Section II - Droit pénal. Partie spéciale - Société de l'information et droit pénal

Rapport général

Emilio C. Viano

Dans Revue internationale de droit pénal 2013/3 Vol. 84 , pages 311 à 334
Éditions érès

ISSN 0223-5404
ISBN 9782749240404
DOI 10.3917/ridp.843.0311
Date de mise en ligne : 08/06/2014

I

XIXème Congrès International de Droit Pénal
XIXth International Congress of Penal Law
XIX Congreso Internacional de Derecho Penal

COLLOQUE PRÉPARATOIRE
Moscou (Russie), 24-27 avril 2013
Section I – Droit pénal. Partie Spéciale
Société de l'information et droit pénal

PREPARATORY COLLOQUIUM
Moscow (Russia), 24-27 April 2013
Section I –Criminal Law. Special Part
Information Society and Penal Law

COLOQUIO PREPARATORIO
Moscú (Rusia), 24-27 abril 2013
Sección I – Derecho Penal. Parte Especial
Sociedad de la información y Derecho penal

SECTION II – DROIT PÉNAL. PARTIE SPÉCIALE

SOCIETÉ DE L'INFORMATION ET DROIT PÉNAL

RAPPORT GÉNÉRAL*

Emilio C. VIANO

Selon l'étude sur la cybercriminalité globale (Projet 2013) de l'Office des Nations Unies contre la drogue et le crime (ONUDC), en 2011, environ 33% de la population mondiale, soit 2,3 milliards de personnes, pourrait accéder à Internet. Fait intéressant, près des deux tiers vivent dans les pays en développement et près de la moitié sont âgés de moins de 25 ans. La pénétration rapide et universelle des services à large bande se reflète dans la prédiction que d'ici l'an 2017, 70 % de la population mondiale sera abonnée. Il est clair que d'ici là, il sera difficile de conceptualiser une infraction qui ne laisse pas de preuve électronique reliée à une connexion de protocole Internet. Les récentes révélations d'interceptions massives ou l'enregistrement des communications électroniques aux États-Unis, en Europe et dans d'autres régions du monde par les Etats-Unis et d'autres pays, ainsi que la création d'une banque de données importante sur les communications et les déplacements des personnes, nous donnent un aperçu de la portée et de l'étendue du nouveau monde électronique dans lequel nous entrons. La cybercriminalité augmente de manière exponentielle selon certains. Cela est inévitable compte tenu du fait que toutes les communications et transactions personnelles, professionnelles, commerciales, financières, de la justice, gouvernementales et d'entreprise sont profondément et de plus en plus entrelacées grâce aux outils et aux modalités électroniques. Marchés noirs, vols de données, collectes et ventes de renseignements personnels et financiers, création et distribution de logiciels malveillants, gestion de réseaux de zombies infectant les appareils électroniques, sont parmi les exemples les plus courants de la croissance d'entreprises criminelles heurtant le droit pénal et l'administration

* Le présent rapport général est basé sur les rapports nationaux fournis par les 18 sections nationales. Les rapports nationaux sont résumés plus en détail dans le Résumé des Rapports Nationaux. Ce document suit le format du questionnaire de la section II.

de la justice aujourd'hui. Il semble que la plupart des activités criminelles actuelles sont d'une nature organisée. Les compétences complexes nécessaires pour être un hacker il y a quelques années, ne sont plus nécessaires aujourd'hui. Presque tout le monde, dit-on, peut devenir un hacker et s'engager dans des activités frauduleuses par Internet. Dans de nombreux pays en développement, il a été rapporté que des groupes de jeunes gens se livrent à la fraude et à l'escroquerie.

Partout dans le monde, la cybercriminalité couvre l'ensemble des activités criminelles, du crime financier aux attaques destinées à compromettre la confidentialité, l'intégrité et l'accessibilité du système. Les perceptions de la quantité et de la dangerosité de la cybercriminalité varient. Il y a souvent une grande différence entre la conscience, la perception et la reconnaissance de la part du secteur privé par rapport aux entités gouvernementales. Pour des raisons différentes, allant de l'absence de reconnaissance de la cybercriminalité dans le droit à l'absence de formation appropriée pour la police, les statistiques officielles sont particulièrement peu fiables ou très limitées. Les enquêtes de victimisation, là où elles ont été menées, semblent donner des résultats plus corrects.

Les lois sur la cybercriminalité

Comme pour tout autre problème majeur, social et pénal, la loi est l'instrument privilégié dans la lutte contre la cybercriminalité. Les lois doivent en premier lieu définir et ériger certains cybercomportements en infractions. Ensuite, il existe d'autres domaines d'intervention à approfondir tels que les questions de procédure, les problèmes de compétence, les défis de la collaboration internationale et la responsabilité, souvent controversée, pénale et/ou civile, des "ISP", les fournisseurs de service d'Internet. Dix-sept pays ont répondu au questionnaire de l'enquête de la section II, la majorité d'entre eux à partir de l'Europe ; deux, le Brésil et l'Argentine, de l'Amérique du Sud; un, les Etats-Unis, de l'Amérique du Nord; un, le Japon, de l'Asie ; et aucun d'Afrique ou d' Océanie. Aussi, les résultats doivent être limités à ce contexte. Toutefois, cela peut également refléter l'état de la législation internationale. Trop peu de pays ont des lois substantielles et procédurales adaptées en matière de cybercriminalité. En fait, il s'agit d'une situation déséquilibrée avec l'Europe et l'Amérique du Nord, en particulier, qui ont une législation assez développée alors que de nombreux autres pays ne disposent pas encore d'un véritable corpus législatif dans ce domaine. Ainsi, il y a un déséquilibre entre les différentes régions du monde. Les pays adoptent généralement et plus facilement la législation pénale afin d'interdire certaines infractions cybernétiques. Cette intervention législative ne s'accompagne pas cependant du droit procédural nécessaire pour lutter contre les problèmes délicats tels que la preuve électronique, les protocoles d'enquête, les questions de compétence au-delà des frontières et les accords régissant

