la cybercriminalité (secteur privé).

Une entreprise de conseil en sécurité se montra moins préoccupée, du moins pour les entreprises avec une haute technologie : « *oui, cela implique parfois des initiés mais ce n´est pas fréquent. La plupart des préjudices est causée par des parties externes. Il est vrai que les banques sont très cloisonnées et, même s´il y avait des initiés, il est probable que les préjudices qu´ils pourraient causer seraient assez limités* ».[91]

L´évaluation et l´examen des procédures et des politiques de sécurité sont une partie essentielle des principes du cycle de vie de la sécurité de l´OCDE. De nombreux répondants du secteur privé ont signalé l´importance de superviser les incidents de sécurité en temps réel. Une entreprise internationale de conseil a déclaré : '*nous avons besoin de mécanismes pour une participation et des renseignements concrets en temps réel. C´est un problème complexe ; il doit y avoir une taxonomie, une priorisation et une détermination quand un incident est grave ; tout le monde doit parler le même langage même si les objectifs sont différents*, et*, être concrets et réalisables en temps réel*'.[92]

Golden Eye contre Telefónica

Un producteur de films, et des détenteurs des droits d´auteurs de films pornographiques engagèrent une procédure judiciaire en 2011 pour obtenir les noms et les adresses de presque 10 000 usagers présumés avoir violé les droits d´auteurs en utilisant des logiciels de partage de fichiers BitTorrent. La Haute cour d´un pays d´Europe du nord autorisa la procédure pour un seul plaignant, en commentant que si cela allait plus loin "cela reviendrait pour la cour à sanctionner la vente des droits sur la vie privée et la protection des données des défendeurs au plus offrant." La cour se souciait aussi du fait que la nature des films en question puisse être utilisée pour embarrasser des clients innocents pour qu´ils paient des règlements des droits intolérablement élevés.

La Haute cour imposa de nombreuses conditions à la lettre qui pourrait être envoyée aux infracteurs allégués, en raison « de l´impact ... sur des consommateurs ordinaires qui pouvaient ne pas avoir accès à un avis juridique spécialisé, qui pouvaient être innocents des accusations portées contre eux et qui pouvaient être embarrassés ou bouleversés d´être accusés d´avoir été impliqués dans des partages de fichiers au contenu pornographique»...

Moyennant ces protections, un appel des douze autres plaignants fut accueilli. La Cour d´appel rendit une ordonnance qui exigeait que les fournisseurs de services divulgue les données des clients qui étaient présumés avoir enfreint les droits, permettant ainsi que d´autres mesures soient prises contre chacun d´entre eux.

Une autre entreprise internationale de conseil a ajouté : « *lorsqu´elles ont les connaissances appropriées elles répondent bien. La situation à laquelle nous faisons face est que de nombreuses entreprises ne sont pas assez compétentes en matière de détection... 12 minutes, et non 12 mois* ».[93] De nombreux répondants du secteur privé ont cependant déclaré que les entreprises pourraient mieux se protéger contre les menaces de la cybercriminalité. Une entreprise internationale de services a déclaré : « *les menaces et les tendances varient, et vont des plus simples aux plus complexes. La clé est de connaître votre réseau et de le contrôler en termes de configurations d´applications et de développer un système de renseignement complexe* ».[94] Un autre fournisseur international de services de technologie a signalé : « *la plupart des usagers ne pourraient pas se permettre d´accorder la priorité à la sécurité 24 heures sur 24 et 365 jours par an (surveillance info/sec)* ».[95] Une entreprise de conseil internationale suggéra que « *le travail en matière de renseignement de sécurité sera sous-traité – presque comme un bureau central pour les informations et les opérations des prises de décisions en mature de sécurité, au lieu que chaque grande organisation opère son propre centre de collecte de renseignements et de sécurité internationale* ».[96]

Outre l´attention portée, *intérieurement*, à leur propre situation en matière de cyber sécurité, certaines entreprises internationales de technologie ont une approche externe proactive afin d´enquêter et de stopper les cyber attaques qui menacent la confiance des clients dans leurs systèmes. Lorsque ces initiatives sont prises dans le plein respect des lois pertinentes, elles peuvent compléter les mesures des services répressifs, et être positives pour la publicité et le moral du personnel.

91 *Ibid.*
92 Entretien de l´étude sur la cybercriminalité (secteur privé).
93 *Ibid.*
94 Entretien de l´étude sur la cybercriminalité (secteur privé).
95 Entretien de l´étude sur la cybercriminalité (secteur privé).
96 *Ibid.*

Certaines des plus longues séries de mesures juridiques concernent les courriels et autres communications non sollicités tels que les messages instantanés. Un des plus grands fournisseurs de services d´Amérique du nord a entamé des douzaines de poursuites contre les personnes qui envoient des messages non sollicités de 1997 à la date, a porté plainte pour atteinte illicite aux biens, enrichissement sans cause et détournement, ainsi que pour des violations aux lois sur les délits informatiques.[97] Par conséquent, un groupe de fournisseurs de services d´Amérique du nord formèrent une alliance contre le spam en 2003 ; ils utilisèrent des lois contre l´envoi de messages non sollicités et contre la conspiration et prirent des mesures légales contre des douzaines de défendeurs présumés être responsables de l´envoi de centaines de millions de messages non sollicités à leurs clients.[98]

Plus récemment, une entreprise internationale de logiciels a présenté de nombreuses actions en justice concernant les botnets, avec deux principales tactiques de verrouillage : prendre le contrôle des mécanismes de contrôle et de commande utilisés pour diriger les machines dans un botnet, et saisir les machines qui contiennent des preuves utiles sur des actes délictueux. Dans un cas récent contre le botnet Nitol, l´entreprise porta plainte pour prendre le contrôle de 70000 sous domaines malveillants. L´opérateur accepta la décision de rediriger les connexions des sous domaines malveillants identifiés, futurs ou existants, vers une machine gérée par un CERT d´Asie de l´est. Ceci réduisait la capacité de l´opérateur des botnets de contrôler les machines en essayant d´atteindre ces domaines, et donnait l´opportunité de notifier aux usagers et à leurs fournisseurs de services que leurs machines avaient été compromises.

Durant les 16 jours postérieurs à la prise de contrôle des sous-domaines malveillants par l´entreprise, les connexions de 7.65m adresses IP uniques furent bloquées. L´opérateur et l´entreprise transmirent toutes les preuves collectées lors de l´enquête à un CERT d´Asie de l´est pour aider à identifier les opérateurs du sous-domaine original. Les données relatives aux machines infectées furent transmises à la « Shadow Server Foundation » et aux CERT nationaux. L´entreprise avait pris antérieurement des mesures similaires contre les botnets Waledac, Rustock, Kelihos et Zeus.[99]

Dans le cas du botnet Zeus, l´entreprise pris plus de mesures d´intervention. Après avoir obtenu un mandat d´un juge fédéral, le personnel technique et les avocats de l´entreprise saisirent les preuves et désactivèrent les serveurs hébergés en Pennsylvanie et en Illinois qui contrôlaient les botnets liés à Zeus. L´entreprise prit aussi le contrôle de 800 domaines utilisés pour coordonner les ordinateurs infectés. Ces actions furent planifiées pour interrompre l´opération de ces botnets, car il n´était pas possible de les stopper complètement.[100] Une troisième stratégie juridique utilisée par l´entreprise est de porter plainte contre les auteurs présumés des codes malveillants, dans le but d´éviter qu´ils ne créent de nouveaux codes malveillants lorsque leurs efforts antérieurs ont été stoppés. En 2012, l´entreprise engagea des poursuites modifiées dans un tribunal de district d´Amérique du nord contre un programmateur établi en Europe de l´est dont le code avait été utilisé pour le botnet Kelihos. Le programmateur concerné souhaitait conclure une convention de règlement confidentielle.[101]

De même, une entreprise de médias sociaux pris des mesures contre les fournisseurs d´outils permettant l´envoi de messages non sollicités, en engageant des poursuites en 2012 contre « cinq des plus agressifs polluposteurs et fournisseurs d´outils pour l´envoi de messages non sollicités, » en alléguant des violations des conditions de service et d´inciter les utilisateurs d´outils à des violations.[102] L´entreprise sollicita une injonction interdisant aux défendeurs de créer ou d´offrir ce logiciel, et demanda des dommages et intérêts d´au moins 700 000 $.[103]

97 Sorkin, D.E., 2001.Approches techniques et juridiques de l´envoi de messages électroniques non sollicités. *Revue juridique de l´université de San Francisco,* 35(2) :359260.

98 McGuire, D., 2004. AOL, les entreprises de messages électroniques attaquent en justice les polluposteurs. *Washington Post*, 28 octobre.

99 Microsoft conclut un règlement avec les défendeurs dans le cas Nitol. 2012. *The Official Microsoft Blog*, 2 octobre, disponible sur : http ://blogs.technet.com/b/microsoft_blog/archive/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitolcase.aspx

100 Microsoft et les dirigeants de l´industrie des services financiers ciblent les opérations de cybercriminalité des botnets Zeus. 2012. *The Official Microsoft Blog*, 25 mars, disponible sur : http ://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-servicesindustry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx

101 Microsoft conclut un règlement avec le second défendeur du cas Kelihos. 2012. *The Official Microsoft Blog*, 19 octobre, disponible sur : http ://blogs.technet.com/b/microsoft_blog/archive/2012/10/19/microsoft-reaches-settlement-with-second-kelihosdefendant.aspx

102 Stopper les polluposteurs. 2012. *Twitter Blog*, 5 April, disponible sur : http ://blog.twitter.com/2012/04/shutting-down-spammers.html

103 *Twitter Inc. contre Skootle Corporation*. 2012. Cour de District des US, District nord de Californie, cas n°. CV 12-01721, 5 avril.

Deux autres grands fournisseurs de services ont aussi engagé des poursuites contre des annonceurs qui faisaient un usage abusif de leurs services. Un grand moteur de recherche obtint, par exemple, une injonction permanente contre une entreprise qui annonçait des systèmes frauduleux de transferts de fonds,[104] et intenta un procès à des annonceurs qui violaient délibérément ses conditions de service.[105] Une grande entreprise de services de réseaux sociaux engagea aussi des poursuites contre une entreprise qui désignait des pages et des liens qui trompaient les usagers et les incitaient à fournir des informations personnelles, à adhérer à des services onéreux de souscription, à « aimer » une page d´un site web et à ensuite le partager avec leurs amis.[106] Le défendeur conclut un accord avec l´entreprise. De nombreuses entreprises de sécurité sur internet rassemblent des données détaillées sur la prévalence des logiciels malveillants et des botnets, qui sont publiées dans des rapports réguliers et transmis à leurs partenaires des entreprises et des services répressifs. Plusieurs entreprises publient des rapports trimestriels sur les menaces, qui contiennent des données sur les niveaux d´infection des machines (y compris des dispositifs mobiles), les violations des bases de données, les attaques telles que l´hameçonnage et des activités spécifiques de cybercriminalité telles que des demandes de rançon et des outils de logiciels criminels.[107] Une entreprise de sécurité d´Europe de l´est a publié des données collectées sur des groupes et des individus impliqués dans la cybercriminalité dans cette région[108] et une autre entreprise de sécurité a récemment publié un rapport qui comparait les profils des cyber délinquants d´Asie de l´est et d´Europe de l´est.[109] Plusieurs entreprises de télécommunications partagent des données sur les patrons de trafic et les attaques sur leurs réseaux. Un de ces observatoires produit, par exemple, une carte mondiale des menaces en temps réel avec des informations quotidiennes sur des faits significatifs.[110] Un phénomène plus récent a été l´utilisation des renseignements recueillis par les entreprises pour répondre aux attaques. Plusieurs organisations du secteur privé aident les entreprises à définir le profil des adversaires et leurs motivations d´attaques. Ces informations permettent d´établir de meilleures défenses techniques, des mesures juridiques soigneusement définies, de tromper (en introduisant, par exemple, de fausses informations sur les propres réseaux des entreprises), et de faire en sorte que les attaques requièrent davantage de ressources.[111] Certaines entreprises ont envisagé de pirater à leur tour les attaquants, mais si cela est techniquement et légalement faisable, c'est une question actuellement peu claire.[112] Dans l´ensemble, les répondants du secteur privé ont décrit une situation mixte en matière de prévention de la cybercriminalité. Les grandes entreprises, en particulier dans le secteur des services financiers, ont des stratégies sophistiquées de prévention, et utilisent des technologies spécifiques de sécurité comme les jetons matériels. Les entreprises de sécurité surveillent activement et publient des rapports réguliers sur l´émergence de nouvelles menaces, et certaines grandes entreprises de technologie ont pris des mesures juridiques proactives pour stopper les botnets, les polluposteurs et les fraudeurs. Les petites entreprises, par contre, ne sont pas aussi bien positionnées et certaines ne prennent pas de précautions basiques ou n´ont pas une vision réaliste des risques de sécurité.

104 Combattre la fraude en ligne : amener les escrocs de « Google Money » devant les tribunaux. 2009. *Google Official Blog*, 8 Ddécembre, disponible sur :http ://googleblog.blogspot.co.uk/2009/12/fighting-fraud-online-taking-google.html

105 Amener les pharmacies illégales devant les tribunaux. 2010. *Google Official Blog*, 22 septembre, disponible sur : http ://googleblog.blogspot.co.uk/2010/09/taking-rogue-pharmacies-to-court.html

106 Facebook, Washington State AG Target Clickjackers. 2012. *Notes de sécurité deFacebook*, 26 janvier, disponible sur : http ://www.facebook.com/notes/facebook-security/facebook-washington-state-ag-target-clickjackers/10150494427000766

107 Voir, par exemple, *le rapport McAfee sur les menaces : troisième trimestre2012*, disponible sur : http ://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

108 Group-IB. 2012. *L´état et les tendances du marché russe de la cybercriminalité 2011*, disponible sur : http ://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf

109 Trend Micro. 2012. *Peter the Great contre Sun Tzu*, disponible sur : http ://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/op_kellermann_peter-the-great-vs-sun-tzu.pdf

110 Voir http ://atlas.arbor.net/about/

111 Higgins, K.J., 2012. Tables tournantes : Identifier les pirates derrière le clavier. *Dark Reading*, 2 octobre, disponible sur : http ://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240008322/turning-tables-id-ing-thehacker-behind-the-keyboard.html

112 Simonite, T., 2012. Lutter contre les pirates informatiques sans se rabaisser à leur niveau. *MIT Technology Review*, 26 juillet, disponible sur : http ://www.technologyreview.com/news/428584/fighting-hackers-without-sinking-to-their-level/

Prévenir la cybercriminalité par le biais des fournisseurs de services internet et d´hébergement

Les fournisseurs de services internet et de services d´hébergement occupent une place de choix dans les infrastructures d´internet. Comme le décrit le premier chapitre (connectivité globale), les fournisseurs de services possèdent ou louent le transport de câbles et de fibres optiques de haute capacité, ainsi que d´autres infrastructures essentielles comme les serveurs, les commutateurs et les routeurs, et (dans le cas des opérateurs de réseaux mobiles) les cellules radio qui permettent que le contenu soit hébergé et distribué aux ordinateurs de bureau et aux dispositifs portables connectés à internet. Que les fournisseurs de services aient un rôle à jouer dans la prévention de la cybercriminalité est à la fois évident, mais nuancé et complexe – car cela met en jeu la responsabilité relative au contenu d´internet des fournisseurs de services. Afin d´évaluer les possibilités de prévention en matière de cybercriminalité pour les fournisseurs de services, il faut tout d´abord examiner de nombreux aspects techniques.

Les fournisseurs de services connectent les usagers à internet en transmettant des données entre les usagers et des dispositifs tels que le web, la messagerie électronique et les serveurs VOIP. Les fournisseurs de services peuvent potentiellement analyser ce trafic, à moins que les usagers n´encodent les données en utilisant un réseau privé virtuel, un serveur proxy, ou une fonctionnalité du logiciel de communications. Les données de l´usager auxquelles le fournisseur de services peut avoir accès incluent le *contenu* des communications – les textes et les images non encodés des sites web ou des courriels – et les données *contextuelles* comme les services visités, la source et la destination des courriels, les moments auxquels ces différents services sont utilisés et le temps que l´usager passe dans les différents services, même lorsque est utilisé le cryptage basique du site web. En général, les données du contenu peuvent être observées seulement au moment où elles sont envoyées et seulement en surveillant explicitement la connexion de l´usager et en stockant les données avec un équipement spécialisé. Une exception notable est lorsqu´un fournisseur de services opère, par exemple, un serveur de messagerie qui stocke les messages pour de longues périodes.

Les personnes utilisent souvent divers fournisseurs de services car ils accèdent l´internet d´endroits différents. Le fournisseur de services du domicile d´un usager est souvent différent de celui de son dispositif mobile. Les fournisseurs d´accès à internet du travail peuvent aussi être différents et la connexion à un réseau sans fil d´un café local impliquera qu´un autre fournisseur de services gère la connexion. Les informations sur les activités d´un individu peuvent donc être dispersées entre plusieurs fournisseurs différents.

Les fournisseurs d´hébergement internet contrôlent les systèmes sur lesquels les sites web et les autres services sont opérés. Comme dans le cas des relations entre les fournisseurs de services internet et leurs clients, les entreprises d´hébergement ont une vision privilégiée du trafic qui passe par les services hébergés de leurs clients. Ils ont donc la possibilité technique de désactiver ou de bloquer l´utilisation illégale de ces services. Les entreprises d´hébergement appliquent généralement des restrictions sur la nature des services qu´ils peuvent héberger par le biais d´accords de services, qui incluent souvent des conduites abusives bien connues telles que l´envoi de grandes quantités de messages non sollicités ou de courriels abusifs, l´hébergement de contenu illégal ou l´utilisation à des fins de violations des droits d´auteurs.

Les fournisseurs de services peuvent jouer un rôle dans la prévention de la cybercriminalité dans deux domaines principaux : (i) avec le stockage des données de l´usager auxquelles auront ensuite accès les services répressifs et qui seront utilisées dans des enquêtes sur la cybercriminalité ; et (ii) avec un filtrage actif des communications ou du contenu d´internet afin d´éviter les actes de cybercriminalité. Cette section examine les aspects techniques et règlementaires de chacun de ces domaines.

Le stockage de données – en raison du volume de trafic qui passe par leurs réseaux, les fournisseurs de services internet ne peuvent pas conserver des registres complets de tout le trafic. Certains pays ont mis en place des systèmes sophistiqués de surveillance d´internet, mais les limitations techniques de la collecte et de l´analyse de grands volumes de données peuvent poser des problèmes. L´enregistrement d´informations moins détaillées (comme les adresses IP assignées à des individus spécifiques à des moments particuliers) peut s´étendre sur une période prolongée. Les fournisseurs de services internet ont généralement la capacité d´exercer une surveillance ciblée des données en temps réel, et (comme cela est mentionné au chapitre quatre (application des lois et enquêtes)), les règles relatives à l´interception licite dans plusieurs états requièrent que les fournisseurs de services internet aient la capacité d´exercer une surveillance ciblée en temps réel des connexions d´un individu ou de locaux.