l'assistance et la coopération internationales. Il s'agit d'un espace juridique "en construction".

I. Pratiques législatives et concepts juridiques

1. Le droit international et la codification des lois pénales

La Convention sur la Cybercriminalité, également connue comme la Convention de Budapest, est le premier et le seul traité international qui tente de répondre aux crimes de l'ordinateur, de l'Internet et électroniques. Ce texte tente notamment d'harmoniser les législations nationales, de renouveler et renforcer les techniques d'enquête et de favoriser la collaboration entre les différentes nations, essentiellement en Europe. Adopté par le Comité des ministres du Conseil de l'Europe le 8 Novembre 2001, il est entré en vigueur relativement rapidement, en moins de trois ans, le 1er Juillet 2004. Dès le milieu de l'année 2013, 39 Etats l'ont ratifié, principalement en Europe, les Etats-Unis l'ayant également fait en 2008. Le Canada et le Japon, tout en participant activement à la rédaction de la Convention, ne l'ont pas encore ratifiée. Le principal objectif de la Convention est d'introduire un cadre juridique commun et une politique criminelle contre la cybercriminalité définie essentiellement comme une violation du droit d'auteur ou comme des activités frauduleuses utilisant l'Internet, la pornographie juvénile, les crimes haineux et les attaques contre la sécurité du réseau. Il existe des défis considérables dans la mise en œuvre de la Convention en raison des différentes traditions juridiques et des valeurs constitutionnelles, comme, par exemple, le renforcement de la protection de la liberté d'expression aux États-Unis qui limite la mise en œuvre de certaines dispositions contre la pornographie juvénile, les crimes haineux et la xénophobie de la Convention et de son Protocole additionnel de 2008 contre la diffusion de matériel raciste et xénophobe par le biais des médias électroniques. La dernière décennie a connu une activité croissante dans l'élaboration, la discussion et l'adoption d'instruments régionaux et internationaux ayant comme objectif la lutte contre la cybercriminalité. Certains de ces instruments sont contraignants tandis que d'autres ne le sont pas. Parmi les organisations internationales actives dans le domaine, à côté du Conseil de l'Europe, on peut citer l'Union Européenne, la Ligue des États Arabes, l'Organisation des Nations Unies, la Communauté des États indépendants (CEI), la Communauté économique des Etats d'Afrique de l'Ouest (CEDEAO), l'Organisation des États Américains (OEA) et l'Organisation des Nations Unies (ONU). La plupart des pays qui ont répondu au questionnaire de la section II mentionne le Conseil de l'Europe et l'Union européenne comme les sources les plus importantes de leur législation en matière de cybercriminalité et aussi comme fondement de leur légitimité et autorité dans l'introduction de ces lois. Il est important de garder à l'esprit la dimension transnationale de nombreux types de cybercrimes. L'activité criminelle peut provenir de l'extérieur du pays afin de poser intentionnellement des problèmes de compétence.

2. Droit et décisions judiciaires nationales

Les pays abordent généralement le problème de la cybercriminalité par l'intermédiaire du droit pénal, en criminalisant différents aspects de cette délinquance. Le droit pénal traditionnel fournit les définitions et les sanctions nécessaires, parfois complétées par des lois spéciales. Ainsi, les catégories générales préexistantes d'infractions sont souvent empruntées et utilisées pour traiter la nouveauté de la cybercriminalité.

Tous les pays se concentrent d'abord sur la création d'une typologie spécialisée pour les aspects centraux de la cybercriminalité. La seule exception est le Brésil où aucune référence n'est faite à la cybercriminalité dans le code pénal. En Allemagne il n'y a pas non plus de lois spéciales sur la cybercriminalité, mais de nombreuses infractions informatiques sont contenues dans le code pénal. Comme c'est le cas dans de nombreux autres pays, il n'existe pas d'approche systématique. Aux États- Unis, il existe une variété de codes et titres depuis les années 1970 qui criminalisent le vol des ordinateurs, les attaques directes contre des ordinateurs et la conduite criminelle en utilisant des ordinateurs. Globalement, l'impact des décisions de justice est limité. Les différents pays interrogés ne signalent que peu de jurisprudence à ce jour. Par exemple, en Allemagne les décisions judiciaires ont un impact limité sur la législation. Très peu de décisions judiciaires ont conduit à des modifications de la loi sur la cybercriminalité. Les seules exceptions sont la Russie, les Etats-Unis et le Japon. En Russie la Cour suprême aurait joué un rôle actif dans la mise en œuvre de dispositions spécifiques sur la fraude informatique alors qu'aux Etats-Unis, pays de Common Law, les décisions judiciaires ont un impact profond sur le droit pénal relatif à la cybercriminalité. Au Japon, tandis que les législateurs n'ont pas été très actifs dans l'adoption de nouvelles lois pénales ou la modification de lois existantes, le pouvoir judiciaire a joué un rôle important dans l'interprétation extensive des lois pénales dès 1987.