La protection des données – le stockage et le traitement des données des fournisseurs de services internet sont soumis, dans plusieurs pays, aux lois sur la protection des données qui imposent des obligations sur la protection et l´utilisation des informations personnelles.[113] En 1990, l´Assemblée générale des Nations Unies a adopté des principes directeurs pour la règlementation des fichiers informatisés contenant des données à caractère personnel.[114] Ils incluent dix principes, tels que le principe de licéité et de loyauté, d'exactitude et de finalité, et s´appliquent à « *tous les fichiers informatisés publics et privés* ». Le principe de sécurité stipule que ces fichiers devraient être protégés contre « *les risques humains, tels que l´accès non autorisé, l´utilisation détournée de données ou la contamination par des virus informatiques* ». Une révision, en 2012, des lois sur la protection des données mentionna qu´il y avait des lois complètes dans 89 pays et des projets de lois dans 10 autres pays.[115]

Certains cadres juridiques régionaux sur la protection des données – comme le cadre juridique de l´UE – incluent des règles spécifiques sur la protection des données dans le secteur des communications électroniques.[116] Conformément à ce cadre, les services de communications accessibles au public doivent prendre « *des mesures d´ordre technique et organisationnel appropriées afin de garantir la sécurité...le cas échéant conjointement avec le fournisseur du réseau public de communications en ce qui concerne la sécurité du réseau* ». Les données de trafic des usagers peuvent être traitées seulement à des fins spécifiques et il faut les éliminer ou les rendre anonymes lorsqu´elles ne sont plus nécessaires (voir le paragraphe suivant sur la conservation des données.) Les états membres de l´UE peuvent restreindre certains de ces droits pour protéger des objectifs comme « *la sécurité publique et pour permettre la prévention, la recherche, la détection et la poursuite d'infractions pénales ou l´utilisation non autorisée de systèmes de communications électroniques* ». Lors de la collecte des informations pour l´étude, la majorité des pays répondants ont indiqué des dispositions constitutionnelles et/ou législatives pour protéger la confidentialité des données personnelles. La finalité générale des lois sur la protection des données était de *« régir la collecte, l´utilisation et la divulgation des renseignements personnels afin de reconnaitre le droit des personnes de voir leurs renseignements protégés et le besoin des organismes de recueillir ces renseigements ».*[117] Pour ce qui concerne la contribution des fournisseurs de services à la prévention de la cybercriminalité, les lois sur la protection des données ont de nombreux effets. Les restrictions au traitement des données ne devraient pas en général (du moins s´il existe les exceptions légales suffisantes) empêcher que les services répressifs accèdent légalement aux données des clients des fournisseurs de services à des fins d´enquête. Une exception typique mentionnée était que *« un organisme autre qu´un organisme d´application de la loi (y compris une entreprise) qui détient des informations personnelles est autorisé à divulguer ces informations à des services répressifs sans violer la loi sur la confidentialité lorsque cela est raisonnablement nécessaire pour appliquer le droit pénal ».*[118]

113 L´OCDE et le Conseil de l´Europe ont fixé des principes similaires pour le traitement des données personnelles au début des années 80(voir les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données, 1980 ; la Convention du Conseil de l´Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ETS n°. 108, 1981.) D´autres organisations régionales ont depuis adopté des règles sur la protection des données, y compris notamment la coopération économique Asie-Pacifique, la communauté économique des pays d´Afrique de l´ouest et l´Organisation des états américains (voir le cadre de protection de la vie privée de l´APEC, 2005 la loi complémentaire A/SA.1/01/10 sur la protection des données personnelles dans la CEDEAO, 2010, et la Résolution 2661 de l´Assemblée générale sur l´accès aux informations publiques et la protection des données personnelles, 2004). L´Union européenne a développé une gamme complète de règles sur la protection des données, qui font partie de la Charte européenne des droits fondamentaux (ainsi qu´un droit à vie privée plus large qui inclut les communications). La Directive sur la protection des données contient des règles qui s´appliquent aux organisations du secteur public et du secteur privé, y compris les fournisseurs de services internet (voir la Directive

95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 sur la protection des personnes en ce qui concerne le traitement des données à caractère personnel et la libre circulation de ces données. OJ L 281, 23/11/1995 p.31 -50.)

114 Assemblée générale des Nations Unies, Résolution 45/95, 14 décembre 1990.

115 Greenleaf, G., 2012. Lois sur la confidentialité des données internationales : 89 pays, et continuer à accélérer. *Privacy Laws & Business International Report*, thème115, Supplément spécial.

116 Directive 2002/58/EC du Parlement européen et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. OJ L 201, 31.7.2002, pp.37–47.

117 Questionnaire de l´étude sur la cybercriminalité Q22.

118 Questionnaire de l´étude sur la cybercriminalité Q24.

Toutefois, les obligations dérivées de la protection des données qui exigent que les données personnelles soient éliminées lorsqu´elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées, peuvent avoir un impact pour les enquêtes en matière de cybercriminalité menées par la police. Comme le mentionnait le chapitre quatre (application des lois et enquêtes), de nombreuses autorités des services répressifs ont mentionné les problèmes causés par la durée restreinte de conservation des données des fournisseurs de services et cela peut être dû, dans certaines circonstances, à l´effet des lois sur la protection des données. De plus, les lois sur la protection des données – comme pour toutes les organisations et les personnes qui traitent les données personnelles – contribuent à prévenir la cybercriminalité du point de vue des fournisseurs de services, car elles fournissent des normes en matière de traitement des données qui aident à garantir la sécurité et l´intégrité des données de l´usager.

Conservation des données – l´effet combiné des lois sur la protection des données et les implications financières liées au stockage de grandes quantités de données, a un impact sur le fait que les fournisseurs de services n´aient pas des délais indéfinis de conservation des données. Pour aider les enquêtes menées par les services répressifs, de nombreux pays ont introduit des exceptions aux lois sur la protection des données qui exigent que les fournisseurs de services stockent des types spécifiques de données relatives aux activités en ligne des clients durant certains délais (un an), durant lesquels les enquêteurs peuvent y avoir accès avec une autorisation judiciaire ou administrative.

La plus largement applicable de ces lois est la directive de l´UE sur la conservation des données.[119] Les états membres de l´UE exigent des fournisseurs de services qu´ils conservent les données nécessaires pour retrouver et identifier la source d´une communication ; identifier la destination, le type et le moment d´une communicationet pour identifier le matériel des usagers. Ces données doivent avoir été stockées durant une période allant de six mois à deux ans. De nombreux tribunaux nationaux ont questionné la proportionnalité et l´impact sur la vie privée de ces exigences.[120]

Un petit nombre de pays ont envisagé ou ont appliqué des lois sur la conservation des données. Un pays d´Océanie a, par exemple, proposé un système de style européen, qui a été examiné par un comité parlementaire mixte.[121] Un autre pays d´Asie du sud a une législation qui autorise le gouvernement à définir des obligations qui exigent que les intermédiaires conservent les registres électroniques, mais ces règles ont été définies seulement pour les cyber cafés.[122] Par contre, la Cour suprême d´un pays d´Amérique du sud a annulé une loi sur la conservation des données en 2009 pour des raisons d´ingérence avec les droits à la vie privée des personnes.[123]

Le Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l´homme et des libertés fondamentales dans la lutte contre le terrorisme a exprimé sa préoccupation car « *dans divers pays, des lois sur la conservation des données ont été adoptées sans que des garanties juridiques sur l´accès à ces informations aient été établies ou sans tenir compte du fait que les nouveaux progrès technologiques estompent les différences entre les données du contenu et des communications data. Alors que les dispositions constitutionnelles tendent à requérir des garanties sur l´accès au contenu des communications, la protection des journaux des transactions est plus limitée. Bien que ces informations puissent faire partie intégrante des enquêtes, elles peuvent aussi être des données sensibles à caractère privé comme le contenu des communications* »[124] Les lois sur la conservation des données peuvent donc représenter une approche pragmatique pour s´assurer que les fournisseurs de services soient à même de mieux collaborer dans la prévention de la cybercriminalité en renforçant leur coopération avec les services répressifs, mais il est important que ces lois soient mises en place avec les garanties procédurales et les protections de la vie privée appropriées.

119 Directive 2006/24/EC du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou raitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications qui amende la Directive 2002/58/EC (OJ L 105/54, 13 avril 2006.

120 Brown, I. 2010. La conservation des données de communications dans un internet en évolution. *Journal International de droit et de technologie de l´information* 19(2) :95-109.

121 Le bureau du procureur général du gouvernement australien, 2012. *Équiper l´Australie contre des menaces émergentes et en évolution : un document de travail pour accompagner l´examen du comité parlementaire mixte de la sécurité et des renseignements d´un paquet d´idées relatives à la sécurité nationale comprenant des propositions pour la réforme de l´interception des télécommunications, la réforme de la sécurité du secteur des télécommunications et la réforme de la législation sur le secteur du renseignement d´Australie.*

122 Privacy International. 2012. *Rapport de pays : l´Inde, la vie privée dans un monde en développement*, disponible sur : https ://www.privacyinternational.org/reports/india-0

123 Halabi, Ernesto c/ P.E.N. - ley 25.873 (Acción de clase, Argentina).

124 Conseil des droits de l´homme des Nations Unies, Treizième session, A/HRC/13/37, 28 décembre 2009, p.16.

Notification de la violation des données – le stockage des données des clients des fournisseurs de services peut être affecté par les exigences de signalement obligatoire des violations de la sécurité. Le signalement obligatoire des violations de la sécurité aux parties affectées et aux régulateurs, en particulier lorsque des données personnelles sont divulguées, a bénéficié du soutien de nombreux pays. La notification est destinée à permettre aux victimes de violations de la sécurité de prendre des mesures pour réduire l´impact sur la sécurité (en changeant de mots de passe ou de NIP, ou en demandant que de nouvelles cartes de paiement soient émises) ; pour accroître la pression concurrentielle sur les entreprises, afin qu´elles améliorent leur sécuritéet pour soutenir le travail des régulateurs chargés de la protection des données et de la protection des infrastructure essentielles. Il existe des lois sur la notification de la violation des données au niveau infranational dans des pays d´Amérique du nord.[125] L´Union européenne requiert aussi des services et des réseaux public de communication pour signaler les violations significatives aux autorités nationales [126] et aux personnes affectées.[127] L´extension de cette exigence à toutes les organisations qui traitent des données personnelles est actuellement envisagée.[128] Les exigences ou les directives relatives à la notification ont également été introduites par des pays d´Océanie, d´Asie du sud et d´Asie du sud-est.[129] Les notifications des violations des données peuvent représenter un élément important des régimes de sécurité de l´information – applicables aux fournisseurs de services - mais ces lois doivent veiller à définir soigneusement le terme « violation de sécurité », et être utilisées conjointement à d´autres mesures, y compris à des lois efficaces sur la protection des données.

Filtrage du contenu internet – outre les opportunités de prévention de la criminalité liées au stockage des données, les fournisseurs de services peuvent également participer à la prévention de la cybercriminalité en examinant activement les données et les communications d´internet qu´ils véhiculent. Un concept fondamental à cet égard est la possibilité d´un filtrage d´internet effectué par les fournisseurs de services. Le filtrage des connexions internet a lieu, a un certain niveau, sur presque tous les réseaux. Le niveau le plus basique de filtrage est employé pour améliorer la performance et la sécurité du réseau en éliminant les données invalides et corrompues. Les fournisseurs de services ont aussi la capacité technique de filtrer des contenus malveillants ou illicites spécifiques. Plusieurs fournisseurs de services mettent en place un filtrage basique des messages non sollicités pour les comptes de messagerie de leurs usagers, et peuvent aussi fournir une protection contre le trafic malveillant bien connu provenant des virus ou des tentatives d´hameçonnage, en refusant le trafic identifié comme tel.

Les messages non sollicités et les botnets – le filtrage des messages non sollicités est un problème important pour tous les fournisseurs de services de messagerie en raison du grand volume de messages non sollicités envoyés et reçus quotidiennement. Les moyens par lesquels les messages non sollicités sont filtrés sont variés et complexes, et incluent l´analyse de l´origine des courriels pour identifier des sources connues de spam, ainsi qu´une analyse textuelle pour identifier des phrases communes et des patrons de contenus dans les messages. Les messages identifiés comme des messages non sollicités sont parfois totalement éliminés ou transmis à l´usager dans des « dossiers de courrier indésirable ». Outre le filtrage des messages non sollicités, les fournisseurs de services peuvent combattre le trafic malveillant comme celui généré par les botnets.

125 La Conférence nationale des assemblées législatives des états, 2012. Lois sur la notification des violations de la sécurité de l´état, sur http ://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

126 L´article 13a de la Directive 2002/21/EC du Parlement européen et du Conseil du 7 mars 2002 sur un cadre règlementaire commun pour les réseaux et les services de communications électroniques (OJ L 108, 24.4.2002, pp.33–50).

127 L´article 4 de la Directive 2002/58/EC du Parlement européen et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques(OJ L 201 , 31/07/2002 pp.37-47).

128 Les articles 31 et 32 de la Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes à l´égard des traitements de données à caractère personnel et à la libre circulation de ces données COM(2012) 11 final.

129 Maurushat, A., 2009. Lois sur notification des violations de données dans le monde de la Californie à l´Australie. *Lois sur la vie privée et commerce international.* UNSW document de recherche juridique n°. 2009-11.

> Lorsque les fournisseurs de services sont notifiés, ou voient à partir des patrons de trafic d´internet qu´une machine dans leur réseau semble faire partie d´un botnet ou est infectée par un logiciel malveillant, une option consiste à bloquer totalement ou partiellement le trafic de cette adresse et de notifier à l´usager les mesures à prendre pour éliminer le logiciel malveillant. Ces notifications peuvent provenir d´entreprises de sécurité qui surveillent les botnets, en utilisant des techniques comme les machines « pots de miel » qui attirent délibérément les logiciels malveillants. Les fournisseurs de services peuvent aussi prendre des mesures proactives pour identifier les machines compromises en surveillant le trafic pour détecter des signatures connues, mais une grande quantité de ciblage est nécessaire pour que cela soit efficace. Un examen effectué par l´Agence européenne chargée de la sécurité des réseaux et de l´information concluait que : « *Identifier le trafic de botnet parmi le trafic bénin et régulier revient à chercher une aiguille dans 100 millions de bottes de foin ».* Comme le mentionnait le chapitre cinq (application des lois et enquêtes), la surveillance du trafic général peut aussi, dans certaines circonstances, créer des conflits avec les lois sur la protection des données et de la vie privée.[130]

Filtrage du contenu – comme cela est examiné dans le contexte de la responsabilité des fournisseurs de services, les lois de certains pays exigent que les fournisseurs de services bloquent l´accès à des contenus illégaux comme la pornographie infantile. Les fournisseurs de services peuvent le faire de diverses manières, en faisant des compromis avec la vitesse, le coût, l´efficacité et la précision. En utilisant le filtrage *DNS*, les fournisseurs de services peuvent contrôler les réponses données aux usagers par leur serveur DNS server, restreignant ainsi l´accès à un domaine, comme « google.com », sans restreindre l´accès à une page spécifique ou à une série de résultats de recherche. Ceci est facile à contourner car les utilisateurs peuvent simplement utiliser des serveurs DNS alternatifs qui donneront des résultats réels. Le filtrage de l´en-tête *IP* peut être utilisé pour bloquer des ordinateurs individuels en se basant sur leur adresse ou pour bloquer partiellement des services spécifiques comme le web ou les courriels. Etant donné que plusieurs sites web peuvent être exécutés sur un seul serveur internet, ceci peut affecter des sites web non reliés – et parfois très nombreux. *L´Inspection approfondie des paquets* peut être utilisée pour examiner la partie essentielle du trafic internet. Ceci permet un filtrage extrêmement flexible, mais requiert un matériel coûteux sur les liaisons à haut débit des fournisseurs de services et peut ralentir toutes les connexions des usagers.

Dans la pratique, de nombreux régimes de filtrage emploient une combinaison de ces approches et forment un filtre hybride. Souvent, de simples filtres, comme les filtres basés sur les DNS, sont utilisés pour identifier le trafic à rediriger vers des filtres plus complexes. Cette approche hybride permet un filtrage sophistiqué ave des ressources réduites.

Une autre riposte possible des fournisseurs de services face au contenu illicite, est de ralentir le trafic plutôt que de le bloquer. Cette approche peut être utilisée pour rendre un service si incommode que les usagers l´éviteront. Des exemples de ceci incluent le ralentissement de connexions web encodées, pour obliger les usagers à utiliser des versions des sites web non encodées et qui donc peuvent être inspectées et la pratique utilisée par les fournisseurs de services pour ralentir le trafic de partage de fichiers comme BitTorrent.

Les possibilités de filtrage ou de blocage du contenu, y compris lorsque la finalité est la prévention de la cybercriminalité, ont suscité de nombreuses inquiétudes en matière des droits de l´homme. Le Conseil des droits de l´homme a, par exemple, souligné l´importance de l´accès à internet pour la liberté d´expression et d´autres droits de l´homme. Une résolution adoptée lors de sa 20ème session : « *Affirme que les mêmes droits que les personnes ont hors ligne doivent aussi être protégés en ligne, en particulier la liberté d´expression,* » et « *demande à tous les états de promouvoir et faciliter l´accès à internet ».* [131] Le Rapporteur spécial pour la promotion et la protection du droit à la liberté d´opinion et d´expression, a également appelé l´internet « *un outil indispensable pour réaliser de nombreux droits de l´homme, combattre l´inégalité et accélérer le développement du progrès humain... en facilitant l´accès à l´internet de*

toutes les personnes, avec le moins possible de restriction du contenu en ligne, devrait être une priorité pour tous les états ».[132]

130 Hogben, G., (ed.) 2011. *Botnets : Détection, Mesure, Désinfection & Défense*. ENISA, pp.73-74.
131 A/HRC/20/L.13, 29 juin 2012.
132 A/HRC/17/27, 16 May 2011.

La responsabilité des intermédiaires – le filtrage du contenu internet est étroitement lié à la possibilité d´imposer une responsabilité aux fournisseurs de services pour le contenu. Les fournisseurs de services internet ont généralement une responsabilité limitée en tant que « simples conduits » de données. Cependant, comme cela a été commenté précédemment, en particulier dans le contexte de l´hébergement, les modifications du contenu transmis accroissent la responsabilité, ainsi que la connaissance réelle ou présumée d´une activité illégale dans certains systèmes juridiques. D´autre part, des mesures expéditives prises après la notification réduisent la responsabilité.[133] Plusieurs systèmes juridiques incluent la notion de responsabilité secondaire lorsqu´une partie qui a contribué aux actes illicites d´une autre partie, peut être partiellement responsable des préjudices résultants. Étant donné que l´utilisation d´internet s´est généralisée au milieu des années 90, des inquiétudes relatives à l´impact de l´incertitude quant à la responsabilité des fournisseurs de services et des hébergeurs des contenus en ligne, sur l´économique numérique émergente, ont surgi. De nombreux pays ont réagi en adoptant des législations « horizontales » qui limitaient cette responsabilité dans plusieurs domaines du droit. Ces dispositions protégeaient généralement les intermédiaires qui n´étaient pas responsables pour ce qui concerne la transmission ou l´hébergement du contenu d´une tierce partie, à condition qu´ils respectent certaines conditions, comme notamment l´élimination d´un contenu spécifique après en avoir reçu la notification. De nombreux états ont aussi introduit une réglementation « verticale » concernant la responsabilité secondaire dans des domaines spécifiques, comme la protection des enfants, les données personnelles, la contrefaçon, la diffamation, les fraudes de paiement, les noms de domaine et les paris en ligne.[134] Des pays d´Amérique du nord et d´Europe ont introduit deux des premiers régimes horizontaux qui avaient de nombreux éléments communs. La législation d´un pays d´Amérique du nord comprend, par exemple, une ample limite relative à la responsabilité des fournisseurs de services, sauf pour ce qui concerne la confidentialité des communications, les lois sur la propriété intellectuelle et les dispositions pénales fédérales. Elle stipule que « *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 informatif... aucune action ne peut être intentée et aucune responsabilité ne peut être imposée en vertu d´une loi locale ou d´une loi de l´état qui ne soit pas en conformité avec la présente section ».*[135] La Directive de l´UE sur le commerce électronique [136] protège également les fournisseurs de services et d´autres « *fournisseurs de services intermédiaires* » qui fournissent des biens ou des services en ligne. Ceci exclut plusieurs domaines du droit, comprenant la taxation, la protection des données, les cartels et les paris. Pour ce qui concerne les fournisseurs de services qui sont un « *simple transport* » de transmissions, la Directive de l´UE stipule que les états doivent « *veiller à ce que le fournisseur de services ne soit pas responsable des informations transmises* ». Les services de stockage (caching) de l´information sont également protégés afin de rendre plus efficace la transmission, à condition qu´ils respectent les règles concernant l´accès à, et la mise à jour de ces informations, et qu´ils éliminent ou bloquent l´accès à l´information après l´avis d´élimination des données source. Les hébergeurs de contenus doivent rapidement éliminer ou bloquer l´accès aux informations illicites lorsqu´ils ont une connaissance réelle ou présumée de son existence.

Les états de l´UE déclarent qu´ils ne peuvent pas imposer une obligation générale aux fournisseurs de services afin qu´ils surveillent les informations qu´ils transmettent ou stockent, ou « *qu´ils recherchent activement des faits ou des circonstances révélant des activités illicites* ». Les tribunaux ou les autorités administratives peuvent toutefois exiger que les fournisseurs de services « *mettent fin ou préviennent les infractions*, ou établissent des « *procédures régissant le retrait ou le blocage de l´accès à l´information* ».[137]

Outre le domaine spécifique de la responsabilité, les droits d´auteurs ont reçu beaucoup d´attention. Dans un pays d´Amérique du nord, la responsabilité secondaire en cas de violation des droits d´auteurs est spécifiquement limitée par la législation.[138]

133 OCDE, 2011. *Le rôle des intermédiaires d´internet pour atteindre les objectifs de politique publique*. DSTI/ICCP(2010)11/FINAL, pp.13, 16-17, 24.

134 *Ibid.*

135 47 USC § 230 - Protection pour le blocage et le dépistage privés du matériel offensant.

136 Directive 2000/31/EC du Parlement européen et du Conseil du 8 Juin2000 relative à certains aspects juridiques des services de la société de l´information, notamment du commerce électronique dans le marché intérieur. OJ L 178, 17 juillet 2000, pp.1–16.

137 *Ibid.*

138 17 USC § 512 - Limitations de responsabilité concernant les contenus en ligne.

Ceci crée des sphères de sécurité pour les prestataires de services qui fournissent des communications de réseau numérique transitoire, les systèmes de mise en antémémoire, l´hébergement de contenus, et des outils de localisation de l´information. Ils requièrent généralement un système de notification et suppression, une politique pour mettre fin aux comptes des contrevenants récidivistes et la mise en place de mesures techniques basées sur les normes pour contrôler l´accès aux œuvres. Les titulaires de droits peuvent déposer une plainte et solliciter une injonction pour bloquer l´accès au matériel illicite, pour mettre fin aux comptes d´utilisateurs, ou pour tout autre recours tout aussi efficace qui soit le moins contraignant possible pour le fournisseur de services, à cet effet.

Il y a également eu un vaste débat international sur la responsabilité des intermédiaires de prendre des mesures contre la pornographie infantile. De nombreux pays d´Europe du sud, d´Asie de l´est et de l´ouest et d´Océanie exigent que les fournisseurs de services bloquent l´accès aux usagers aux sites qui contiennent ce matériel.[139] Interpol maintient une liste mondiale d´adresses de sites web qui contiennent du matériel « au caractère grave », que les fournisseurs de services sont tenus de bloquer, dans certains pays, conformément aux lois sur les télécommunications. Cependant, le Parlement européen a rejeté une proposition législative de la Commission européenne qui aurait imposé aux fournisseurs de services un blocage obligatoire dans l´UE, en laissant la décision individuelle aux états membres.[140]

Les fournisseurs d´hébergement et de services internet peuvent donc avoir un rôle essentiel dans la prévention de la cybercriminalité car leur position leur permet de connecter les personnes et les organisations à internet. Ils peuvent conserver les journaux qui pourront être utilisés durant les enquêtes sur les activités criminelles ; aider les clients à identifier les ordinateurs compromis ; bloquer certains types de contenus illicites comme les messages non sollicitéset en général maintenir un environnement de communications sécurisé pour leurs clients. Les lois sur la protection des données exigent dans plusieurs pays que les fournisseurs de services protègent les données des clients et les pouvoirs d´enquêtes doivent pouvoir garantir l´accès à ces données à la police. Les lois qui prévoient l´interférence avec la libre circulation des informations sur internet doivent aussi tenir compte des règles sur la liberté d´expression. La protection pour les fournisseurs de services et autres intermédiaires contre la responsabilité a été un facteur essentiel de la rapide croissance des services en ligne, bien que certaines responsabilités soient imposées aux fournisseurs de services comme les mesures qu´ils sont tenus de prendre lorsque des violations aux droits d´auteurs ou d´autres infractions leur sont signalées.

La participation du milieu universitaire à la prévention de la cybercriminalité

Les institutions académiques et les organisations intergouvernementales sont des intervenants importants dans la prévention et la lutte contre la cybercriminalité. Ces institutions peuvent notamment apporter une contribution avec le partage et le développement des connaissances ; le développement de politiques et de lois ; le développement de normes techniques et de technologie ; la fourniture d´assistance techniqueet la coopération avec les services répressifs.

Le partage et le développement des connaissances – en réponse aux demandes formulées par les gouvernements et l´industrie relatives aux besoins de développement de la main d´œuvre et des professionnels en matière de cybersécurité, les institutions académiques ont établi des programmes d´éducation spécialisés et des centres de formation pour consolider les connaissances et la recherche et augmenter la synergie des connaissances entre les domaines et les disciplines. Un nombre croissant d´universités proposent des diplômes, des certificats et une éducation professionnelle sur des thèmes liés à la cybersécurité et la cybercriminalité afin de promouvoir « *l´éducation et la formation de jeunes adultes et de futurs professionnels relatives aux pratiques informatiques sécurités et aux questions techniques* »[141].

139 Voir OCDE 20111. *Le rôle des intermédiaires d´internet pour atteindre les objectifs de politique publique*. DSTI/ICCP(2010)11/FINAL, p.46

140 L´article 25(2) de la Directive 2011/92/EU relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie, qui remplace la Décision cadre du Conseil 2004/68/JHA (OJ L 335, 17.12.2011)

141 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q70.

Les universités promeuvent aussi l´apprentissage appliqué et le développement de réseaux sociaux contre la cybercriminalité par le biais de l´organisation d´ateliers et de conférences. Ceci est l´occasion d´échanger des informations et des conseils sur des ripostes et des mesures préventives, de cultiver la coopération informelle, de créer des mécanismes pour signaler des actes spécifiques et de développer des solutions techniques.

Les universitaires qui contribuent aux efforts pour contrôler la cybercriminalité proviennent de diverses disciplines, qui incluent la science et l´ingénierie informatiques, le droit, la criminologie et la sociologie. Il y eut lors des deux dernières décennies une augmentation significative du nombre de revues académiques consacrées à des thèmes liés au cyberespace, à la cybersécurité et à la cybercriminalité.[142] La sensibilisation et la recherche sur des thèmes connexes ont donné lieu à un nombre croissant de rapports techniques, de recherche et de publications évaluées par les pairs, d´analyses de données des organismes et de recherches exclusives non publiées.

Le développement des lois et des politiques – les spécialistes universitaires apportent une contribution significative au développement et à l´amendement des lois et des politiques. Au niveau régional, national et international, les universitaires fournissent des conseils juridiques et élaborent des lois sur une gamme de thèmes qui incluent l´incrimination, la confidentialité et la vie privée, les protections juridiques et constitutionnelles. Ces conseils sont fournis par le biais de divers mécanismes comme la participation à des groupes consultatifs et des groupes de travail, les contrats institutionnels et individuels et les programmes d´assistance technique. Un intervenant universitaire a, par exemple, mentionné que les centres de recherche informatique ont fréquemment un rôle de coordinateurs pour *« les activités des chercheurs spécialisés dans divers domaines de travail liés à la cybercriminalité (juridique, criminologique, expertise technique) »*.

La technologie et les normes techniques – les universités réalisent des recherches en sciences pures et appliquées sur la technologie informatique, dans le contexte du secteur universitaire-privé et/ou de coopération gouvernementale, de recherche subventionnée externe ou interne, ou pour sécuriser le réseau universitaire. Les universités peuvent aussi contribuer à la criminalistique informatique, aux analyses des preuves et aux analyses de données des organismes. Outre les recherches institutionnelles et individuelles, les universités représentent aussi des partenaires importants et des facilitateurs de la coopération avec leur participation à des organisations professionnelles, des organismes de normalisation et des groupes de travail. Quelques stratégies nationales en matière de cybersécurité mentionnent explicitement le rôle joué par les universités pour sécuriser le cyberespace.[143]

Assistance technique – les programmes universitaires d´assistance technique dans le domaine de la cybercriminalité sont souvent conçus à l´intention des services répressifs nationaux et internationaux et des organismes de justice pénale et de sécurité nationale. Les universités fournissent aussi une assistance technique aux sociétés, aux petites et moyennes entreprises et à d´autres institutions académiques. Ces programmes couvrent divers domaines fondamentaux liés aux techniques d´enquêtes, à la conservation des preuves et à la criminalistique numérique ; à l´analyse des logiciels malveillants, à l´analyse des contenus (différentes des analyses criminalistiques) ; aux politiques, à la gouvernance, à la conformité, à l´élaboration et à l´amendement des lois, au soutien en matière de poursuites et de procès.[144] Conjointement aux activités de développement des connaissances et d´assistance technique, quelques universités ont développé des programmes spéciaux d´éducation, par exemple, en matière de criminalistique numérique et d´enquêtes sur la cybercriminalité, auxquels la police et les autorités gouvernementales inscrivent leurs employés comme étudiants.

La coopération avec les services répressifs – l´expertise des universités en matière de cybersécurité et de cybercriminalité favorise la coopération avec les services répressifs. Les universitaires qui ont répondu au questionnaire coopèrent avec les services répressifs par le biais du développement des connaissances, les normes techniques et l´assistance technique. Néanmoins de nombreux

répondants ont également déclaré qu´ils n´avaient pas d´interaction directe avec lesservices répressifs.[145]

142 En incluant, par exemple, « *Cyberpsychology, Journal of Psychosocial Research on Cyberspace ; Cyberspace and Intellectual Property ; Digital Evidence andElectronic Signature Law Review ; Journal of Law & Cyber Warfare ; International Journal of Cyber Behavior, Psychology, and Learning ; International Journal of Cyber Society and Education ; International Journal of Cyber Ethics in Education ; International Journal of Cyber Warfare and Terrorism ; International Journal of Cybercriminology ; International Journal of Electronic Security and Digital Forensics ; and Journal of International Commercial Law and Technology* ».

143 L´Australie, la République tchèque, l´Estonie, l´Allemagne, l´Inde, le Japon, les Pays-Bas, la Nouvelle Zélande, le Nigéria, le Royaume Uni et les États-Unis se trouvent parmi les pays dont les stratégies nationales mentionnent spécifiquement le milieu universitaire comme un partenaire et un intervenant essentiel de leurs stratégies nationales de cybersécurité.

144 Les autres thèmes incluent la coopération internationale, la criminalité organisée transnationale, la technologie et les télécommunications générales, et les questions de prévention.

145 Ceci peut être dû à la position du répondant et aux connaissances des opérations et des systèmes de gestion de risques de l´université. La majorité des répondants étaient des membres de la faculté et non du personnel en TI de l´université ou du personnel de sécurité ou de gestion de risques.

Les universitaires ont fréquemment indiqué que la disponibilité des ressources pour multiplier les efforts éducatifs et la communication représentait un problème. Un répondant a, par exemple, déclaré que : « *il n´y a pas de motifs institutionnels généraux pour la coopération– les organismes d´état n´ont pas de normes ni de budget pour la coopération avec les universités. Tous les contacts existants et la coopération dont donc informels* ». « *Le financement, la taille des effectifs et la disponibilité du personnel universitaire spécialisé* »,[146] pour appuyer les efforts de sécurité publique, sont considérés nécessaires pour améliorer les résultats, et il faut en particulier « *augmenter le financement pour la recherche en matière d´analyse et d´outils criminalistiques, et pour la formation d´un personnel compétent* ».[147] Malgré le besoin de « *plus de ressources et d´ouverture des services répressifs, et davantage de recherches appliquées dans le milieu université* »,[148] il existe un potentiel significatif pour accroître la coopération avec les institutions gouvernementales et les services répressifs.

146 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q70.
147 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q70.
148 Questionnaire de l´étude sur la cybercriminalité (OIG et universités). Q70.

Page intentionnellement laissée vierge

PREMIÈRE ANNEXE : DESCRIPTIONS DES ACTES

Actes contre la confidentialité, l´intégrité et la disponibilité des systèmes et des données informatiques	
Accès illégal à un système informatique	Se réfère à des actes qui impliquent l´accès total ou partiel à un système informatique sans autorisation ni justification. C´est le cas, lorsqu´un délinquant contourne la protection du pare-feu et entre dans le système informatique d´une banque (par exemple). Ceci peut aussi être le cas lorsqu´un usager continue à être connecté à un système informatique au-delà du temps autorisé, comme dans le cas où un contrevenant réserve la capacité d´un serveur pour une période déterminée mais continue à l´utiliser alors que la période a expiré. Certaines approches nationales requièrent que le contrevenant contourne les mesures de protection ou agisse avec une intention spécifique.
Accès illégal, interception ou acquisition de données informatiques	Se réfère à des actes qui impliquent l´accès à des données informatiques sans autorisation ni justification, et cela inclut l´obtention de données durant un processus de transmission qui ne sont pas destinées à être publiques, ainsi que l´obtention de données informatiques (en copiant les données) sans autorisation. C´est le cas, lorsqu´un délinquant accède illégalement à une base de données informatiques, à des transmissions de registres dans un réseau sans fil sans autorisation, ou lorsqu´un contrevenant, qui travaille pour une entreprise copie des fichiers pour les emmener sans autorisation. Certaines approches nationales requièrent que les données pertinentes soient protégées contre les accès non autorisés et incluent l´interception des émissions électromagnétiques qui peuvent ne pas être considérées comme des données informatiques. L´espionnage industriel peut fréquemment impliquer l´acte d´accès illégal, d´interception ou d´acquisition de données informatiques.
Interférence illégale de données ou de systèmes informatiques	Se réfère à des actes qui entravent le fonctionnement d´un système informatique ainsi qu´aux actes qui impliquent des dommages causés aux données informatiques ainsi que leur détérioration, altération ou suppression sans autorisation ni justification. C´est, par exemple, le cas lorsqu´un délinquant soumet une telle quantité de demandes à un système informatique que celui-ci ne peut plus répondre aux demandes légitimes (ceci est appelé une attaque par déni de service), élimine des fichiers de programmes informatiques nécessaires au bon fonctionnement d´un serveur internet, ou altère des registres d´une base de données informatiques. Certaines approches nationales contemplent seulement les actes liés aux données alors que d´autres couvrent également les manipulations du matériel informatique. Le piratage des systèmes informatiques des infrastructures essentielles (comme les systèmes de distribution d´électricité ou d´eau) peut donner lieu à une interférence illégale de données ou à des dommages causés au système
Production, distribution, ou possession d´outils informatiques malveillants tools	Se réfère à des actes qui impliquent le développement ou la distribution de solutions logicielles ou de matériel informatique qui peuvent être utilisées pour commettre une infraction liée à l´informatique ou à internet. C´est, par exemple, le cas lorsqu´un délinquant développe un outil logiciel pour automatiser des attaques de déni de service. Afin d´éviter une interférence avec l´utilisation légitime de ces outils (par des experts en sécurité), certaines approches nationales requièrent que l´outil soit exclusivement destiné à des fins illégales ou que la personne agisse avec l´intention d´utiliser l´outil pour commettre un délit.
Mesures de protection contre la violation de données ou de la vie privée	Se réfère à des actes qui impliquent l´utilisation d´un système informatique pour traiter, diffuser, obtenir ou accéder à des informations personnelles en violation des dispositions sur la protection des données. C´est, par exemple, le cas lorsqu´un contrevenant exploite un commerce en ligne et divulgue des informations personnelles de la base de données de ses clients dont il devait garder la confidentialité.

Fraude ou falsification informatique	Se réfère à des actes qui impliquent l´accès illégal ou l´interférence avec des données ou un système informatique avec l´intention d´obtenir de l´argent de manière trompeuse ou malhonnête ou d´autres bénéfices économiques ou d´évader une responsabilité, ainsi que les actes qui impliquent une interférence avec des données ou un système informatique de façon à créer de fausses données informatiques. C´est, par exemple, le cas lorsqu´un délinquant modifie le logiciel utilisé par une banque pour rediriger le processus de transfert d´argent vers son propre compte, ou lorsqu´un délinquant modifie un courriel authentique d´une institution financière avec l´intention sous-jacente de commettre une fraude. L´envoi de ces messages est une tentative pour obtenir des informations personnelles ou pour commettre une fraude. Cela est également appelé « hameçonnage ». Pour ce qui concerne les falsifications liées à l´informatique, certaines approches nationales requièrent que les données informatiques originales concernant la documentation soient destinées à créer des obligations juridiques contraignantes, d´autres requièrent seulement que le délinquant tente que la version modifiée résultante soit prise en compte ou utilisée comme si elle était authentique
Infractions informatiques liées à l´identité	Se réfère à des actes qui impliquent le transfert, la possession ou l´utilisation sans justification du moyen d´identification d´une autre personne, avec l´intention de commettre, aider ou encourager des activités criminelles illicites. C´est, par exemple, le cas lorsqu´un délinquant obtient sans autorisation des informations relatives à un permis de conduire d´un système informatique et vend ces données ou les utilise pour dissimuler sa véritable identité lorsqu'un délit est commis. Certaines approches nationales limitent l´application de ces dispositions à certains instruments d´identification.
Infractions informatiques liées aux droits d´auteurs et aux marques déposées	Se réfère à des actes qui impliquent le fait de copier du matériel stocké dans des données informatiques ou de générer des données informatiques en violant les protections des droits d´auteurs et des marques déposées. C´est, par exemple, le cas lorsqu´un délinquant distribue une chanson protégée par des droits d´auteurs par le biais d´un système de partage de fichier sans la permission du titulaire des droits d´auteurs.