De plus en plus, les pays sont également actifs dans d'autres domaines connexes comme ceux de l'enquête sur la cybercriminalité, les questions de compétence qui sont particulièrement frustrantes étant donné la nature internationale de la criminalité électronique, le domaine des preuves électroniques, et le besoin croissant d'assistance et de coopération internationales.

II. Délits de la cybercriminalité spécifiques

4. Intention

Quand il s'agit de l'état d'esprit requis, la catégorie fondamentale est l'intention ou l'absence de celle-ci. Comme dans toutes les catégories d'infractions, l'état mental de l'auteur est d'une grande importance. Dans tous les rapports nationaux, l'intentionnalité est requise. Bien sûr, il est essentiel de tenir compte des différentes définitions ou compréhensions de «l'intention». Le Brésil exige

une intention spécifique quand il s'agit d'obtenir, modifier ou détruire des données ou de rendre le système vulnérable en vue d'obtenir un avantage illicite. Le Japon exige également une intention spécifique pour de nombreuses infractions édictées " aux fins de … ".

5. Négligence

Les différentes traditions juridiques ont un impact sur la terminologie utilisée en cette matière. Les différentes nuances de la notion de négligence peuvent apparaître sous des marques comme «délibérément », « sciemment », « par négligence » et « imprudence». Globalement, la majorité des pays indique qu'il y a des infractions de négligence dans ce domaine, mais six rapports font état de l'absence d'infractions non-intentionnelles dans cette matière. En règle générale, très peu d'infractions peuvent être commises par négligence.

1. Intégrité et la fonctionnalité du système informatique

A. Accès et interception de la transmission illégale

L'accès à un système informatique est essentiel car c'est la première étape pour des opérations ultérieures. C'est pourquoi la tentative de gagner un accès illégal, non autorisé, à un système informatique a été l'une des premières activités illégales à être criminalisée L'effet négatif majeur est de compromettre l'accès, l'intégrité et la fonctionnalité du système. Ceci ouvre la porte au vol d'identité, aux activités frauduleuses, à la falsification et éventuellement à des actions plus complexes, insidieuses et nuisibles à travers l'implantation de virus, de logiciels malveillants et des botnets. Il n'est pas surprenant que tous les pays qui ont répondu à l'enquête AIDP le criminalisent. Certains utilisent l'expression de qualification spécifique d'«l'accès sans droit». Pour certains, comme les États-Unis, un simple accès sans autorisation ou dépassant le niveau d'autorisation suffit à constituer une infraction. Il n'est pas nécessaire d'utiliser un logiciel spécial pour écraser le système. L'exception est le Brésil qui n'a aucune interdiction spécifique d'accès illégal. Pour de nombreux pays, la production, l'offre, la distribution, la vente et/ou la possession de logiciels ou de périphériques de piratage est une infraction distincte.

Ainsi, les législations des pays qui ont répondu au questionnaire de la section II appliquent des traités et accords internationaux ou régionaux contre la cybercriminalité. Uniformément, ils interdisent l'accès illégal à un système électronique. Il faut également noter que certains pays se concentrent davantage sur les données ou les informations stockées sur un système que sur le système lui-même. D'autres pays, comme la Russie, ne protègent pas toutes les informations. Ils exigent que les informations soient déjà protégées par la loi. Pour compliquer encore plus les choses, certains pays, comme la Turquie, la Pologne, l'Italie, la Suède, le Brésil, la Belgique et le Luxembourg ne définissent pas spécifiquement une ou plusieurs notions comme l'ordinateur ou les données

électroniques. Certains pays considèrent que l'entrée sans autorisation est suffisante pour que l'infraction ait lieu tandis que d'autres exigent un élément supplémentaire comme l'intention ou une action qui fait suite à l'entrée non autorisée. Pour certains, l'entrée illégale est une infraction uniquement lorsqu'elle est liée à comportement subséquent criminel grave. Il semble qu'il existe donc des différences importantes entre certains pays pour lesquels le simple accès sans autorisation est suffisant tandis que d'autres requièrent d'autres éléments, liés par exemple à l'intention ou aux conséquences de l'entrée illégale comme le fait de copier des informations, de modifier ou perturber le fonctionnement du système, du réseau, etc. Ainsi, il y a une zone grise entre le caractère suffisant de la simple entrée et l'exigence d'actions supplémentaires. Aussi la nature du crime ou des crimes commis joue un rôle dans certains pays qui criminalisent l'entrée seulement si elle est reliée à des crimes graves. Il y a aussi des circonstances aggravantes, comme la distribution, divulgation, vente, publication, etc. des données ou des informations obtenues. Dans le cas des données gouvernementales du renseignement de haute sécurité, cela peut entraîner de très graves accusations de trahison et/ou de complicité avec l'ennemi.