Envoi ou contrôle de l´envoi de messages non sollicités	Se réfère à des actes qui impliquent l´utilisation d´un système informatique pour envoyer des messages à un grand nombre de destinataires sans autorisation ni demande préalable. Afin d´éviter une interférence avec les activités régulières des communications des clients, certaines approches nationales exigent que le contrevenant mentionne de fausses informations d´en-tête dans ces messages.
Actes liés à l´informatique causant un préjudice personnel	Se réfère à des actes qui impliquent l´utilisation d´un système informatique pour harceler, tyranniser, menacer, traquer, intimider ou terroriser un individu. C´est, par exemple, le cas lorsqu´un délinquant envoie des images ou des messages insultants, menaçants, offensifs ou abusifs (ceci est aussi appelé « trolling »), ou utilise un système informatique pour traquer, surveiller ou interférer avec le bien être émotionnel ou physique d´un individu. Les actes qui constituent seulement une diffamation sont exclus de cette catégorie.
Actes liés à l´informatique impliquant du racisme ou de la xénophobie	Se réfère à des actes qui impliquent l´utilisation d´un système informatique pour distribuer ou mettre à disposition un matériel raciste et xénophobe, ou pour menacer ou insulter un individu ou un groupe de personnes pour des raisons racistes ou xénophobes. Le terme matériel raciste et xénophobe désigne tout matériel écrit, toute image ou autre représentaion d´idées ou de théories qui préconisent, promeuvent ou encouragent la haine, la discrimination ou la violence contre un individu ou un groupe de personnes pour des raisons de race, de couleur ou d´origine ethnique, ou de religion si cela est utilisé comme un prétexte pour l´un de ces facteurs .
Production, distribution, ou possession de pornographie infantile liées à l´informatique	Se réfère à des actes qui impliquent l´utilisation d´un système informatique pour produire, créer, distribuer, accéder, visionner, recevoir, stocker ou posséder une représentation, par un moyen quelconque, d´une personne réelle ou fictive mineure ou paraissant être âgée de moins de 18 ans, s´adonnant à des activités sexuelles explicites réelles ou simulées ou toute représentation des organes sexuels d´un enfant à des fins principalement sexuelles. C´est, par exemple, le cas lorsqu´un délinquant télécharge une photo numérique qui montre un abus sexuel commis sur un enfant.
Sollicitation ou prédation sexuelles des enfants liées à l´informatique	Se réfère à des actes qui impliquent l´utilisation d´un système informatique pour proposer une rencontre à un enfant qui n´a pas atteint la majorité sexuelle, à des fins sexuelles. C´est, par exemple, le cas lorsqu´un délinquant discute sur internet avec un enfant en prétendant être aussi un enfant, et propose une rencontre à l´enfant avec l´intention d´abuser de l´enfant. Ce comportement est aussi appelé « prédation sexuelle ». Certaines approches nationales peuvent limiter l´infraction aux cas où la sollicitation est suivie d´un acte matériel qui entraîne une rencontre.
Actes d´appui auterrorisme liés à l´informatique	Se réfère à des actes qui impliquent l´utilisation d´un système informatique pour appuyer des infractions de terrorisme. Ceci inclut l´utilisation d´un système informatique pour communiquer un message au public, avec l´intention d´inciter à commettre un délit de terrorisme, lorsqu'un tel comportement, qu'il préconise directement ou non de commettre des infractions terroristes, crée un danger qu'une ou plusieurs de ces infractions puissent être commises (« incitation au terrorisme » liée à l´informatique). Ceci inclut aussi l´utilisation d´un système informatique pour recueillir ou mettre à disposition des fonds avec l »intention qu »ils soient utilisés, partiellement ou totalement, pour l'exécution d'un acte terroriste (délit de financement du terrorisme lié à l´informatique). Ceci inclut aussi l´utilisation d´un système informatique pour la planification, la préparation ou l´organisation d´un acte de terrorisme (délit de planification de terrorisme lié à l´informatique). Un délit de terrorisme signifie tout acte établi en conformité avec les instruments juridiques internationaux contre le terrorisme, ou destiné à causer la mort ou des dommages corporels graves à toute personne civile, ou à toute autre personne qui ne participe pas directement aux hostilités dans une situation de conflit armé, lorsque par sa nature ou son contexte cet acte est destiné à intimider une population, ou à contraindre un gouvernement ou une organisation internationale à accomplir ou à s´abstenir d´accomplir un acte quelconque.

ANNEXE DEUX : MESURER LA CYBERCRIMINALITÉ

Statistiques sur les délits enregistrés par la police

Les statistiques sur les délits enregistrés par la police sont généralement considérées comme les statistiques les plus proches des faits criminels.[1] Néanmoins, il est bien connu que les délits enregistrés par la police représentent seulement les faits dont la police a pris connaissance. Par conséquent, cela dissimule généralement « le chiffre noir » (souvent important) de la criminalité.[2]

Pour les actes de cybercriminalité, la différence entre la victimisation et les délits enregistrés par la police peut représenter divers ordres de grandeur. La victimisation des fraudes en ligne pour les cartes de crédit des consommateurs signalée dans les enquêtes sur la population peut, par exemple, être 80 fois plus élevée que le total des fraudes et des falsifications informatiques enregistrées par la police dans le même pays.[3] Conformément à une enquête sur la population qui portait sur presque 20 000 utilisateurs d´internet dans 24 pays, seulement 21 % des répondants qui dirent avoir été victimes d´un acte de cybercriminalité l´avaient signalé à la police.[4]

Une autre difficulté relative aux statistiques sur les délits enregistrés par la police est le développement d´une approche comparative internationale pour identifier l´implication des données ou des systèmes informatiques dans un acte spécifique. Les systèmes de signalement des incidents de la police nationale ont plusieurs manières pour enregistrer un acte comme un cyberdélit. Les champs d´enregistrement peuvent utiliser des indicateurs comme « *si l´ordinateur a été l´objet d´un délit* » ou « *si l´auteur du délit a utilisé un équipement informatique pour commettre le délit* ».[5] D´autres approches sont basées sur des articles de la législation pénale nationale et couvrent donc seulement un nombre limité d´actes de cybercriminalité, comme « l´usage abusif de l´informatique ».[6] Ceci donne lieu à des statistiques policières qui vont des actes conventionnels où un ordinateur a été l´outil ou l´objet du délit, à des statistiques concernant seulement des infractions spécifiques en matière de technologie.[7] Dans le premier cas, il peut être difficile d´appréhender le seuil et la signification de l´utilisation de l´équipement informatique pour « perpétrer » un délit particulier.[8] Dans le second cas, les comparaisons transnationales peuvent être faites seulement si les législations nationales – et les catégories correspondantes utilisées à des fins statistiques – sont équivalentes. Pour comprendre, par exemple, si les statistiques de la police concernant « *l´accès informatique non autorisé* » dans un pays peuvent être comparées aux statistiques concernant « *l´accès informatique illégal* » dans un autre pays, il est nécessaire d´examiner les éléments sous-jacents de l´infraction dans les droits pénaux respectifs. Méthodologiquement, il est donc très difficile de justifier les comparaisons des statistiques sur la cybercriminalité de la police.

Les informations collectées pour l´étude incluaient la demande, formulée aux pays, de fournir le nombre d´infractions enregistrées par la police correspondant à chacun des 14 actes énumérés dans la première Annexe (Descriptions des actes).

---

1 Nations Unies. 2003. *Manuel pour développer un système de statistiques de justice pénale.*

2 Nations Unies. Douzième congrès des Nations Unies sur la prévention de la criminalité et la justice pénale. 2010. *Etat de la criminalité et de la justice pénale dans le monde : Rapport du secrétaire général.* A/CONF.213/3. 1 février 2010.

3 ONUDC calculs à partir du questionnaire de l´étude sur la cybercriminalité. Q30 ; et Symantec. 2012. *Rapport Norton sur la cybercriminalité 2012.*

4 Symantec. 2011. *Rapport Norton sur la cybercriminalité 2011.*

5 Département de Justice des États Unis. Bureau fédéral d »enquête (FBI). 2000. *Système national de signalement des incidents. Volume 1 : directives sur la collecte des données.* Disponible sur http ://www.fbi.gov/about-us/cjis/ucr/ucr

6 Voir, par exemple, la Commission économique des Nations Unies pour l´Europe, la Conférence des statisticiens européens. *Principes et cadre pour une Classification internationale des délits à des fins statistiques.* ECE/CES/BUR/2011/NOV/8/Add.1. 11 octobre 2011. L´Annexe I synthétise les systèmes nationaux de classification des délits.

7 Centre canadien de la statistique juridique. 2002. Cybercriminalité *: questions, sources de données et faisabilité de la collecte de données auprès de la Police.*

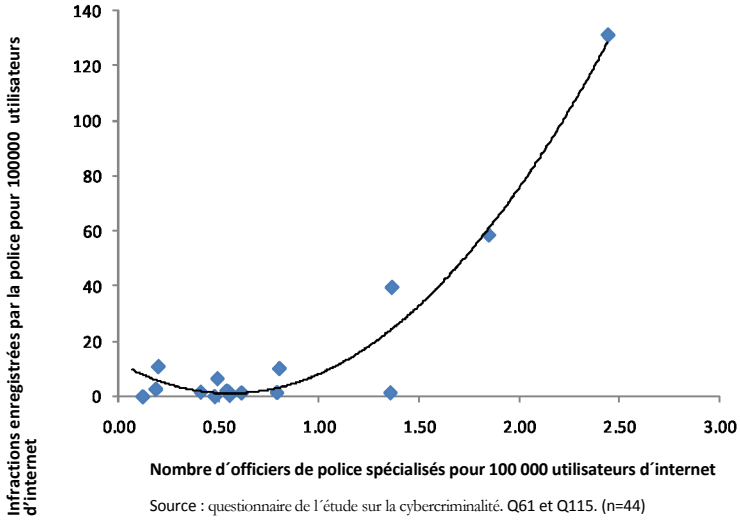
8 Les statistiques historiques peuvent inclure le nombre de « vol de véhicule à moteur » ou « cambriolage/entrée par effraction » dans lesquels un ordinateur a été l´outil ou l´objet de l´infraction .*Ibid.*

Pour chaque description d´acte, on demanda aux répondants de fournir les statistiques disponibles des années 2008, 2009 et 2010, et de spécifier si les données fournies correspondaient, selon le droit, à un cyberdélit spécifique ou à une infraction générale.[9] Par exemple, les infractions enregistrées par la police pour « *accès illégal à un système informatique* » peuvent être enregistrées sur la base d´une disposition pénale spécifique qui couvre cet acte. Les infractions enregistrées par la police pour « *fraude ou falsification liée à l´informatique* », peuvent, par ailleurs, correspondre à une sous-catégorie de l´infraction générale de fraude dans laquelle a été identifiée l´implication d´un ordinateur.

Parmi les pays qui ont répondu aux questions sur les statistiques de la police, pour les 14 actes de cybercriminalité (et 3 catégories additionnelles), moins de 40 % des pays ont indiqué que les statistiques enregistrées pour ces infractions étaient disponible. Moins de 20 % des champs de données possibles – concernant tous les actes de cybercriminalité et les années – furent complétés.[10] Ceci peut indiquer qu´il est difficile pour de nombreux pays de collecter les statistiques enregistrées par la police relatives aux actes de cybercriminalité. Lorsqu´on leur demanda la raison pour laquelle les statistiques n´étaient pas disponibles, de nombreux pays mentionnèrent les difficultés de désagrégation et d´agrégation – que les actes requis ne se distinguent pas des actes enregistrés, ou que les données ne puissent pas être facilement compilées en fonction des catégories utilisées par le questionnaire.[11] Ceci démontre les difficultés pour déterminer une classification commune des cyberdélits qui pourrait être utilisée à des fins statistiques. Plusieurs pays ont associé les difficultés relatives aux statistiques policières aux cadres juridiques et ont signalé que l´absence de dispositions juridiques spécifiques signifiait qu´il n´existait aucune catégorie correspondante dans les statistiques policières. Dans les cas où il n´existait pas de disposition spécifique certains pays fournirent une estimation. Un pays fournit, par exemple, le nombre total d´infractions de falsifications ou de fraudes enregistrées par la police, avec l´estimation du pourcentage d´infractions commises en utilisant un système informatique.[12]

Un pays déclara, par exemple, que « *des ressources limitées et la nature complexe de la cybercriminalité rendent très difficiles la collecte et l´analyse des données statistiques d´une manière qui pourrait offrir une vision complète et précise du problème aux gouvernements, au secteur privé et aux utilisateurs de la technologie. Les éléments de la cybercriminalité sont souvent accessoires à d´autres infractions pénales, de nombreux actes ne sont jamais signalés par les victimes ou sont signalés aux compagnies de cartes de crédit ou aux fournisseurs de services et non aux autorités publiques. Un problème supplémentaire dans ce domaine est le fait que de nombreuses infractions sont transnationales ou d´origine incertaine, et de nombreuses infractions impliquent un ciblage massif de victimes, et cela peut fournir des données statistiques différentes en fonction de la manière de les comptabiliser : le simple acte d´envoyer un courriel frauduleux à des millions d´adresses peut été compté comme un seul ou plusieurs millions de tentatives, par exemple, et pourrait générer des milliers d´infractions commises si l´acte criminel a réussi* ».[13]

Rapports entre la police spécialisée et les infractions enregistrées (fraude ou falsification informatique)



Source : questionnaire de l´étude sur la cybercriminalité. Q61 et Q115. (n=44)

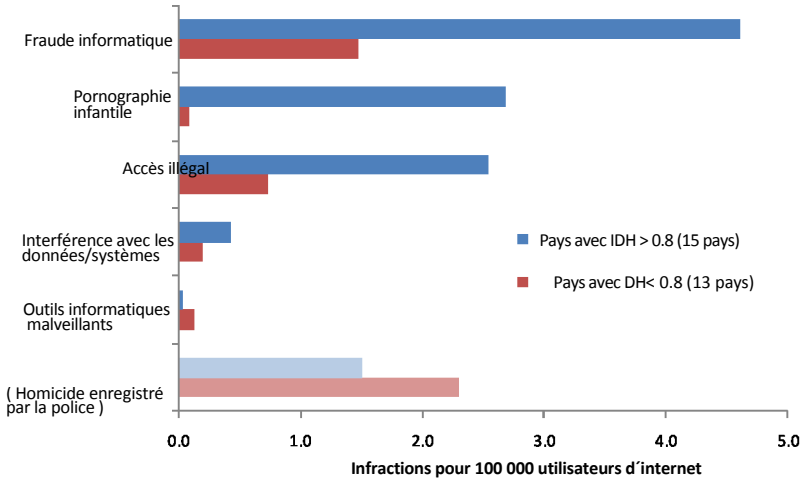
9 Questionnaire de l´étude sur la cybercriminalité Q54-71.
10 *Ibid.*
11 Questionnaire de l´étude sur la cybercriminalité. Q75.
12 Questionnaire de l´étude sur la cybercriminalité Q61.
13 Questionnaire de l´étude sur la cybercriminalitéQ76.

L´examen des statistiques de la police montre de nombreux patrons. Tout d´abord, il y a de nombreux indices indiquant – comme le suggérait la comparaison avec les données d´une enquête sur les victimes – que les cyberdélits enregistrés par la police ne sont pas un bon indicateur des niveaux sous-jacents de cybercriminalité.

Le taux des infractions spécifiques de cybercriminalité enregistrées par la police peut être associé au niveau de développement d´un pays et à la capacité de la police spécialisée. Le nombre de pays qui ont fourni des données est relativement bas. Toutefois, pour ce groupe restreint de pays, ceux qui disposent de nombreux agents de police spécialisés en cybercriminalité enregistrent un nombre plus élevé d´infractions de cybercriminalité – du moins pour les falsifications et les fraudes liées à l´informatique.[14] La comparaison est illustrée en montrant le nombre d´agents de police spécialisés et le nombre d´infractions enregistrées pour 100 000 utilisateurs d´internet dans chaque pays, afin de fournir un dénominateur équitable pour la comparaison.[15]

Ce patron s´explique probablement par le fait que la police prend connaissance de seulement un petit pourcentage des actes de cybercriminalité, et ce pourcentage pourrait vraisemblablement être accru avec l´utilisation de ressources et de capacités d´enquête additionnelles.[16] Un second patron est lié aux statistiques de la police et au niveau de développement des pays. Quatre types d´actes de cybercriminalité enregistrés par la police—la fraude ou la falsification informatique, les infractions de pornographie infantile, l´accès illégal à un système informatique et l´interférence illégale avec des données ou des systèmes informatique – sont plus élevés pour chaque 100 000 utilisateurs d´internet dans le groupe de pays qui ont de très hauts niveaux de développement humain, que pour le groupe de pays qui ont un développement humain plus bas. La figure montre le nombre moyen d´infractions enregistrées par la police pour 100 000 utilisateurs d´internet dans 15 pays dont le IDH est supérieur à 0.8, par rapport aux 13 pays dont le IDH est inférieur à 0.8.[17] Il est possible que les niveaux absolus de certains de ces délits soient en fait plus élevés dans les pays les plus développés. Les résultats de l´enquête sur la population pour les fraudes aux consommateurs liées à l´informatique, montrent un niveau de victimisation légèrement plus élevé dans les pays les plus développés.[18] Néanmoins, les enquêtes suggèrent une situation inverse pour les autres actes de cybercriminalité dont sont victimes les personnes – avec des niveaux généralement plus élevés de victimisation dans les pays les moins développés.[19] La situation des ressources de la police, associée au fait que les homicides enregistrés par la police [20] sont plus élevés dans les pays moins développés, peut suggérer que la plus grande capacité de la police en matière d´enquêtes sur la cybercriminalité dans les pays développés est responsable,

Actes de cybercriminalité enregistrés par la police, par niveau de développement du pays



Source : questionnaire de l´étude sur la cybercriminalité. Q54-70. (n=28)

14 Questionnaire de l´étude sur la cybercriminalité. Q115 et Q61.

15 Nombre d´utilisateurs d´internet provenant des indicateurs des télécommunications /TIC dans le monde 2012. Le nombre des utilisateurs est utilisé comme la base au lieu de la population totale car les personnes qui ne sont pas en ligne ne sont pas en principe vulnérables à la victimisation de la majorité des actes de cybercriminalité – malgré des exemples d´ acquisition illégale de données informatiques à partir d´un ordinateur autonome.

16 Voir, par exemple, Harrendorf, S., Smit, P. 2010. Les attributs du système de justice pénale – les ressources, les performances et le caractère punitif. *dans* : Institut européen pour la prévention du crime et la lutte contre la délinquance, affilié à l'Organisation des
Nations Unies(HEUNI). *Statistiques internationales sur la criminalité et la justice*. Helsinki.

17 Questionnaire de l´étude sur la cybercriminalité Q55, Q57, Q58, Q61, et Q68.

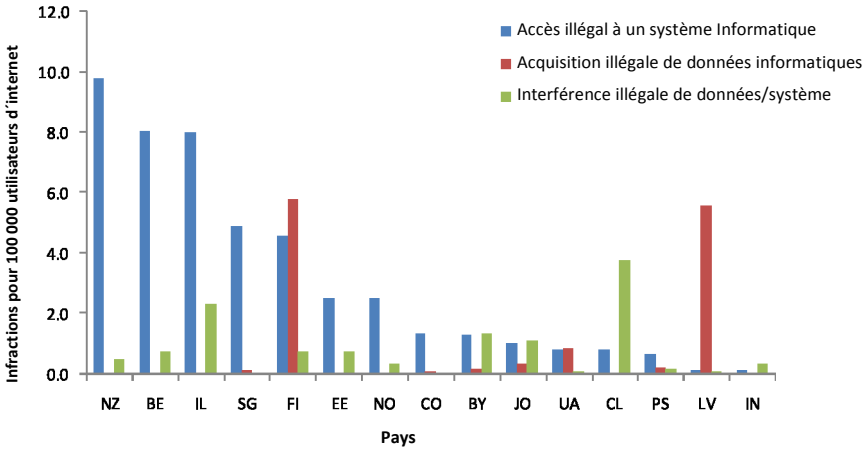
18 Voir, par exemple, Van Dijk, K.J.M., Van Kesteren, J.N., et Smit, P. 2008. *Victimisation criminelle dans le contexte international. Principaux résultats de 2004-2005 ICVS et EU ICS*. La Hague : Boom Legal Publishers.

19 Pour ce qui concerne, par exemple, la pornographie infantile voir ONUDC. 2010. *La mondialisation du crime : une évaluation de la menace du crime transnational organisé*, chapitre 10.

20 Les taux des homicides enregistrés par police sont présentés pour 100 000 membres de la population, au lieu de 100 000 utilisateurs d´internet.

en partie, des importantes différences entre les deux groupes de pays examinés. Il existe un second patron qui complique l´interprétation des statistiques sur les cyberdélits enregistrés par la police, qui concerne les différences dans l´utilisation comparative des infractions des services répressifs. Les actes d´accès illégal à un système informatique, d´acquisition illégale de données informatiques et d´interférence illégale avec des données ou des systèmes informatiques, représentent généralement des conduites distinctes selon le droit. Cependant, dans la pratique, ils peuvent être combinés dans une seule conduite – comme dans le piratage d´un système informatique, la reproduction de données informatiques d´un système et la corruption de données informatiques d´un système. Une, deux ou trois infractions séparées peuvent être enregistrées par la police, en fonction de la disponibilité des preuves, de la caractérisation de la conduite, des priorités politiques et des règles de dénombrement des infractions.[21] L´examen des statistiques enregistrées par la police pour trois infractions dans la catégorie des « *actes contre la confidentialité, l´intégrité et la disponibilité des données et des systèmes informatiques* » montre des variations significatives selon les pays. Il n´existe pas de relation claire entre ces trois infractions. Ce n´est pas le cas pour toutes les catégories qui montrent des niveaux relativement équivalents dans chaque pays. De plus, dans certains pays, une catégorie est plus élevée que les deux autres catégories, dans d´autres pays deux catégories sont plus élevées. De nombreux pays n´ont pas de statistiques disponibles pour les trois catégories. Même s´il n´est pas prouvé que ces différences ne reflètent pas les caractéristiques sous-jacentes réelles des infractions, cette diversité est probablement due aux effets d´enregistrement et d´enquête. Quand on leur demanda s´ils considéraient que le système statistique actuel de la police pour enregistrer les actes de cybercriminalité était suffisant, deux tiers des pays répondants considéraient que leur système national était insuffisant.[22] Les répondants déclarèrent que le système d´enregistrement des statistiques de la police pouvait être amélioré de nombreuses façons, ceci est détaillé dans l´encadré de cette page.[23]

Actes contre les données et les systèmes informatiques enregistrés par la police par pays déclarant



Source : questionnaire de l´étude sur la cybercriminalité. Q54-70.

Amélioration des statistiques de la police sur la cybercriminalité

- Installer un signal dans le système d´enregistrement pour identifier les éléments de cybercriminalité des délits
- établir un seul organisme centralisé d´enregistrement pour les statistiques relatives à la justice pénale et aux services répressifs.
- Développer des règles de dénombrement normalisées- en particulier pour les actes qui visent de multiples victimes (comme l´hameçonnage).
- Développer les systèmes de classification des délits pour qu´ils reflètent la cybercriminalité.

21 L´application des principes des règles de l´infraction peut donner lieu à ce que soient enregistrés seulement les infractions les plus graves d´une conduite. Questionnaire de l´étude sur la cybercriminalité Q73.
22 Questionnaire de l´étude sur la cybercriminalité Q76.
23 *Ibid.*

Malgré ces limitations, les pays ont déclaré que les statistiques sur les actes de cybercriminalité enregistrés par la police étaient importantes pour développer des politiques de lutte contre la cybercriminalité. Un pays a, par exemple, déclaré que « *tous les quatre ans, les statistiques de la police ainsi que les informations sur l´impact, les menaces et la vulnérabilité, y compris les cyberdélits, sont analysés dans le réseau de sécurité de la police nationale et cela est ensuite utilisé pour établir les priorités du plan national de sécurité pour la police et la justice* ».[24] Plusieurs pays ont déclaré que les statistiques de la police ne devraient pas être utilisées isolément et qu´il valait mieux les associer à d´autres sources de données. Les pays ont signalé que cela était notamment le cas pour la cybercriminalité, car le long processus nécessaire pour générer les statistiques enregistrées par la police ne correspondait pas au rythme des changements technologiques ou des tendances de la cybercriminalité. Les informations provenant de l´évaluation des experts sur les changements technologiques actuels et anticipés, ainsi que l´expérience relative aux infractions actuelles et au développement de la jurisprudence devraient être intégrées aux tendances statistiques. D´autres pays ont mentionné que les statistiques sur les actes de cybercriminalité enregistrés par la police étaient importantes pour les processus de réforme législative et pour sensibiliser le public sur la nature et la portée de la cybercriminalité.[25]

Enquêtes sur la population et les entreprises

Les enquêtes sur la victimisation des délits sont généralement considérées comme l´un des moyens les plus efficaces de collecter des statistiques sur les délits. Elles éliminent, en principe, l´incertitude créée par le « chiffre noir » des délits qui ne sont pas signalés à la police, en recueillant les informations directement auprès de la population des potentielles victimes.[26] En même temps, les enquêtes sur la victimisation des délits comportent leurs propres difficultés méthodologiques, comme la nécessité d´identifier soigneusement la population cible, de concevoir un instrument d´enquête et des bases d´échantillonnage appropriés et de traiter de manière adéquate la non-réponse du sondage.[27] Néanmoins, si une formulation de question et une méthodologie normalisées sont adoptées, les enquêtes sur la victimisation des délits peuvent offrir un niveau raisonnable de comparabilité transnationale.[28] Les enquêtes sur la victimisation des délits, nationales et internationales, n´ont pas jusqu´à présent incorporé systématiquement des questions normalisées en matière de cybercriminalité. Certaines enquêtes nationales sur la population mentionnent *« des expériences négatives lors de l´utilisation d´internet, »*[29] *« des incidents de logiciels malveillants, »*[30] ou *« des menaces d´agression liées à l´informatique »* ou *« des fraudes sur internet »*.[31] D´autres enquêtes nationales couvrent des délits connexes qui peuvent ou non impliquer des donnés ou des systèmes informatiques, comme le *« vol d´identité »*[32] et le *« clonage de cartes bancaires »*.[33] Les enquêtes régionales ont aussi inclus des questions sur la *« réception de courriels frauduleux demandant de l´argent », « des fraudes en ligne où les biens achetés ne sont pas livrés, sont contrefaits ou sont distincts de ceux annoncés »* et *« trouver par hasard du matériel promouvant la haine raciale ou l´extrémisme religieux »*.[34] Les enquêtes internationales, comme les EIVC,[35] incluent seulement une question directement liée à la cybercriminalité – relative aux fraudes lors d´achats sur internet.[36] Les enquêtes sur la population effectuées par le secteur privé posaient des questions sur *« des réponses à de faux sites web ou de faux courriels qui comprenaient des informations personnelles*, « *l´intimidation, le harcèlement, les crimes de haine en ligne » « le piratage de compte de messagerie ou de profils de réseaux sociaux, » « les fraudes de cartes de crédit en ligne, »*[37] et *« les vols de données commis sur internet »*.[38]

24 Questionnaire de l´étude sur la cybercriminalité Q77.
25 *Ibid.*
26 Pour une révision générale de la méthodologie des enquêtes sur la victimisation des délits, voir ONUDC/CEE 2010. Manuel sur les enquêtes de victimisation
27 *Ibid.*
28 Voir, par exemple, Van Dijk, K.J.M., Van Kesteren, J.N., and Smit, P. 2008. *Victimisation criminelle dans le contexte international. Principaux résultats de 2004-2005 ICVS et EU ICS*. LaHague : Boom Legal Publishers.
29 Ministère britannique de l´intérieur. 2012. *crime de haine, cyber sécurité et l´expérience de la criminalité chez les enfants : résultats de 2010/11. Enquête britannique sur la criminalité : Volume supplémentaire 3 sur la criminalité en Angleterre et dans le pays de Galles 2010/11.*
30 AusCert. 2008. *Enquête sur la sécurité des utilisateurs d´ordinateurs particuliers 2008.*
31 Hong Kong *EIVC*. 2010. *Rapport final du EIVC de 2006 de Hong Kong.*
32 Département de Justice des États Unis, Bureau des statistiques judiciaires. 2008. *Supplément sur le vol d´identité de l´enquête nationale sur la victimisation des délits 2008.*
33 INEGI. 2012. *Encuesta Nacional de Victimizacion y Percepcion sobre Seguridad Priblica 2012 (ENVIPE), Cuestionario Principal.*
34 Commission européenne. 2012. *Eurobaromètre spécial 390 : Cybersécurité.*
35 Pour des détails sur l´enquête internationale sur les victimes des délits, voir http ://www.crimevictimsurvey.eu et http ://rechten.uvt.nl/icvs
36 *EIVC*2010, le questionnaire inclut un questionnaire de suivi pour les répondants qui ont indiqué avoir été victimes de fraudes aux consommateurs. La question était « comment la fraude a-t´elle eu lieu ? Dans quelles circonstances [achats sur internet ?] »
37 Symantec. 2012. *Rapport Norton sur la cybercriminalité 2012.*

Les organisations du secteur privé effectuent des enquêtes sur la victimisation des entreprises en matière de cybercriminalité.[39] Certaines de ces enquêtes utilisent un échantillon statistique, mais la majorité sont des enquêtes sur des clients ou sur des informateurs clés sélectionnés. Quelques enquêtes nationales gouvernementales couvrent aussi la victimisation des entreprises.[40] De plus, l´enquête communautaire Eurostat sur l´utilisation des TIC dans les entreprises a récemment inclus des questions sur la cybercriminalité et la cybersécurité dans un module spécialisé.[41] Les questions posées dans les enquêtes sur les entreprises utilisent souvent le terme « incident de sécurité » pour couvrir une ample gamme d´actes de cybercriminalité, y compris l´accès illégal par piratage ou par l´intrusion d´un système étranger, l´interférence avec des systèmes/données sous la forme d´une infection avec un logiciel malveillant ou d´une attaque DDoS, une fraude informatique commise par des initiés ou l´acquisition illégale de données informatiques sous la forme d´une violation de données. Il existe une diversité significative dans l´utilisation de la terminologie, dans la manière dont les questions sont posées et dans la fréquence d´inclusion de questions liées à la cybercriminalité dans les enquêtes de victimisation. Il n´est pas rare que des questions concernant la cybercriminalité soient incluses dans des « modules » spéciaux des principales enquêtes périodiques de victimisation – et cela rend difficile l´élaboration de données en séries chronologiques. Quelques enquêtes incluent les pays en développement,[42] mais les enquêtes se concentrent principalement sur les pays développés et il existe un besoin urgent de données d´enquêtes d´une grande partie du monde. Lors de la collecte des informations pour l´étude, très peu de pays étaient à même de fournir des informations sur les enquêtes de population ou les enquêtes d´entreprises pertinentes en matière de cybercriminalité.[43] Lorsque les données des enquêtes étaient disponibles, elles faisaient l´objet de nombreuses critiques – concernant les difficultés pour obtenir un échantillon représentatif, non seulement de la population à risque, mais également de la population qui avait souffert des pertes dues à la cybercriminalité.[44] Développer davantage la méthodologie et la structure des questions sera essentiel pour les futurs efforts visant à mesurer la nature et la portée de la cybercriminalité. Bien que la cybercriminalité soit – à certains égards – une criminalité difficile à mesurer en raison des définitions et du manque de sensibilisation, il existe des précédents pour l´adaptation des méthodologies des enquêtes de victimisation à d´autres délits difficiles à mesurer, comme la violence envers les femmes.[45] De plus, de récents changements dans les EIVC se sont concentrés sur des essais de méthodologies d´enquêtes basées sur internet[46] – ce qui représente une étape importante lorsque la population d´intérêt sont les « utilisateurs d´internet ». Une récente feuille de route pour améliorer les statistiques sur les crimes au niveau national et international souligne l´importance de développer et de tester des enquêtes statistiques pour collecter des données sur des formes spécifiques de cybercriminalité.[47] Dans l´étude, les données statistiques internationalement comparables d´une enquête de population sont utilisées dans la section sur « la perspective d´ensemble de la cybercriminalité ».

38 McAfee/ Alliance nationale de cybersécurité. 2012. *Enquête sur la cybersécurité en ligne.*

39 Voir, par exemple, Computer Security Institute. 2011. *Enquête sur la sécurité et les délits informatiques du CSI 2010/2011* ; PricewaterhouseCoopers.
2012. *état global des enquêtes sur la sécurité de l´information* ; Ponemon/Check Point Software Technologies. 2012. *L´impact de la cybercriminalité sur les entreprises*et Ponemon/HP Enterprise Security. 2012. *Coûts des études sur la cybercriminalité 2012.*

40 Voir, par exemple, Département de Justice des États Unis, Bureau de statistiques judiciaires. 2006. *Enquête nationale sur la sécurité informatique* et l´institut australien de criminologie. 2009. *L´évaluation des entreprises australiennes de la sécurité informatique des utilisateurs : une enquête nationale.*

41 Eurostat. 2011. *Enquête communautaire sur l´usage des TIC et le commerce électronique dans les entreprises.* Disponible sur http ://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

42 Voir, par exemple, Symantec. 2012. *Rapport Norton sur la cybercriminalité 2012* (inclut l´Afrique du sud), et Pricewaterhouse Coopers.2011.
la Cybercriminalité : une protection contre la menace croissante. Enquête mondiale sur les délits économiques (couvre 78 pays y compris 13 pays d´Afrique).

43 Questionnaire de l´étude sur la cybercriminalité Q10.

44 Florêncio, D., Heetrley, C. 2011. *Enquêtes sur le sexe, les mensonges et la cybercriminalité.* Disponible sur : http ://research.microsoft.com/pubs/149886/sexliesandcybercrimesurveys.pdf

45 Voir Johnson, H., et Nevala. S. 2010. *Enquête internationale sur la violence contre les femmes(IVAWS).*

46 Voirhttp ://crimevictimsurvey.eu

47 La Commission statistique des Nations Unies. 2012. *Rapport de l´institut national mexicain de statistiques et de géographie et de l´ONUDC sur les statistiques sur la criminalité : une feuille de route pour améliorer les statistiques sur la criminalité au niveau national et international* E/CN.3/2013/11 du 19 décembre 2012.

Initiatives de signalement pour les victimes

Les victimes d´un cyberdélit préfèrent souvent le signaler à un centre de signalement spécialisé en matière de cybercriminalité, comme un site web ou une ligne d´assistance plutôt que d´utiliser les voies traditionnelles de la police (bien qu´il y ait généralement des liens étroits entre les centres de signalement et les services répressifs). Ces initiatives de signalement existent dans de nombreux pays, y compris des pays de l´Asie du sud,[48] d´Amérique centrale,[49] d´Europe de l´ouest[50] et d´Amérique du nord.[51] Les sites de signalement volontaire pour les victimes sont également de plus en plus nombreux dans les pays en développement, comme en Afrique de l´ouest.[52] Comme dans le cas des statistiques de la police, les données provenant des centres de signalement de la cybercriminalité ont un important « chiffre noir » d´actes non signalés. Leur utilisation pour des comparaisons internationales des niveaux de cybercriminalité n´est donc pas appropriée. Même les tendances des plaintes peuvent être aussi bien dues aux niveaux de sensibilisation des victimes qu´aux faits sous-jacents.[53] Néanmoins, les statistiques provenant des mécanismes de signalement pour les victimes fournissent un aperçu de la répartition des actes de cybercriminalité dans un pays déterminé. Les statistiques peuvent, par exemple, montrer des caractéristiques comme plus de types de fraudes informatiques signalées, la répartition par âge et par sexe des victimes ou la nature du contenu illégal signalé.[54] Comme dans le cas des statistiques enregistrées par la police, la comparabilité des données des signalements des victimes peut être renforcée par le développement de classifications normalisées pour les actes de cybercriminalité.

Informations de cybersécurité basées sur la technologie

Les actes de cybercriminalité sont peut-être uniques parmi les délits en général, car il existe des mesures de prévention répandues basées sur la technologie – y compris des anti-virus, des produits de sécurité des réseaux et des pare-feu.[55] Le rôle de ces produits est généralement basé sur l´analyse, l´identification et le filtrage de certaines signatures électroniques. Ceci peut être basé sur le contenu ou sur le trafic, comme les communications allant ou venant d´adresses IP sur listes noires.[56] Plusieurs produits incluent aussi une détection heuristique qui examine le comportement de connexions et de fichiers suspects dans des conditions prédéterminées. Les journaux d´activités créés par les produits de sécurité basés sur la technologie capturent alors un sous ensemble de données informatiques du contenu et du trafic qui peuvent – dans certaines circonstances – correspondre à des éléments d´un acte de cybercriminalité. La tentative de commettre ou commettre des actes d´accès illégal à un système informatique, ou d´interférence illégale avec des données ou des systèmes informatiques, peuvent être détectés par ces produits qui génèrent une riposte. Une analogie serait le système d´alarme d´une maison qui détecte des incidents ayant lieu aux fenêtres et aux portes de la maison. Le fait qu´une alarme se déclenche ne signifie pas nécessairement qu´un délit a été commis. Un certain nombre de délits peuvent toutefois déclencher l´alarme. L´avantage des produits de cybersécurité basés sur la technologie est que de très nombreuses alarmes peuvent signaler des évènements enregistrés à un site central – et cela permet la production de statistiques agrégées de cybersécurité. De nombreux fournisseurs de cybersécurité du secteur privé élaborent des rapports basés sur ces statistiques.[57]

48 Voir http ://www.cybercellindia.com/#
49 Voir http ://fiscalia.chihuahua.gob.mx/intro/?page_id=3029
50 Voir https ://www.meldpuntcybercrime.nl/english_information.html ;http ://www.cybercrime.admin.ch/content/kobik/en/home/meldeformular.html ; ethttp ://www.actionfraud.police.uk/home
51 Voir http ://www.ic3.gov/default.aspx
52 Voir http ://cybercrime.interieur.gouv.ci/?q=node/4
53 Les rapports annuels du centre de signalement IC3 des ÉtatsUnis ont beaucoup augmenté entre les années 2000 à 2009 et se sont stabilisés en 2010 et 2011. Voir le centre de plaintes pour les délits sur internet. 2011. *Rapport des délits surinternet 2011.* Par contre, le nombre de rapports reçus par le centre de signalement suisse a diminué de 2007 à 2011. Voir le Service de Coordination de la Lutte Contre la Criminalité sur internet (SCOCI) 2011. *Rapport Annuel 2011.* La sensibilisation en matière de mécanismes de signalement peut augmenter ou diminuer avec le temps en fonction de facteurs tels que l´ampleur et la constance de la publicité qui accompagne ces mécanismes.
54 *Ibid.*
55 Voir OCDE. 2002. *Recommandations du Conseil concernant les lignes directrices pour la sécurité des réseaux et des systèmes d´information vers une culture de la sécurité* 25 juillet 2002 - C(2002)131/FINAL.
56 Callanan, C., Gercke, M., De Marco, E., et Dries-Ziekenheiner, H. 2009. *Etude sur le blocage d´internet, équilibrer les ripostes à la cybercriminalité dans les sociétés démocratiques.* Aconite internet Solutions, octobre 2009.