B. Les données et les interférences du système

Intimement liées aux activités illégales précédentes, les données et les interférences du système sont criminalisées par de nombreux pays. L'interception non autorisée, la destruction, l'effacement, l'endommagement, la modification de l'information et des données importantes ou l'entrave à l'accès constituent des infractions dans la plupart des pays qui ont répondu au questionnaire de l'AIDP. Interdire l'interception étend la protection aux données qui sont transmises, en dehors et au-delà de celles qui sont stockées. Ceci souligne le caractère confidentiel des données en transit. Il existe à ce sujet des différences substantielles. Par exemple, les tribunaux américains n'ont pas étendu la protection de la vie privée conférée aux courriers en transit aux données transmises électroniquement.

C. Fausses données

À part quelques exceptions, la plupart des pays érige en délit le fait de produire des données fausses ou de falsifier des données authentiques. Afin de protéger les intérêts financiers en particulier, l'utilisation frauduleuse de traitement des données est criminalisée. Les opérateurs et toutes les personnes impliquées sont généralement pénalisés. Certains pays, comme la Finlande et la Suède, n'ont pas de lois spéciales sur la falsification de données et utilisent à la place les dispositions générales sur la contrefaçon. Aux États-Unis, certains Etats, comme la Géorgie, ont des lois spécifiques contre la falsification. Certains pays, comme par exemple l'Allemagne, n'ont pas de définition légale de l'ordinateur et/ou des données électroniques, ce qui pose problème. Certains chercheurs proposent que le mot «données» signifie « une description électronique de l'information ».

D. Abus de dispositifs et hacking

Logiciels, périphériques, mots de passe et codes utilisés pour accéder sans autorisation ou droit de le faire, à des systèmes électroniques sont très en demande et en usage de nos jours, et pas seulement par des particuliers ou des organismes privés. L'application du droit pénal à la mauvaise utilisation des dispositifs et au piratage est complexe en raison des différentes étapes, l'exigence d'une intention ou au moins la connaissance, la conscience de pour quel objectif les données ou ces éléments sont obtenus ou utilisés, et aussi l'importance de la distinction entre les différents types de hackers : les "chapeaux blancs" ou "éthiques" qui mettent leurs compétences vers l'identification des faiblesses systémiques permettant l'accès non autorisé dans le but d'exposer la vulnérabilité et sa correction par rapport aux « chapeaux noirs » ou « contraires à l'éthique » qui tentent de pénétrer irrégulièrement et de mener des activités illégales. Protéger les hackers "chapeau blanc" du risque de poursuites afin qu'ils puissent accomplir leurs précieux services s'observe dans certains pays. Aux États-Unis, paraît-il, l'Administration nationale de la sécurité offre une certification de hackers "éthiques" et ce type de piratage a été largement utilisé par les militaires. Dans l'ensemble, la plupart des pays criminalisent les logiciels, les dispositifs, les mots de passe et des codes qui permettent ou facilitent l'accès non autorisé ou illégal à des systèmes électroniques. Cependant, il existe des nuances subtiles. Par exemple, l'Argentine ne pénalise pas le développement d'outils, d'applications et de programmes ; le Danemark ne criminalise pas l'outil d'un pirate informatique ; l'utilisation non autorisée d'un kit de piratage ? n'est pas criminalisée en Autriche ; l'Italie, la Russie et la Suède ne pénalisent pas la simple possession des outils de piratage et exigent de plus amples informations sur l'intention, l'objectif poursuivi («sciemment »), etc. ; la Russie criminalise un logiciel seulement lorsqu'il est délibérément conçu pour le piratage et l'auteur doit avoir, en outre, l'intention d'utiliser ces outils pour commettre des crimes. Alors que le Japon ne pénalise pas la tentative d'accès non autorisé, il criminalise explicitement "l'utilisation" d'un enregistrement électromagnétique qui donne une commande non autorisée aux fins de l'exécution dans l'ordinateur d'un autre sans motifs valables. Les Etats-Unis, comme la Russie, exigent qu'une personne sache ou ait des raisons de savoir que le but d'un dispositif est le piratage. En Allemagne aussi, l'infraction exige que l'objectif de l'auteur soit de causer des dommages à la personne qui est autorisée à utiliser les données. Le Royaume-Uni adopte une approche différente. Bien qu'il n'y ait pas de réponse du Royaume-Uni au questionnaire de l'AIDP, il est intéressant de noter que dans ce pays l'accès non autorisé n'est pas légal. Le Code pénal allemand sanctionne les actes préparatoires à une infraction, mais, de manière incohérente, il ne pénalise pas la tentative de commettre la même infraction. La production, l'acquisition, la vente, la diffusion ou la fourniture d'un mot de passe ou autres codes de sécurité

qui permettent l'accès aux données constituent des infractions. Les mêmes actes liés aux logiciels sont également pénalisés. Il n'existe aucune disposition exonérant des activités de piratage des hackers "chapeaux blancs". Le seul élément qui peut aider à exclure la responsabilité pénale est l'absence de mens rea. Il n'y a aucune infraction qui pénalise la diffusion de l'information piratée en général. Toutefois, la divulgation de secrets industriels au public est punissable comme la distribution faite avec l'intention d'obtenir un gain financier ou de causer des dommages financiers à autrui. La simple possession de l'outil d'un pirate n'est pas expressément criminalisée dans le code pénal allemand. Il est considéré comme une infraction administrative.