57 Voir, par exemple, AVG. 2011. *Rapport sur les menaces alimentées par la communauté 2012* ; Cisco 2011. *Rapport sur les menaces Cisco2011* ; IBM.2011. *IBM Rapport sur les menaces et les risques 2011* ; McAfee 2012. *McAfee Rapport sur les menaces. Premier trimestre 2012* ; Microsoft. 2011. *Rapport de renseignements de sécurité Microsoft. Volume 12* ; PandaLabs. 2012. *Rapport trimestriel PandaLabs. Avril-juin 2012* ; Sophos. 2012. *Rapport sur les menaces de sécurité 2012* ; Symantec. 2011. *Internet*

Les fournisseurs utilisent toutefois des définitions ; des méthodes de dénombrement ; des séries temporelles, des couvertures géographiques et des présentations de données sensiblement différentes.[58] Par conséquent, la comparaison des statistiques provenant des « rapports sur les menaces » produits par le secteur privé est extrêmement difficile. Dans certains cas ces données sont présentées comme des statistiques sur la cybercriminalité.[59] Il peut donc être plus approprié de voir ces informations de cybersécurité basées sur la technologie comme des indicateurs du phénomène de la cybersécurité qui peuvent, ou non, constituer des actes de cybercriminalité.

Les informations sur les menaces électroniques provenant des produits de cybersécurité peuvent cependant être utilisées avec précaution, pour faciliter la compréhension des patrons de la première catégorie de cybercriminalité : les actes contre la confidentialité, l´intégrité et la disponibilité des données ou des systèmes informatiques. Ces informations peuvent avoir un niveau élevé de comparabilité internationale, car ces produits– qui utilisent le même système de collecte et de traitement de données– sont probablement installés sur de multiples systèmes informatiques dans divers pays. Cette étude utilise des informations de cybersécurité basées sur la technologie pour caractériser un outil particulier, le botnet, qui est souvent utilisé dans des actes de cybercriminalité.

La majorité des pays ont signalé que les statistiques de la police n´étaient pas adéquates pour enregistrer les actes de cybercriminalité. Alors qu´une légère majorité des pays européens ont déclaré que les statistiques de la police étaient suffisantes pour enregistrer les actes de cybercriminalité, la grande majorité des pays de toutes les autres régions ont déclaré que les statistiques de la police étaient insuffisantes pour enregistrer ces cas

---

Rapport sur les menaces de sécurité. 2011 menaces, Volume 17 ; Défense totale. 2011. *Rapport sur les menaces : fin de l´année 2011*et Trend Micro. 2011. *TrendLabs résumé de sécurité annuel.*

58 *Ibid.* Voir aussi PricewaterhouseCoopers. 2012. *L´œil du cyclone. Principaux résultats de l´enquête sur l´état mondial de la sécurité de l´information 2012 ; Forum économique mondial.* 2012. Risques internationaux 2012, 7ème ed.

59 Voir entre autre, Symantec. 2011. *Rapport sur les menaces de sécurité sur internet. 2011 Tendances, Volume 17.*

ANNEXE TROIS : DISPOSITIONS DES INSTRUMENTS RÉGIONAUX ET INTERNATIONAUX

Définitions	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre 2005/222/JHA)	Union européenne[9] (proposition de directive 2010/0273)	Union européenne[10] (décision cadre 2001/413/JHA)	Union européenne[11] (directive 2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifs types)	Ligue des états arabes[13] (convention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Système informatique/d'information	Art. III-	Arts. 1(b) 1(e) 1(n)	Art. 3		Art. 1(a)		Art. 1	Art. 1(a)	Art. 2(a)			Arts. 3(5) 2(6)* 2(17)*	Arts. 2(1) 2(5)	Art. 1		
Réseau informatique/d'information		Art. 1(s)											Art. 2(6)	Art 1		
Dispositif/support de stockage			Art. 3									Arts. 3(7) 3(9)				
Infrastructure essentielle		Art. 1(g)										Art. 3(8)			Annx 1	
Donnée/Information informatique (y compris programme informatique)	Art. III-	Arts. 1 (c 1 (1(j)	Art. 3	Art. 1(b)	Art. 1(b)		Art. 1	Art. 1(b)	Art. 1(b)			Arts. 3(6) 2(9)*	Art. 2(3) 2(4)	Art. 1		
Enregistrement électronique		Art. 1(j)	Art, 2*									Art. 2(15)*				
Information ou donnée de l´abonné/trafic/contenu		Arts. 1(f) 1(v)	Art. 3		Arts. 1(d) 18		3(18)					Arts. 2(7)* 2(27)* 2(28)*	Art. 2(9)			
Communication électronique/courriel	Art. III	Art. 1(m)					Art. 1					Art. 2(14)*				
Logiciel malveillant		Art. 1(r)		Art. 1(c)												
Fournisseur de services (internet)		Art.1 1(t)	Art. 3		Art.1 (c)							Arts. 3(1) 3(2) 3(11) 3(17)	Art. 2(2)			
Enfant/Mineur	Art. III		Art. 10(3)		Art. 9(3)	Art. 3	Art. 1				Art. 2(a)	Art. 3(3)				Art. 2(c)

Définitions	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre 2005/222/JHA)	Union européenne[9] (proposition de directive 2010/0273)	Union européenne[10] (décision cadre 2001/413/JHA)	Union européenne[11] (directive2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifs types)	Ligue des états arabes[13] (convention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Cybercriminalité/ Délit informatique				Art.1 (a)											Annx 1	

Incrimination	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre 2005/222/JHA)	Union européenne[9] (proposition de directive 2010/0273)	Union européenne[10] (décision cadre 2001/413/JHA)	Union européenne[11] (directive2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifs types)	Ligue des états arabes[13] (convention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Accès illégal à un système informatique	Arts. III(15) III(16)	Arts. 18 19	Arts. 5 7		Art. 2		Arts. 2 3	Art. 2(1)	Art. 3			Arts. 4 5	Art. 6	Arts. 3,5 15 22		
Accès illégal, interception ou acquisition de données informatiques	Art. III(23)	Arts. 19 21	Arts. 5 8	Art. 3(1) (a)	Arts. 2 3		Art. 6		Art. 6			Arts. 6 8	Arts. 6 7 18	Arts. 3 8		
Interférence avec des données informatiques	Arts. III(19) III(20	Arts. 20 22(a)	Art. 6	Art. 3(1) (c)	Art. 4		Arts. 5 7	Art. 4	Art. 5	Art. 3		Art. 7	Art. 8	Art. 6		
Interférence illégale avec un système informatique	Arts. III(18) III(19)	Art.	Art. 7 3(1)22(a)	Art. (c)	Art. 5		Art. 4	Art. 3	Art. 4	Art. 3		Art. 9	Art. 6	Art. 7		
Outils informatiques malveillants	Art. III(22)	Art. 2 2 (b 2 2 (c	Art. 9	Art. 3(1) (b)	Art. 6		Art. 12	Art. 5	Art. 7	Art. 4		Art. 10	Art. 9			
Violation des mesures de protection des données ou de la vie privée	Arts. III(27) III(54)			Art. 3			Art. 11				Art . 15(a) (1) 1					
Falsification liée à l´informatique	Arts. (24.	Art. 23			Art. 7		Art. 8			Arts. 4		Art. 11	Arts. 18	Art. 4		

1Directive 2002/58/EC (n´est pas une exigence stricte

Incrimination	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre 2005/222/JHA)	Union européenne[9] (proposition de Directive 2010/0273)	Union européenne[10] (décision cadre 2001/413/JHA)	union européenne[11] (directive 2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifs types)	Ligue des états arabes[13] (convention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Fraude liée à l´informatique	Arts. III(25) III(26) III(41)	2 4 (a 2 4 (b			Art. 8		Arts. 9 10 23			A 2 ' 4		Art. 12	Art. 11	Arts. 10 11 12		
Infractions relatives aux outils de paiement électronique										Art. 2			Art. 18	Art. 11		
Délit lié à l´identité												Art. 14				
Infractions relatives aux droits d´auteurs et aux marques déposées				Art. 3(1) (d)	Art. 10								Art. 17	Art. 14		
Messages non sollicités		Art. 19(g)									Art. 13(3)2	Art. 15				
Harcèlement, extorsion, ou actes causant un préjudice personnel liés à l´informatique	Arts. III(40) III(41)	Art. 25										Art. 18		Art. 9		
Actes de racisme ou de xénophobie liés à l´informatique	Art. III(34) III(35) III(36)				Art. 3,4,5 (OP)		Arts. 18,19 20									
Déni ou justification de génocides ou de crimes contre l´humanité liés à l´informatique	Art. III(37)				Art. 6 (OP)		Art. 21									
Production, distribution, ou possession de pornographie infantile liées à l´informatique	Arts. III(29) III(30) III(31) III(32)		Art. 10		Art. 9	Art. 20	Art. 14-17				Art. 5	Art. 13	Art. 12			Art. 3
Sollicitation ou prédation sexuelle des enfants liées à l´informatique						Art. 23					Art. 6					
Actes d´appui au terrorisme liés à l´informatique	Art. III(40)	Arts. 18 19 20 22(a)											Art. 15	Art. 21		

2 Directive 2002/58/EC (n´est pas une exigence stricte d´incrimination).

Incrimination	Infractions de blanchiment de capitaux liées à l´informatique	Infractions de trafic illicite liées à l´informatique	Infractions contre l´ordre, la moralité ou la sécurité publique liées à l´informatique	Infractions liées aux enquêtes des services répressifs	Circonstances aggravantes pour des délits classiques commis au moyen d´un système informatique	Tentative, aide ou conseil	Responsabilité des entreprises
Union africaine[1]				Art. III(54)	Art. III(40)		
COMESA[2]						Art.	Art. 27
Commonwealth[3]				Arts. 13 21			
Communauté des états indépendants[4]							
Conseil de l´Europe[5] (convention de Budapest et OPC)				Arts. 16(3) 20(3) 21(3)		Arts. 11 7(OP)	Art. 12
Conseil de l´Europe[6] (convention de Lanzarote)						Art. 24	Art. 26
CEDEAO[7]			Arts. 14 15 16 17		Art. 22		
Union européenne[8] (décision cadre 2005/222/JHA)							
Union européenne [9] (proposition de directive 2010/0273)						Art. 8	
Union européenne [10] (décision cadre 2001/413/JHA)							
Union européenne [11] (directive2011/92/EU)							
UIT/CARICOM/CTU[12] (textes législatifs types)				Arts. 16 17			
Ligue des états arabes[13] (convention)	Art. 15	Art. 16	Arts. 12 13 14 15	23(3) 28(3) 29(3)	Art. 21		
Ligue des états arabes [14] (loi type)	Art. 19	Arts. 17 18	Arts. 16 19 20				
Organisation de coopération de Shanghai [15]							
Nations Unies [16] (CRC OP)							

Pouvoirs procéduraux	Perquisition pour du matériel ou des données informatiques	Saisie de matériel ou de données informatiques
Union africaine[1]	Art. III(50)	Art. III(51)
COMESA[2]	Arts. 37 (a) 37 (b)	Art. 37 (c)
Commonwealth[3]	Art. 12	Arts. 12 14
Communauté des états indépendants[4]		
Conseil de l´Europe[5] (convention de Budapest et OPC)	Arts. 19(1) 19(2)	Art. 19(3)
Conseil de l´Europe[6] (convention de Lanzarote)		
CEDEAO[7]	Art. 33	Art. 33
Union européenne[8] (décision cadre 2005/222/JHA)		
Union européenne [9] (proposition de directive 2010/0273)		
Union européenne [10] (décision cadre 2001/413/JHA)		
Union européenne [11] (directive 2011/92/EU)		
UIT/CARICOM/CTU[12] (textes législatifs types)	Art. 20	Art. 20
Ligue des états arabes[13] (convention)	Art. 26	Art. 27(1)
Ligue des états arabes [14] (loi type)		
Organisation de coopération de Shanghai [15]		
Nations Unies [16] (CRC OP)		

Ordonnance pour les données informatiques stockées		Art 36(a).	Art. 15		Art. 18(1)							Art. 22 (a)	Art. 25(1)			
Ordonnance pour les informations de l´abonné		Art. 36(b)			Art. 18(1) (b)							Art. 22 (b)	Art. 25(2)			
Ordonnance pour les données stockées du trafic		Art. 34(a) (ii)	Art. 16		Art. 17(1) (b)							Art. 24	Art. 24			
Collecte des données de trafic en temps réel		Art. 38	Art. 19		Art. 20							Art. 25	Art. 28			
Collecte des données du contenu en temps réel	Art. III(55)	Art. 39	Art. 18		Art. 21							Art. 26	Art. 29			
Conservation rapide des données informatiques	Art. III(53)	Arts. 33 34(a) (i) 35	Art. 17		Arts. 16 17(1) (a)		Art. 33					Art. 23	Art. 23(2)			
Utilisation d´outils criminalistiques à distance						Art. 30(5)					Art. 15	Art. 27				
Accès transfrontalier aux données informatiques		Art. 49(b)			Art. 32(b)								Art. 40(2)			
Fourniture d´assistance		Art. 37(d)	Art. 13		Art. 19(4)							Art. 21	Art. 27(2)			
Conservation des données informatiques		Arts. 29 30 31								Arts. 3 6						

Preuves électroniques	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre 2005/222/JHA)	Union européenne[9] (proposition de directive 2010/0273)	Union européenne[10] (décision cadre2001/413/JHA)	Union européenne[11] (directive2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifs types)	Ligue des états arabes[13] (convention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Recevabilité des preuves/registres électroniques	Art. I(24)	Art. 5(a)	Arts. 20 3* 11*				Art. 34					Arts. 5* 7(1)* 12*				
Recevabilité de la signature électronique			Art. 12									Art. 14*				
Fardeau de prouver l´authenticité			Art. 5*									Art. 9*				
Règle de la meilleure preuve			Art. 6*									Art. 6*				

Imprimés comme preuves												Art. 8*				
Présomption d´intégrité			Art. 7*									Art. 7(2)*				
Preuves sur les normes enregistrement/ conservation			Art. 8*									Art. 10*				
Preuves/registres électroniques d´autres pays et documents étrangers												Art. 16* 17*				

Juridiction	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre 2005/222/JHA)	Union européenne[9] (proposition de directive 2010/0273)	Union européenne[10] (décision cadre 2001/413/JHA)	Union européenne[11] (directive2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifst ypes)	Ligue des états arabes[13] (onvention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Principe de territorialité		Art. 40 (a)(i)	Art. 4(a)		Art. 22 (1)(a)	Art. 25 (1)(a)		Art. 10 (1)(a)	Art. 13 (1)(a)	Art. 9 (1)(a)	Art. 17 (1)(a)	Art. 19(a)	Art. 30 (1)(a)			Art. 4(1)
Utilisation de système/données informatiques localisés sur le territoire		Art 40(a)(i)														
Dirigé contre des systèmes/données informatiques localisés sur le territoire		Art. 40 (a)(iii)						Art. 10 (2)(b)	Art. 13 (2)(b)							
Principe de nationalité (auteur de l´infraction)		Art. 40(c)	Arts. 4(c),(d)		Art. 22 (1)(d)	Art. 25(1) (d)		Art. 10 (1)(b)	Art. 13 (1)(b)	Art. 9 (1)(b)	Art. 17 (1)(b)	Art. 19(c)	Art. 30 (1)(d)			Art. 4 (2)(a)
Principe de nationalité (victime)						Art. 25(2)					Art. 17 (2)(a)					Art. 4 (2)(b)
Résidence habituelle						Arts.25(1) (e 25(2) 25(5)			Art. 13 (1)(b)		Arts. 17 (2)(c)					Art. 4 (2)(a)
Personne morale – principe de constitution								Art. 10 (1)(c)	Art. 13 (1)(c)	Art. 9 (1)(c)	Art. 17 (2)(b)					
Principe des intérêts de l´état													Art. 30 (1)(e)	Art.		
Juridiction quand l´extradition est refusée		Arts. 40(d)			Art. 22(3)	Art. 25(7)		Art. 10(3)		Art. 10(1)			Art. 30(2)			Art. 4(3)

Navire et aéronef		Art. 40(b)	Art. 4(b)		Arts. 22 (1)(b) (c)	Arts. 25 (1)(b) (c)						Art. 19(b)	Arts. 30 (1)(b) (c)			Art. 4(1)
Double incrimination			Art. 4(d)		Art. 22 (1)(d)					Art. 9 (1)(b)	Art. 17(4)	Art. 19	Art. 30 (1)(d)			
Juridiction concurrente		Art. 4 0 (e)			Art. 22(5)	Art. 25(8)		Art. 10(4)					Art. 30(3)			
Etablissement du lieu de l´infraction		Art. 4 0 (f)									Art. 17(3)					

Coopération internationale	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre 2005/222/JHA)	Union européenne[9] (proposition de directive 2010/0273)	Union européenne[10] (décision cadre 2001/413/JHA)	Union européenne[11] (directive2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifs types)	Ligue des états arabes[13] (convention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Principe général de coopération internationale	Art. III(14)	Art. 41		Art. 5	Art. 23	Art. 38(1)									Art. 3-5	Art. 10
Extradition pour infractions liées aux instruments		Art. 42(c)			Art. 24	Art. 38(3)				Art. 10			Art. 31			Art. 5
Entraide judiciaire		**Arts. 43(a) 45**		**Art.**	**Arts. 25 27**	**Art. 38(3)**	**Art. 35**			**Art. 11**			**Arts. 32 34**			**Art. 6**
Mécanisme pour une assistance rapide		Art. 43(b)		Arts. 6(2) 7(1)	Art. 25(3)								Art. 32(3)			
Assistance – conservation des données		Art. 46			Art. 29								Art. 37			
Assistance – saisie/accès à /collecte de/divulgation de données informatiques		Arts. 47 48 51			Arts. 30 31 34								Arts. 38 39 41[42]			
Accès transfrontalier aux données informatiques		Art. 49(b)			Art. 32(b)								Art. 40(2)			
Transmission d´informations non sollicitées/échange d´informations		Art. 44			Art. 26			Art. 11	Art. 14	Art. 12			Art. 33			
Confidentialité de la demande		Art. 45(e)		Art. 9	Art. 28								Art. 36		Art. 6	

Double incrimination		Arts, 42(a), 43(d)			Arts. 24(1), 25(5)								Arts. 32(5) 37(3) 37(4)			
Etablissement de point de contact ou de réseau 24/7		Art. 52			Art. 35			Art. 11	Art. 14				Art. 43			

Responsabilités du fournisseur de services	Union africaine[1]	COMESA[2]	Commonwealth[3]	Communauté des états indépendants[4]	Conseil de l´Europe[5] (convention de Budapest et OPC)	Conseil de l´Europe[6] (convention de Lanzarote)	CEDEAO[7]	Union européenne[8] (décision cadre2005/222/JHA)	Union européenne[9] (proposition de directive 2010/0273)	Union européenne[10] (décision cadre 2001/413/JHA)	Union européenne[11] (directive2011/92/EU)	UIT/CARICOM/CTU[12] (textes législatifs types)	Ligue des états arabes[13] (convention)	Ligue des états arabes[14] (loi type)	Organisation de coopération de Shanghai[15]	Nations Unies[16] (CRC OP)
Obligations de surveillance		Art. 17								Art. 15		Art. 28				
Fourniture volontaire d´informations		Art. 17(b)														
Notifications de suppression		Art. 16														
Responsabilité de l´accès des fournisseurs providers		Art. 12								Art. 12		Art. 29				
Responsabilité de stockage des fournisseurs		Art. 13								Art. 13		Art. 31				
Responsabilité d´hébergement des fournisseurs		Art. 14								Art. 14		Art. 30				
Responsabilité relative aux hyperliens des fournisseurs/ moteurs de recherche		Art. 15										Art 32, 33				

1 Union africaine, 2012. Projet de Convention sur l´établissement d´un cadre juridique pour la cybersécurité en Afrique.
2 Marché commun de l´Afrique orientale et australe (COMESA), 2011. Projet de loi type sur la Cybersécurité
3 Le Commonwealth, 2002. (i) projet de loi sur les délits liés aux ordinateurs et à l´informatique (ii) loi type sur les preuves électroniques (indiquée par*).
4 Communauté des états indépendants, 2001.Accord de coopération en matière de lutte contre les infractions liées à l´information informatique.
5 Conseil de l´Europe, 2001. Convention sur la cybercriminalité et le protocole additionnel à la Convention sur la cybercriminalité, relatif à l´incrimination des actes racistes et xénophobes commis par le biais de systèmes informatiques.
6 Conseil de l´Europe, 2007. Convention sur la protection des enfants contre l´exploitation sexuelle et les abus sexuels.
7 Communauté économique des états de l´Afrique de l´ouest(CEDEAO), 2009. Projet de directive sur la lutte contre la cybercriminalité au sein de la CEDEAO.
8 Union européenne, 2005. Décision cadre du Conseil 2005/222/JHA sur les attaques contre les systèmes d´information.
9 Union européenne, 2010. Proposition finale COM(2010) pour une directive du Parlement européen et du Conseil sur les attaques contre les systèmes d´information et qui abroge la Décision cadre du Conseil 2005/222/JHA.
10 Union européenne, 2001. Décision cadre du Conseil 2001/413/JHA sur la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces.

11 Union européenne, 2011. Directive 2011/92/EU du Parlement européen et du Conseil pour lutter contre l´exploitation sexuelle et les abus sexuels des enfants et la pédopornographie, qui remplace la Décision cadre du Conseil 2004/68/JHA.

12 L´Union internationale des télécommunications (UIT)/la communauté des Caraïbes (CARICOM)/l´Union caraïbe des télécommunications(CTU), 2010. (i) textes législatifs types sur la cybercriminalité /les cyberdélits et (ii) les preuves électroniques (indiqué par *).

13 Ligue des états arabes, 2010. Convention arabe sur la lutte contre les infractions relatives à la technologie de l´information.

14 Ligue des états arabes, 2004. Loi arabe type sur la lutte contre les infractions relatives aux systèmes de technologie de l´information.

15 Organisation de coopération de Shanghai, 2010. Accord de coopération dans le domaine de la sécurité internationale de l´information.

16 Nations Unies, 2000. Protocole facultatif à la Convention concernant la vente d´enfants, la prostitution des enfants et la pornographie infantile.

17 Union européenne, 2002. Directive 2002/58/EC du Parlement européen et du Conseil relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

18 Union européenne, 2006. Directive 2006/24/EC du Parlement européen et du Conseil sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

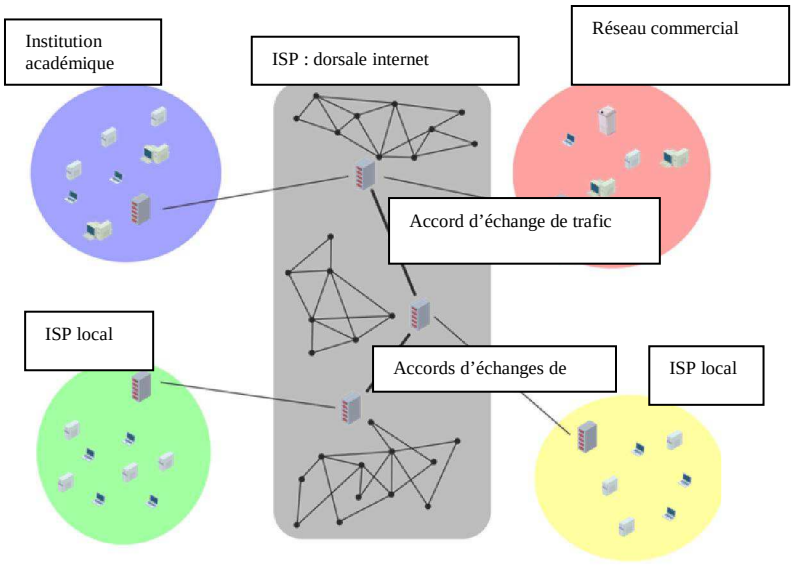
19 Union européenne, 2000. Directive 2000/31/EC du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l´information, notamment du commerce électronique dans le marché intérieur.

Page intentionnellement laissée vierge

ANNEXE QUATRE : L´INTERNET

L´internet est une combinaison de réseaux qui communiquent entre eux – le mot « internet » est simplement une abréviation du mot « inter-networking ». Ces réseaux sont formés par des ordinateurs individuels allant des ordinateurs personnels domestiques aux super-ordinateurs, qui communiquent entre eux grâce à une infrastructure mondiale sans fil et de câbles physiques.

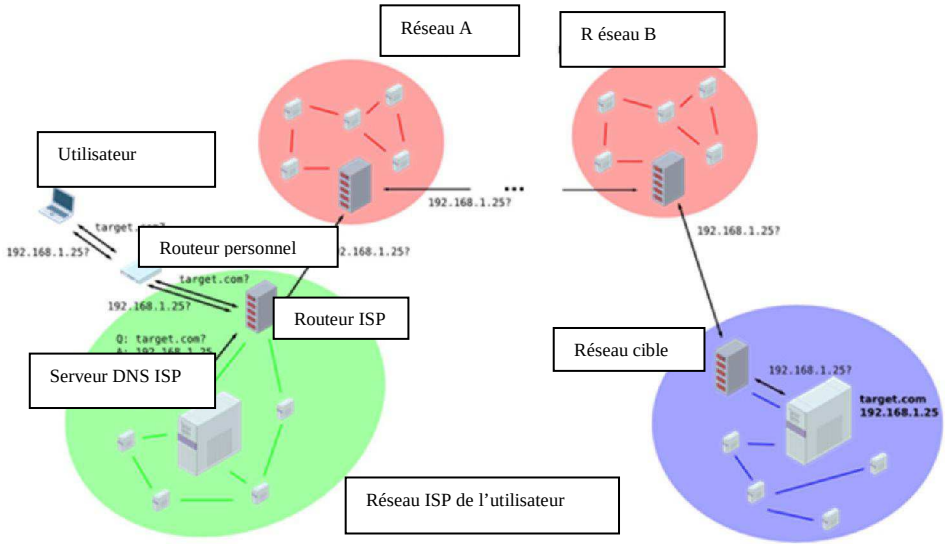
Les routeurs gèrent le transfert des données qui circulent sur ces réseaux. Ce peut être de petits dispositifs de faible puissance ou de puissantes machines qui gèrent des milliers de connexions individuelles et de grandes quantités de trafic. Les routeurs réunissent les réseaux des ordinateurs individuels pour constituer l´internet, en transférant des informations et en fournissant les adresses numériques qui permettront aux ordinateurs de se connecter les uns aux autres partout dans le monde.



Comment fonctionne l´internet ?

Il y a plusieurs types de trafic internet. Le plus commun est lié au *World Wide Web,* qui fut d´abord développé par l´Organisation européenne pour la recherche nucléaire (CERN) à la fin des années 98. Le web a d´abord été conçu comme un système de documents contenant des liens vers d´autres documents – un concept connu comme les « hypertextes » qui a été proposé dès les années 1930.[1]
En cliquant sur un lien dans un navigateur web, une série d »opérations sont lancées et entraînent l´affichage d´une nouvelle page web dans un ordinateur. Ce processus est illustré par la figure ci-dessous. La première étape consiste à traduire le nom lisible par l´humain d´un service, comme www.target.com, à l´adresse numérique de protocole internet (IP) que les ordinateurs peuvent utiliser pour localiser d´autres ordinateurs sur internet. Ceci est réalisé en utilisant un serveur du système de noms de domaine (DNS), généralement opéré par le fournisseur de services de l´usager, dont la localisation est généralement fournie à l´ordinateur de l´usager lorsqu´ils se connectent pour la première fois. Plusieurs alternatives de serveurs DNS sont disponibles – des exemples bien connus sont opérés par OpenDNS, ainsi que par Google.[2]
Lorsque l´adresse IP de l´ordinateur distant est connue, des informations peuvent lui être envoyées. Ceci peut prendre la forme de demandes de données, comme une page web, qui est ensuite renvoyée par le navigateur web de l´utilisateur. À cet effet, l´information est décomposée en séquences de paquets – de petites quantités de données qui circulent indépendamment sur internet avant d´être rassemblées sur l´ordinateur distant. Chaque paquet contient l´adresse IP de l´ordinateur distant, l´information relative au type de données incluses dans le paquet et les données elles-mêmes.

1 Ziewitz, M. et Brown, I. 2013. La préhistoire de la gouvernance d´internet *.dans* Brown, I. *guide de recherche sur la gestion d´internet.* Cheltenham : Edward Elgar.
2 Voir http ://www.opendns.com ethttps ://developers.google.com/speed/public-dns/



Les paquets n´incluent généralement pas d´informations sur la route de leur destination. En revanche, comme dans le cas d´un système postal, seule la destination est donnée. Les routeurs que les paquets rencontrent décident quelle sera la manière la plus efficace d´atteindre la destination. Ainsi, l'internet peut répondre rapidement et de manière flexible lorsqu´une partie du réseau est endommagée ou surchargée en choisissant des routes alternatives pour les données.

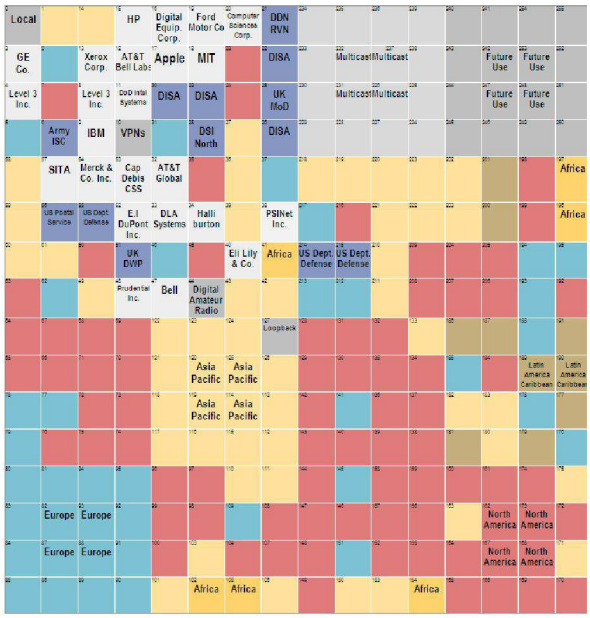
Mécanismes de connectivité

L´internet se base sur une série de normes techniques pour transmettre et acheminer les données. Le *Protocole internet* (IP) établit la manière dont les données sont décomposées en blocs pour la transmission et la manière dont les adresses de la source et la destination sont spécifiées. La Version 4 est la plus couramment utilisée (IPv4), bien qu´il y ait une tendance en faveur du plus récent IPv6. Afin de créer des services comme le web, des protocoles supplémentaires se superposent au cœur du protocole internet. L´exemple le plus commun est le protocole de contrôle de transmission TCP, qui fournit un mécanisme de transport fiable et évite l´envoi de trop de données en même temps. Un autre protocole, le protocole de datagramme utilisateur UDP, ne fournit pas de garanties de livraison, mais permet une transmission hautement efficace et flexible pour les communications en temps réel, de voix, par exemple.

Chaque ordinateur sur internet est associé à une adresse unique, écrite sous la forme de quatre nombres comme 192.168.1.1. Les routeurs utilisent ces adresses *IP* pour acheminer chaque paquet vers sa destination. Le TCP et l´UDP ajoutent des numéros de ports qui spécifient le service vers lequel le paquet est dirigé :

Service	**Transport**	**Numéro de port**
SMTP (courriel)	TCP	25
Web (HTTP)	TCP	80
Web sécurisé (HTTPS)	TCP	443
DNS	UDP	53
SSH (canal sécurisé à distance)	TCP	22

L´attribution de trois séries d´identifiants uniques pour internet – les noms de domaines, les adresses IP et les numéros du système autonome (SA), les numéros de ports et de paramètres des protocoles – est supervisée par une association d´intérêt général à but non lucratif des États-Unis d´Amérique : ICANN, *la société pour l´attribution des noms de domaines et des numéros sur l´Internet.*[3] L´ICANN coordonne également l´opération et l´évolution du système de serveur de noms racine DNS, ainsi que le développement de la politique concernant ces fonctions techniques.[4] Les fonctions d´attribution et d´enregistrement des ressources d´internet correspondent à cinq *registres régionaux internet* qui attribuent des blocs d´adresses IP à des organisations telles que les fournisseurs de services internet et les institutions académiques.



Il existe un nombre limité d´adresses IPv4 disponibles. Les adresses IPv4 sont des nombres de 32 bits – des nombres pouvant être exprimés sous forme binaire en utilisant 32 chiffres – et qui permettent 2^{32}, soit environ 4,3 milliards d´adresses. Étant donné qu´internet a connu une croissance au-delà de toute attente, ces nombres se sont rapidement terminés, sans que de nouveaux dispositifs puisent être ajoutés. Pour y remédier, un effort majeur est actuellement en cours pour mettre en place sur internet une nouvelle version du protocole internet, IP version 6 (IPv6). L´IPv6 accroît le nombre disponible d´adresses en utilisant des nombres de 128 bits, et en créant 2^{128} adresses – écrit en notation décimale, ce nombre comprend 39 chiffres. Il est à espérer que cela sera suffisant pour l´avenir proche. La figure précédente montre le total actuel disponible et les adresses IPv4 attribuées.[5] De grands blocs d´adresses IPv4 disponibles sont attribuésà des registres nationaux. Pour des raisons historiques, certains blocs de niveau supérieur comme 18.x.x.x sont aussi attribués à des individus du secteur privé et des organisations académiques ou gouvernementales.

Le système de noms de domaines (DNS)

Afin qu´elles soient plus accessibles aux utilisateurs humains, les adresses sur internet sont aussi écrites comme des *noms de domaines* en utilisant le système des noms de domaines. Outre l´attribution des adresses IP, l´ICANN administre le DNS par délégation d´autorité des registres des noms de domaines. Ces registres sont des bases de données de tous les noms de domaines enregistrés dans *les domaines génériques de premier niveau* (gTLD), tels que .com, .net, .int, .mil, .gov et les *domaines nationaux de premier niveau* (ccTLD) tels que .de (Allemagne) et .cn (Chine). Les registres sont chargés de maintenir les renseignements précis relatifs à la localisation de chaque domaine.

3 Les Articles sur la constitution de la Société pour l´attribution des noms de domaines et des numéros sur internet sont disponibles sur http ://www.icann.org/en/about/governance/articles

4 La Société pour l´attribution des noms de domaines et des numéros sur internet. 2012. *Règlements de la Société pour l´attribution des noms de domaines et des numéros sur internet.*

5 L´autorité chargée de l´attribution des numéros sur internet. 2012. *IANA registre des adresses IPv4.*

Lorsqu´un nouveau domaine est enregistré, il est géré par un des nombreux *registrars*. Cette entreprise vérifie que le nouveau domaine n´existe pas déjà, puis informe le registre central qu´un nouveau domaine a été requis et transmet la localisation des renseignements précis relatifs au domaine. Ces informations sont ensuite retransmises, au cours de 24 heures, aux principaux serveurs DNS du monde.

Dans chaque domaine de premier niveau se trouvent les noms d´organisations bien connues qui ont enregistré le nom. L´entreprise Google, par exemple, a enregistré le nom « google » dans le domaine de premier niveau .com, pour produire le domaine google.com. Des noms individuels peuvent être attribués aux ordinateurs dans leur domaine. Le nom « www » est un nom standard pour les ordinateurs qui exécutent un serveur web et cela figure généralement au début des adresses web comme www.google.com.[6] De même, les points mail.google.com offrent les services GMail de Google. Certains TLD se divisent en sous catégories comme, par exemple, .co pour les entreprises ou .ac pour les universités au Royaume Uni. Ceci signifie que la présence en ligne de Google au Royaume Un est enregistré sur www.google.co.uk.

Le nouveau programme gTLDde ICANN permettra la création de nouveaux domaines de premier niveau, en permettant des noms tels que .baby ou .book soient enregistrés. La complexité et les coûts d´enregistrement des nouveaux gTLDs sont élevés, mais le programme augmentera significativement le nombre d´alternatives possibles pour les noms de domaines.

Services communs

Une des applications les plus communes d´internet à ses débuts était les messages électroniques, ou courriels, qui restent l´un des principaux services – une adresse de courrier électronique est devenue aussi importante qu´un numéro de téléphone ou une adresse physique pur de nombreuses transactions modernes.

Outre les courriels, la force motrice de l´internet a été le web, qui a coïncidé avec l´essor du nombre d´usagers en ligne dans les années 90. Depuis lors, les outils dits « Web 2.0 » ont permis la croissance des contenus générés par les utilisateurs. Ces sites permettent aux utilisateurs de partager leurs vies et leurs intérêts avec des amis, de télécharger des photos et des vidéos, de créer des journaux ou des *blogs* et d´héberger d´autres activités. Un troisième service amplement utilisé est le système vocal sur *IP*, ou VoIP. Ceci permet de faire facilement et à bas prix des appels téléphoniques, des vidéos et des conférences en ligne. Une autre technologie essentielle est le réseautage pair à pair (P2P) qui connecte directement les ordinateurs des usagers les uns aux autres, afin de partager des fichiers ou des données. Le réseautage P2P networking contraste avec les services traditionnels où toutes les connexions passent par un serveur central. Les réseaux les plus communs P2P étaient à l´origine Napster et Gnutella qui permettaient de partager des fichiers de musique. Plus récemment un système appelé BitTorrent a permis le partage extrêmement rapide et efficace de fichiers volumineux, comme les applications de logiciels et les vidéos. BitTorrent fonctionne en faisant en sorte que tous les utilisateurs téléchargent des blocs de données. Pour distribuer un fichier volumineux comme une vidéo, BitTorrent divise le fichier en petits blocs. Lorsque les usagers téléchargent ces blocs, cela rend les blocs déjà téléchargés disponibles pour d´autres usagers.

Connectivité limitée

Plusieurs régions d´Afrique du sud et de l´est ont d´abord été connectée à des services internet à haut débit, avec la pose de câbles sous-marins en 2009. En 2012, le continent africain ne représentait que 6 pour cent de la connectivité internet mondiale.

Les connexions internet basées sur les téléphones mobiles ont dépassé les connexions internet basées sur les lignes téléphoniques fixes depuis 2008. Dans de nombreuses régions d´Afrique, malgré les améliorations de l´infrastructure disponible, les téléphones portables restent de loin le moyen le plus commun d´accéder à des services internet. Ceci a donné lieu à l´émergence d´une série de services visant les utilisateurs de téléphones portables et de monnaie électronique basée sur les crédits des téléphones portables, pour rechercher des résultats transmis par des messages de textes de texte SMS.

6 En réalité, Google gère leur site web sur plusieurs ordinateurs différents. « www » est en réalité un *alias* qui s´applique aux ordinateurs requis.

Par conséquent, si davantage d´usagers téléchargent un fichier et partagent des parties du fichier, cela augmente la vitesse du téléchargement pour d´autres usagers. Le succès de cette approche est démontrée par le fait que BitTorrent représentait entre 10 et 15 % du total cumulatif du trafic internet fixe en Europe et en Amérique du nord au second semestre de 2012.[7]

Gouvernance

Depuis ses débuts, de nombreuses institutions ont eu une influence sur le développement et le fonctionnement d´internet. Il s´agit d´organismes gouvernementaux traditionnels, d´entreprises et de groupes de bénévoles.[8]

Le principal organisme de normalisation est le *groupe d´étude sur l´ingénierie internet* (IETF). Intégré par des volontaires du monde entier, l´IETF développe et adopte de nouvelles normes pour les technologies internet et pour la coordination avec d´autres organismes de normalisation. Les productions les plus connue de l´IETF sont les *demandes d´observations* ou RFC. Elles décrivent ouvertement de nouveaux protocoles, de façon à ce que quiconque puisse construire des technologies compatibles.