Aux Etats-Unis, les kits de piratages ne sont pas strictement réglementés. Leur utilisation n'est sanctionnée que si les informations ou données obtenues sont divulguées. La politique principale est de développer des contreforts, d'augmenter la sensibilisation du public, et de transférer la responsabilité à l'utilisateur qui doit avoir une protection anti-virus ou anti-malware etc., mise à jour régulièrement, plutôt que de se concentrer sur le piratage, en particulier pour protéger les pirates gouvernementaux et militaires "éthiques".

2. Protection des données

A. Violation du secret des données privées

Les données privées sont définies ici comme des données qui appartiennent à la vie privée des personnes, mais qui n'identifient pas ou ne permettent pas d'identifier l'état civil, l'orientation sexuelle, l'état de santé, les habitudes et les préférences d'achat du sujet. Ces données sont parfois collectées automatiquement depuis qu'elles existent dans le compte électronique de la personne, par exemple par le biais de cookies, ou elles sont obtenues à partir des personnes qui doivent fournir cette information afin d'obtenir certains avantages comme l'assurance médicale, une carte de crédit, un compte bancaire, le permis de conduire, l'inscription à un programme ou un cours à l'université, l'obtention d'une appartenance à une organisation, club, fidélisation ou d'un programme de client fréquent, etc. Compte tenu des nombreuses révélations faites, notamment par Wikileaks, Edward Snowden et d'autres, la question de ce que «la vie privée » signifie vraiment aujourd'hui, de la valeur réelle des promesses de protéger cette intimité par des collecteurs de données par rapport à leurs pratiques réelles, et le rôle que des divers organismes gouvernementaux légalement, illégalement, en contournant la loi, ou interprétant la loi à leur avantage peuvent jouer, est d'une importance primordiale. Par exemple, il a été rapporté que, bien que Microsoft promette à ses utilisateurs de respecter leur vie privée, il a collaboré étroitement avec les services de renseignement américains pour permettre l'interception des communications des utilisateurs, notamment en aidant l'Agence Nationale de Sécurité (NSA) pour contourner le cryptage de la compagnie de messages et de chats. D'autres révélations récentes montrent que ce n'est que

l'un des nombreux grands fournisseurs de services d'internet qui collabore avec les gouvernements et les agences de renseignement. En Juin 2013, le journal The Guardian a révélé que la NSA a affirmé avoir «accès direct» à travers son programme de Prisme aux systèmes de nombreuses grandes entreprises de l'Internet, comme Microsoft, Skype, Apple, Google, Facebook et Yahoo. Il a été rapporté dans les médias que, si l'Union Européenne et plusieurs pays ont exprimé leur indignation d'être espionnés par les Etats-Unis, ils ont effectivement coopéré et ont même participé au programme dans une certaine mesure. Il a également été mis en lumière l'augmentation des liens et des échange d'informations entre les programmes de surveillance et d'espionnage de l'armée américaine, des agences de sécurité et le secteur privé, en particulier les organismes financiers et bancaires, afin de donner aux élites des informations précieuses, parfois à l'avance, leur permettant ainsi de continuer à dominer les marchés. Tout cela doit être pris en compte au moins pour mettre en perspective les différentes assertions, les garanties et les lois qui sont censées régir et protéger la vie privée des citoyens et des consommateurs dans les différents pays. Alors que les lois peuvent effectivement avoir un effet protecteur de la vie privée, leur application est parfois remise en cause. Selon divers rapports des médias, une réglementation proposée récemment par l'Union Européenne pour protéger la vie privée du citoyen et du consommateur a été affaiblie et différée en partie à cause du lobbying non agressif mais intensif des Etats-Unis et des principaux fournisseurs d'accès à Internet. L'exploration de données est tout simplement trop rentable. Les fondements juridiques, éthiques et civiques de la vie privée promis au citoyen et au consommateur par la loi, là où elle existe, et par les géants des médias électroniques et sociaux, doivent être réexaminés, reconstruits et renforcés au niveau international pour rétablir un seuil minimum de crédibilité et d'efficacité.

Tous les pays qui ont répondu au questionnaire de l'AIDP pour la Section II, ont, à des degrés différents, des systèmes législatifs élaborés qui protègent apparemment les droits du citoyen et du consommateur et leur accès au système électronique des réseaux sociaux, ainsi que leurs inscriptions à diverses activités, programmes et adhésions, transactions financières et bancaires ou obtentions de divers types d'assurance, notamment médicale.