La société pour l´attribution des noms de domaines et des numéros sur l´internet (ICANN) gère les adresses IP et les noms de domaines. L´ICANN est une société privée à but non lucratif enregistrée en Amérique du nord. La structure organisationnelle de l´ICANN inclut les réunions tri-annuelles du Comité consultatif gouvernemental (GAC) qui fournissent un forum pour recevoir des avis et pour la représentation des gouvernements nationaux.

L´*Union internationale des télécommunications* (UIT) établit les normes pour les communications télégraphiques et téléphoniques, et pour le spectre radioélectrique. Le règlement des télécommunications internationales (RTI) complète la Convention internationale des télécommunications, pour établir les principes généraux relatifs à la fourniture et l´opération de divers aspects des communications mondiales, y compris les flux de trafic et la qualité des services. Les RTI ont été élaborés avant qu´internet ne devienne une plateforme dominante pour les communications internationales et ne font donc aucune référence spécifique à internet.

Routage internet

Lorsque les ordinateurs envoient des informations sur internet, celles-ci circulent sur de nombreux réseaux avant d´atteindre leur destination. Pour déterminer la meilleure route, les réseaux networks annoncent leur capacité de gérer certaines routes en utilisant un protocole appelé BGP – le protocole d´échange de route.

Le BGP est l´un des principaux protocoles d´internet, mais il existe quelques caractéristiques spécifiques de sécurité dans le protocole et les erreurs de configuration peuvent avoir des conséquences significatives. Par exemple au début de l´année 2010, un petit fournisseur de services d´Asie de l´est commença annonça 35000 routes entre les réseaux au lieu des 40 habituelles. La conséquence fut qu´on signala que 10 pour cent des réseaux du monde entier avaient été acheminés de manière erronée pendant environ vingt minutes.

Histoire

Les origines d´internet remontent à un projet de recherche mené par l´Agence des projets de recherches avancées (ARPA, puis DARPA) du Département de la Défense des ÉtatsUnis en 1969, qui visait à permettre l´accès à distance aux rares ressources informatiques de l´époque hébergées par des entreprises et des institutions académiques. Le réseau qui surgit de ce projet, appelé ARPANET, différait totalement des premiers réseaux de télécommunications qui employaient le nouveau

7 Sandvine. 2012. *Rapport sur le phénomène mondial internet 2H 2012.*

8 Ziewitz, M. et Brown, I. 2013. La préhistoire de la gouvernance d´ internet. *dans* Brown, I. *guide de recherche sur la gestion d´internet.*. Cheltenham : Edward Elgar.

concept de commutation de paquets plutôt que la traditionnelle approche de commutation de circuits, et cela permettait que les communications peu fiables de cette époque soient beaucoup plus efficaces et solides.

La croissance d´ARPANET fut rapide, comme plusieurs autres réseaux similaires des États-Unis d´Amérique et d´Europe. Etant donné que le nombre de réseaux augmentait, Vinton Cerf et d´autres personnes financèrent la recherche d´ARPA pour faire en sorte que les réseaux communiquent entre eux. Le résultat de ce travail fut la première spécification du *protocole de contrôle de transmission internet* en 1973, qui fournit un moyen de réunir différents réseaux et qui incluait la première utilisation du terme « internet ». Les techniques développées pour ce travail restent au cœur de l´internet actuel.

En 1989, Tim Berners-Lee, qui travaillait au CERN, a développé le world-wide web (la toile), qui permettait que des documents, ou des *pages*, fassent un lien avec d´autres documents stockés dans le réseau. Le logiciel de Berners-Lee »s fut accessible gratuitement et devint extrêmement populaire au début des années 1990. En 1994, les restrictions sur les activités commerciales sur internet furent assouplies. Ceci, ainsi que la popularité croissante du web, causa l´explosion de l´utilisation personnelle et commerciale d´internet durant les années 90. Les fournisseurs commerciaux de services connectaient les utilisateurs à internet et à une série d´outils et de services d´information qui ne cessaient d´augmenter. Les premières très grandes entreprises d´internet surgirent au milieu des années 90, avec principalement les premiers moteurs de recherche, qui aidaient à trouver un sens à la multitude d´informations disponibles. Yahoo!, fondé en 1994, fut un des premiers chefs de file, suivi de Google en 1998. Depuis lors, les sites web simples et statiques ont fait place à des sites interactifs qui permettent aux usagers de créer et de partager des contenus, et cela donna lieu à l´essor des réseaux sociaux. La vitesse de connexion a explosé et cela a permis que des vidéos et de la musique soient diffusées sur des ordinateurs personnels.

Annonces ciblées

Le modèle commercial prédominant sur le web est la publicité. Des sites web populaires comme Google, Facebook et Yahoo! vendent des espaces publicitaires aux entreprises, distribuent des annonces à des millions d´usagers qui vont sur ces sites tous les jours.
Des services comme Facebook et Google sont disponibles gratuitement pour les usagers. De plus en plus, ces sites suivent les activités des usagers et les analysent, ou explorent les données pour construire des profils qui seront ensuite utilisés pour présenter des annonces ciblées qui visent les intérêts d´usagers spécifiques.
Le succès de ce modèle de services gratuits alimentés par des publicités ciblées a permis que Google ait des revenus de 50 milliards de $ annuels et que la valeur de Facebook ait été estimée à 104 milliards de $ lorsqu´il s´est introduit en bourse vers la mi-2012.

Informatique en nuage

Avec le développement d´internet, ont émergé de nouvelles approches informatiques. La plus importante est peut-être l´informatique en nuage. Au lieu de stocker les informations sur les ordinateurs personnels ou du bureau, ou d´acheter et d´actualiser des logiciels, le nuage permet aux usagers de stocker toutes leurs données sur des serveurs internet et d´exécuter leurs programmes à distance. La sous traitance de fonctions permet de cette façon à de grands fournisseurs d´informatique en nuage de maintenir la présence physique de l´informatique en nuage dans des centres de données spécialisés à grande échelle. Ces centres de données sont des espaces spécialisés où de grandes banques d´ordinateurs peuvent gérer centralement, connectées à des connexions internet extrêmement rapides, avec des besoins d´alimentation significatifs. L´informatique en nuage offre d´importants avantages en matière de coûts et d´efficacité, mais comprend également certains risques : les données secrètes ou privées stockées dans le nuage représentent une cible intéressante pour les pirates informatiques ; si une connexion internet d´une entreprise a une défaillance il pourrait être impossible d´accéder aux données ou d´exécuter les activités commerciales ; si le service d´informatique en nuage se déconnecte ou est attaqué par des pirates, toutes les personnes et les entreprises qui l´utilisent seront affectées.

ANNEXE CINQ : MÉTHODOLOGIE

Méthodologie adoptée par le groupe d´experts

Lors de la première session, qui a eu lieu du 17 au 21 janvier 2011, le groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée a adopté une « Méthodologie pour l´étude » :[1]

1. Afin d´exécuter le mandat du groupe d´experts concernant l´étude, la structure indiquée ci-après a été élaborée en vue de faciliter la réalisation de l´étude sous l´égide du groupe d´experts.

2. Chaque pays aura le droit de présenter son point de vue, lequel sera reflété dans l´étude.

3. L´Office des Nations Unies contre la drogue et le crime (ONUDC) sera chargé de développer l´étude, d´élaborer un questionnaire, de collecter et d´analyser les données et de développer un projet de texte de l´étude. Pour accomplir cette tâche, l´ONUDC aura recours aux compétences et à l´expertise de divers services thématiques de l´ONUDC (la Division des traités, la Direction de la recherche et des politiques). À cet effet, des ressources extrabudgétaires suffisantes seront mobilisées afin de permettre à l´ONUDC d´exercer ces fonctions efficacement. Pour aider le Secrétariat à veiller à ce que les besoins, les systèmes et l´expertise technologiques soient représentés de manière adéquate, chaque groupe régional fournira au Secrétariat les noms des experts gouvernementaux (pas plus de six), leurs coordonnées et leur domaine d´expertise. Le Secrétariat consultera les experts en qualité de ressources en fonction des besoins.

4. Le Secrétariat consultera et informera régulièrement le Bureau du groupe des experts sur le processus et distribuera aux états membres le procès-verbal des consultations. L´élaboration de la liste d´experts n´est pas destinée à créer un groupe d´experts à composition limitée ou tout autre organe parallèle ou complémentaire du groupe d´experts.

5. En ce qui concerne la collecte des informations, l´ONUDC préparera un questionnaire qui sera distribué aux états membres, aux organisations intergouvernementales et aux entités du secteur privé (voir le calendrier indicatif ci-après) et qui consistera en un seul instrument de sondage, basé sur les grandes lignes du concept/document de travail de la première réunion du groupe d´experts, tel qu´amendé, et sur les recommandations de la première réunion du groupe d´experts, telles qu´elles figurent dans leur rapport.

6. En second lieu, selon les besoins, le Secrétariat, en gardant à l´esprit qu´il est nécessaire que les différentes régions soient représentées de manière équilibrée, consultera les représentants du secteur privé, ainsi que les représentants des fournisseurs de services internet, les utilisateurs des services et d´autres intervenants pertinents ; les représentants du milieu universitaire, des pays développés et des pays en développement ; ainsi que les représentants des organisations intergouvernementales pertinentes.

1 E/CN.15/2011/19

Actions entreprises

Cette méthodologie a été suivie par le biais des actions mentionnées ci-après :

17 au 21 janvier 2011	Adoption de l´ »ensemble de thèmes à examiner dans une étude complète sur l´impact et la riposte à la cybercriminalité » et la « Méthodologie pour l´étude et le calendrier indicatif » de la première session du groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée
14 septembre 2011	Décision du Bureau de réviser le calendrier indicatif en raison de l´échelonnement de la disponibilité du financement de l´étude et pour diffuser un projet de questionnaire préparé par le Secrétariat en anglais, seulement pour les états membres pour observations avant le 31 octobre 2011.
23 septembre 2011	Projet de questionnaire envoyé à tous les états membres pour observations par la note verbale CU 2011/168.
10 octobre au 16 novembre 2011	Observations écrites relatives au questionnaire reçues des 18 états membres et incorporées par le Secrétariat dans toute la mesure du possible.
19 janvier 2012	Version définitive du questionnaire approuvée par le Bureau.
29 février 2012	Questionnaire envoyé dans six langues officielles à tous les états membres par la note verbale CU 2012/19 à achever avant le 31 mai 2012. Les états membres sont également invités à désigner des organisations spécifiques du secteur privé ou des institutions académiques afin qu´elles reçoivent le questionnaire de l´étude. Les organisations du secteur privé, les institutions académiques et les organisations intergouvernementales sont invitées à compléter le questionnaire de l´étude.
15 au 19 avril 2012	Atelier régional de soutien à l´étude se déroulant à Nairobi, Kenya, auquel assistèrent 10 pays d´Afrique et une organisation intergouvernementale.
24 au 27 avril 2012	Atelier régional de soutien à l´étude se déroulant à Beyrouth au Liban, auquel assistèrent 12 pays d´Asie de l´ouest et d´Afrique du nord et deux organisations intergouvernementales.
5 au 10 mai 2012	Atelier régional de soutien à l´étude se déroulant à Bangkok, Thaïlande, auquel assistèrent 11 pays d´Asie et une organisation intergouvernementale.
11 mai 2012	Note verbale de rappel CU 2012/102 concernant le questionnaire de l´étude envoyé à tous les états membres.
6 juin 2012	Note verbale de rappel CU 2012/117 concernant le questionnaire de l´étude envoyé à tous les états membres. La date d´achèvement du questionnaire est reportée au 30 juin 2012.
13 septembre 2012	Rapport du Secrétariat au Bureau élargi sur le statut des réponses au questionnaire, et la délibération du Bureau élargi sur les étapes suivantes.
1er octobre 2012	Aperçu des informations sur la législation pertinente que le Secrétariat devra utiliser pour l´analyse et l´ébauche envoyées à tous les états membres par la note verbale CU 2012/176 pour observations et corrections, à remettre avant le 9 novembre 2012.
24 octobre 2012	À la suite de la réunion du Bureau élargi du 13 septembre 2012, décision de la présidence du groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée de convoquer la seconde session du groupe d´experts dans la semaine du 25 février 2013.
24 octobre au 30 janvier 213	Commentaires écrits sur la législation reçus des 16 états membres.
9 novembre 2012	Résultats préliminaires de l´étude envoyés aux experts désignés par les groupes régionaux.
6 décembre au 14 janvier 2013	Commentaires écrits sur les résultats préliminaires de l´étude reçus par quatre experts désignés par les groupes régionaux.
30 janvier 2013	Synthèse de l´étude complète sur la cybercriminalité envoyée aux participants enregistrés à la seconde session du groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée.
8 février 2013	Version complète de l´étude sur la cybercriminalité envoyée aux participants enregistrés à la seconde session du groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée.
25 au 28 février 2013	Seconde session du groupe intergouvernemental d´experts sur la cybercriminalité à composition non limitée.

Informations collectées

Soixante-neuf États Membres envoyèrent leurs réponses au questionnaire, avec la répartition géographique suivante :

Afrique	Afrique de l´est	2
	Afrique du nord	4
	Afrique australe	3
	Afrique de l´ouest	2
	TOTAL	11
Amérique	Caraïbes	2
	Amérique centrale	1
	Amérique du nord	2
	Amérique du sud	8
	TOTAL	13
Asie	Asie de l´est	3
	Asie du sud est	4
	Asie du sud	4
	Asie de l´ouest	8
	TOTAL	19
Europe	Europe de l´est	8
	Europe du nord	6
	Europe du sud	4
	Europe de l´ouest	6
	TOTAL	24
Océanie	Océanie	2
	TOTAL	2

Plus de 1500 intervenants du secteur privé, 380 du milieu universitaire, et 80 organisations intergouvernementales furent directement invités par le Secrétariat, en conformité avec la méthodologie de l´étude, à apporter des informations pour l´étude. Des organisations du secteur privé, avec une répartition géographique équitable, furent identifiées par le biais du Pacte mondial des Nations Unies, de l´UIT, et de l´affiliation aux associations de l´industrie. Les organisations académiques furent identifiées au moyen d´une liste des 500 meilleures universités du monde. Quarante entités du secteur privé, 16 du milieu universitaire et 11 organisations intergouvernementales répondirent au questionnaire de l´étude, ou répondirent à un entretien téléphonique basé sur le questionnaire de l´étude :

Organisations du secteur privé	Organisations académiques
Accenture	B-Ccentre
Aconite internet Solutions Ltd.	Beijing Normal University
Admiral Insurance Company	Brown University
Allen & Overy LLP	Eberhard Karls University, Tübingen
Betterley Risk Consultants, Inc.	International Association of IT Lawyers
Casdisa de Promociones, S.A.	Masaryk University
Cisco Systems, Inc.	National Institute of Communication Technologies
Cooperativa La Cruz Azul S.C.L.	Norwegian Police University College
Danfoss A/S	Royal Melbourne Institute of Technology
Digicel Group Ltd.	University of Adelaide

Ernst & Young Global Limited	Université de Durham
Estudio de Informática Forense	Université de Erlangen-Nuremberg
FIRST.org, Inc.	Université de Lausanne
Gloria Group	Vrije Universiteit Brussel
Hewlett-Packard Company	Waseda University/School of Law
Hogan Lovells	Xi'an Jiaotong University
Huawei Technologies Co., Ltd.	**Organisations intergouvernementales**
I2 Integrity International	Conseil de l´ Europe
InfoCom Research, Inc.	Union européenne
International Cyber Security Protection Alliance	FAO
internet Security Alliance	IFAD
ID Experts Corp.	INTERPOL
Juniper Networks, Inc.	OSCE
KPMG International Cooperative	UNCTAD
Logica Pvt Ltd	UNDP
McKinsey & Company, Inc.	UNHCR
Mitsubishi UFJ Financial Group, Inc.	UNICRI
Nippon Telegraph and Telephone Corporation	UNWomen
OSDE Organización de Servicios Directos Empresarios	
Palantir Technologies, Inc.	
PricewaterhouseCoopers	
Superintendencia de Telecomunicaciones (Supertel)	
Symantec Corporation	
Team Cymru, Inc.	
Threatmetrix Inc.	
Trend Micro Inc.	
Trustwave	
Verizon Communications Inc.	
Vodafone Group Plc.	
WISeKey SA	

Les résultats des réponses au questionnaire sont présentés dans l´étude dans un modèle composé, qui présente toutes les réponses possibles à une question déterminée, ou bien qui les présente par région ou par niveau de développement du pays. En raison du nombre restreint de réponses provenant d´Océanie, les régions utilisées sont : « Europe », « Asie et Océanie », « Amérique » et « Afrique ».[2]

La plupart des figures présente le « pourcentage des répondants » qui ont sélectionné une réponse spécifique. Dans le cas où de multiples options de réponses sont permises, les pourcentages sont calculés en fonction du nombre total de pays qui ont répondu à une question particulière (« n »), ou en fonction du nombre total de choix de réponses sélectionnés (« r »). Les valeurs « n » et « r » (comme cela est requis) sont indiquées dans toutes les notes des sources des figures. Donc, lorsque « n » est utilisé comme la base de calcul dans ces questions, la somme des résultats présentés peut être supérieure à 100 %. Plusieurs questions du questionnaire de l´étude permettent de sélectionner une option de la liste déroulante et des réponses ou des éclaircissements libres additionnels.

Dans ces cas, toutes les informations fournies dans le cadre des éclaircissements ou des réponses libres ont été analysées, et les données ont été codifiées de manière appropriée, afin d´intégrer les réponses libres aux réponses de la liste déroulante. Dans certains cas, ceci a donné lieu à l´ajout de nouvelles catégories de réponses dans les figures des résultats.

2 Les régions géographiques utilisées sont celles que définit la Division des statistiques des Nations Unies sur http://unstats.un.org/unsd/methods/m49/m49regin.htm

Lorsque les figures utilisent des données quantitatives fournies par les répondants, ceci est fréquemment présenté en utilisant les données pertinentes du dénominateur, y compris le nombre total d´utilisateurs d´internet dans un pays ou le nombre total des effectifs des services répressifs. Certaines figures utilisent la désagrégation par niveau de développement des pays.[3]Lorsque des données quantitatives sont agrégées, les valeurs présentées correspondent aux moyennes avec des quartiles supérieurs et inférieurs indiqués par les barres additionnelles.

3 Les sources utilisées incluent : les indicateurs de développement de la Banque mondiale, l´incorporation des indicateurs mondiaux de télécommunications de l´UIT /ICT (nombre d´usagers d´internet par pays) ; l´indice de développement humain du PNUD ; l´enquête des Nations Unies sur les tendances de la criminalité et le fonctionnement des systèmes de justice pénale (nombre des effectifs des services de justice pénale et des services répressifs et nombre des infractions enregistrées et des suspects pour les délits de viol et d´homicide).

Page intentionnellement laissée vierge

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel : (+43-1) 26060-0, Fax : (+43-1) 26060-5866, www.unodc.org

Imprimé en Autriche
V.13-8069Février 201300