Les collecteurs de données sont généralement tenus de divulguer leurs pratiques d'information avant de recueillir des renseignements personnels des consommateurs. La plupart des pays exige également que la politique de confidentialité soit affichée. L'omission de divulguer la politique de confidentialité est considérée dans certains cas comme un délit (Croatie) et dans d'autres comme une infraction administrative (Italie), sanctionnée par une amende (Danemark). Il est intéressant de noter qu'aux Pays-Bas les données ne sont pas considérées comme des biens ; par conséquent, elles ne sont pas soumises aux

infractions contre les biens. La législation du Japon sur la protection des renseignements personnels ne pénalise pas le transfert et la diffusion de données privées en tant que tels, sauf s'ils sont considérés comme des «secrets commerciaux». La loi fédérale allemande sur la protection des données impose que les données personnelles soient collectées à l'aide de la personne qui les détient, c'est-à-dire de la personne concernée. Cela nécessite la sensibilisation et le consentement de la personne concernée ainsi que sa participation dans le processus de collecte des données. Le droit de collecter des données sur une personne sans que celle-ci ne le sache existe uniquement dans des circonstances exceptionnelles. Si les données sont recueillies sans le consentement de la personne concernée, des obligations d'information particulières doivent être remplies par la suite. La notification doit être généralement compréhensible. Il faut noter que la violation de ces droits ne conduit ni à des sanctions pénales, ni à des sanctions administratives mais à l'intervention du droit civil. Il n'y a également aucune disposition de base qui criminalise de façon générale la transmission et la distribution des données privées. Il faut noter qu'en vertu du droit allemand, la collecte, le traitement et l'utilisation peuvent être légitimes si la législation le permet par le biais de diverses lois particulières ou s'il y a consentement de la personne concernée. Ces principes juridiques sont également applicables aux télécommunications. Aux États-Unis il n'y a pas de loi générale. Il existe des lois spéciales comme la Loi pour protéger les enfants en ligne, la loi Gramm -Leach- Billey qui oblige les institutions financières à mettre en place des garanties appropriées et à fournir une information claire et visible aux consommateurs et la Loi sur la portabilité de l'assurance maladie qui réglemente l'utilisation et la divulgation de l'information protégée sur la santé. Des inquiétudes ont été émises à propos de la protection de la base de données créée par la loi sur la portabilité de l'assurance maladie (la «Obamacare»), qui couvrira toute personne dans les Etats Unis. Cette gigantesque base de données comprendra des données sur les revenus, la taille de la famille, la citoyenneté, le statut d'immigration, le statut d'incarcération, le numéro de sécurité sociale et des informations privée relatives à la santé. Elle va compiler des fichiers sur toute personne aux Etats-Unis et obtiendra ses informations de l'Internal Revenue Service (IRS), du Département of Homeland Security, du Ministère de la Défense, de l'Administration des anciens combattants, de l'Office of Personnel Management, de l'Administration de la sécurité sociale, de la base de données de Medicaid, et du Peace Corps. Par exemple, un bénéfice annuel enregistré sera comparé aux déclarations d'impôt sur le revenu et corrigé en conséquence, s'il y a un écart. Il est à craindre, en premier lieu, que cette base de données soit une cible irrésistible pour les pirates. En outre, la loi prévoit que des organisations privées à but non lucratif, soi-disant protectrices des consommateurs et de la collectivité, appelées «Navigateurs », seront en mesure d'accéder à l'information pour recevoir des subventions afin

qu'elles puissent informer le public sur le nouveau système de santé obligatoire, conseiller et orienter les clients vers des fournisseurs d'assurance. Le risque d'abus est très important. Le potentiel de profits sur la vente de telles informations détaillées et officielles pour toutes sortes de fins, comme l'emploi, la carrière, le niveau de revenus, le pouvoir d'achat, l'assurance, les investissements, l'employabilité, l'admission à certaines lignes de travail ou carrières, l'histoire de la santé, la commercialisation de remèdes, médicaments, et même l'aptitude au mariage dans certaines cultures ethniques, etc., sera très élevé. Avec autant d'organisations privées ayant accès à ces informations intimes sur pratiquement chaque personne aux États-Unis, les experts sur la cybercriminalité s'attendent à de graves atteintes et violations de la vie privée.

B. Violation du secret professionnel

Dans la plupart des pays interrogés, le Code de procédure pénale garantit la confidentialité des avocats, membres du clergé, médecins, psychologues, psychiatres, etc. Les informations sur le personnel et/ou la vie familiale obtenues par les professionnels dans le cadre de leur profession sont protégées. Cependant, cette protection connait des limites. Il existe en principe des obligations de révéler dans l'intérêt public ou l'intérêt prévalant d'un tiers (par exemple, la maltraitance des enfants), si un crime grave est commis ou tenté, et si une personne innocente risque d'être accusée ou reconnue coupable d'un crime. Cependant, par exemple, il n'existe aucune obligation générale en droit finlandais de dénoncer un crime, mais si le crime pouvait encore être évité, il peut y avoir responsabilité pénale pour le fait de ne pas l'avoir signalé.

D'autre part, la loi italienne exige que les professionnels communiquent leurs collectes d'informations et pratiques de gestion avant de recueillir des renseignements personnels des patients ou des clients. Ils doivent divulguer leurs pratiques en matière de traitement des données, mais pas leurs obligations éthiques. Ils doivent informer le patient ou client au sujet de leur contrôle sur la divulgation des données personnelles. La loi prévoit une protection spéciale pour l'identification, les données sensibles et judiciaires.

En Allemagne, la loi fédérale sur la protection des données protège les données personnelles. Des obligations spécifiques de secret professionnel s'appliquent, par exemple, aux membres des organismes de services publics à propos des informations dont ils ont connaissance dans le cadre de leurs activités professionnelles. La même règle s'applique au personnel médical, aux avocats et aux conseillers fiscaux. Toutefois, la divulgation de secrets autorisés par la loi est licite. Le consentement du sujet ou autre justification comme la nécessité (par exemple, pour prévenir un danger imminent) rend également légitime la divulgation de secrets. L'intérêt public peut également être considéré comme ayant une valeur supérieure à l'intérêt de la personne à protéger. Ainsi, les professionnels médicaux doivent divulguer certaines maladies lorsque les

organismes de santé publique l'exigent, les maladies professionnelles aux compagnies d'assurance, la prescription des substances qui se substituent aux drogues illicites, informer les entreprises d'assurance-maladie, et aviser les autorités de naissances ou de décès. Tout le monde doit révéler des informations sur les crimes graves prévus. Le Code pénal allemand vise en détail les professionnels qui ont le devoir de conserver les informations confidentielles qui leur sont confiées. La divulgation et l'exploitation des secrets personnels constituent des infractions pénales.

En ce qui concerne le monde des affaires, aux Pays-Bas, c'est un crime de diffuser intentionnellement au public des informations qu'on est tenu de garder secrètes, comme, par exemple, par rapport à une entreprise où l'on est employé.

C. Traitement illégal de données personnelles et privées

Aux États-Unis, l'utilisation illégale, le transfert et la diffusion de données privées ne sont pas criminalisés. Si quelqu'un subit un préjudice, il doit exercer un recours civil, ce qui peut représenter un coût considérable. Dans d'autres pays (comme le Brésil) le transfert et la distribution illégales des données privées ne sont pas inscrits dans la loi. A l'inverse, en Croatie, au Danemark, en Finlande, en Italie et en Turquie, l'utilisation illégale, le transfert et la diffusion de données privées sont criminalisés. En Allemagne, la collecte illégale, la rétention et le transfert de données à caractère personnel constituent également des infractions. Cependant, l'utilisation illégale n'est généralement pas criminalisée, tout dépend de la situation et du contexte. La collecte des données par les autorités de police en Allemagne n'est licite que si des dispositions légales spéciales le permettent. Au Japon, alors que l'acquisition illégale de données personnelles et des informations constitue un crime**,** la conduite non autorisée relative aux données privées n'a pas été largement criminalisée, à l'exception des secrets commerciaux. Le vol de données personnelles ne représente pas un problème juridique sérieux en Russie comme aux États-Unis ou en Europe. La première loi a été adoptée en 2006 après la ratification de la Convention du Conseil de l'Europe sur la Protection des Individus et prévoit la responsabilité pénale. Cependant, il n'y a pas de dispositions spéciales pour une infraction qui est commise en réseaux informatiques.

L'approche de cette question aux Pays-Bas est très intéressante. Les données ne sont pas considérées comme des « biens» au regard du droit pénal néerlandais. La raison est que les données manquent d'«unicité ». Elles sont en fait multiples. Une personne qui contrôle les données n'en perd pas nécessairement le contrôle si quelqu'un d'autre y a accès, par exemple, en les copiant. La personne les a encore. En conséquence les criminels qui envoient des informations volées digitalement à des tiers ne sont pas punissables, sauf s'ils sont également les pirates.

D. Le vol d'identité

La diversité des moyens de communication personnelle, l'affichage de renseignements personnels, de photographies, et plus encore l'automatisation du traitement des données et la croissance exponentielle de tous les types de transactions qui ne se font plus face-à-face ont parallèlement augmenté les possibilités de vol de renseignements personnels touchant l'identité, notamment l'aspect financier, grâce à l'utilisation de systèmes électroniques. Les cibles recherchées sont les informations contenues sur les cartes de crédit, les comptes bancaires, les documents d'identité comme le permis de conduire ou le passeport, et les adresses IP. Le vol peut se réaliser grâce à un accès non autorisé à des dispositifs électroniques et/ou à des comptes d'une personne, évoqué précédemment comme étape fondamentale pour la commission de la cybercriminalité, au moyen de logiciels malveillants, le phishing ou l'obtention illégale d'informations en vertu de la position, des contacts, ou de l'accès que l'auteur a aux banques de données. Ces données sont accessibles à volonté par les salariés des entreprises gouvernementales dont l'éthique et la capacité de résister aux sollicitations appropriées ne sont pas toujours les traits les plus forts. L'obtention, le transfert, et l'utilisation des données personnelles ainsi obtenues pour des activités criminelles devraient certainement être criminalisés. En fait, au niveau international, il apparaît qu'aucun instrument international contraignant n'envisage et proscrit le vol d'identité. Au niveau national, sur la base des réponses au questionnaire AIDP de la Section II, la plupart des pays utilise des dispositions générales pour criminaliser; certains ont des dispositions spécifiques d'utilisation et d'autres ne l'interdisent pas en tant qu'infraction. Par exemple, l'Argentine, l'Autriche, le Brésil, la Croatie, le Danemark, la Finlande, l'Allemagne, l'Italie, les Pays-Bas, la Fédération de Russie et la Suède n'ont pas dans leur code pénal une interdiction spécifique d'usurpation d'identité. Cependant, en Allemagne, par exemple, des actions spécifiques concernant le vol d'identité peuvent être criminalisées comme infractions administratives ou pénales. Le Brésil inclut le vol d'identité dans les crimes contre la propriété ; en Croatie, il peut être sanctionné comme utilisation illicite de données à caractère personnel ; au Danemark sous les statuts de falsification, vol et fraude ; en Italie, on peut appliquer d'autres catégories comme l'usurpation d'identité, le gain ou les dommages financiers ; et aux Pays-Bas, on peut utiliser le délit de tromperie ou d'extorsion. La position de la Finlande est assez intéressante car elle ne classe pas l'identité d'une personne comme un bien mobilier qui peut être volé. Quelques autres pays, comme la Belgique, le Luxembourg, la Pologne, la Roumanie, la Turquie et les Etats-Unis ont adopté des dispositions spécifiques. Au Japon, le phishing a récemment été pénalisé, mais il n'y a pas de disposition pénale qui punit les atteintes à la personnalité numérique d'une personne.

3. Protection contre les contenus illicites

A. Objet

i. Pornographie juvénile

L'importance du rôle de l'Internet dans la diffusion mondiale de la pornographie est bien connue. La disponibilité instantanée, par internet, du matériel pornographique dans l'intimité de son lieu de résidence ou de son espace personnel constitue un puissant stimulant pour un grand nombre de personnes. Certains soutiennent d'ailleurs qu'au début du phénomène Internet, c'est surtout la pornographie qui a conduit à l'expansion de ce moyen de communication et qui a démontré son potentiel lucratif. L'anonymat et la confidentialité sont des facteurs très attrayants. Depuis une époque récente, on observe un effort international important pour intervenir efficacement contre la pédopornographie et diminuer considérablement, voire éliminer, la diffusion des images et leur la rentabilité**.**

Tous les pays qui ont répondu au questionnaire pénalisent la production, la transmission, la fourniture, l'exportation, l'accès, le téléchargement et le stockage des images de pornographie juvénile. Ils interdisent également l'utilisation de moyens électroniques pour toutes les fonctions liées à la production, à la distribution, à l'accès, au téléchargement, à la possession et l'exportation de pornographie juvénile. Au Japon, ces activités cybernétiques ont été incluses en 2004 dans la loi sur la répression des activités liées à la prostitution des enfants et la pornographie impliquant des enfants. En 2009, l'Allemagne a adopté une loi qui oblige les fournisseurs d'accès à bloquer des sites Web affichant du matériel pornographique juvénile. Toutefois, la loi n'a jamais été appliquée et elle a finalement été abrogée en 2011. Actuellement, en Allemagne, les fournisseurs de services d'Internet effacent directement la pornographie juvénile en coopération avec l'agence de la police fédérale. L'Association internationale des lignes directes internet (INHOPE) joue un rôle actif dans ce domaine en coopérant avec les autorités nationales. Si un contenu pornographique impliquant des enfants est détecté par l'un des membres du réseau, les partenaires nationaux du INHOPE sont contactés. Le fournisseur d'entreposage, qui est responsable de la transmission du contenu, est prié de le supprimer. En Europe, refuser de supprimer du contenu illégal constitue une infraction pénale. Par conséquent, les efforts pour effacer la pornographie juvénile sont plutôt réussis. Dans le cadre de la traite, certains pays, par exemple, l'Italie et les Pays-Bas, interdisent également le «grooming», le leurre et l'exploitation des enfants ou la sollicitation en ligne d'enfants, comme l'Argentine, à des fins pornographiques. Une exception notable est la Belgique et le Luxembourg où la loi ne prévoit pas expressément l'utilisation de l'Internet pour attirer et exploiter les enfants à des fins sexuelles. Certains pays, comme la Pologne, la Russie et la Suède, ne définissent pas expressément la pornographie enfantine. La plupart des autres pays (Argentine, Autriche,

Croatie, Danemark, Finlande, Italie et États-Unis) utilisent des définitions conformes aux normes internationales, à la différence du Japon qui utilise une autre définition. La Finlande n'utilise pas le terme «pornographie juvénile» ou «spectacle pornographique» dans son Code pénal. Dans le cas des pays qui n'ont pas de dispositions spécifiques sur la pédopornographie, celle-ci peut être passible de poursuites sur d'autres fondements. En Russie, par exemple, le contenu illégal est interdit en tant qu'activité extrémiste dans les communications publiques qui peuvent nuire à des enfants. Donc le code pénal ainsi que la loi sur l'extrémisme peuvent être utilisés. La Pologne considère les réseaux informatiques mondiaux comme un lieu public pour la communication. Bien qu'il n'existe aucune définition légale de la pornographie juvénile dans le droit pénal suédois, sa signification est proche de celle des instruments internationaux. Globalement, c'est la représentation visuelle et matérielle qui est interdite. Les matériaux auditifs ne sont pas souvent couverts. En outre, puisque les actions liées à la pornographie juvénile peuvent être commises à l'aide de différents médias et d'images disponibles hors ligne, dans un certain nombre de pays, il existe une préférence pour une approche générique et neutre qui couvre la «technologie et les médias» plutôt qu'un ordinateur spécifique. Il existe enfin des différences dans la terminologie utilisée pour décrire la population qui doit être protégée, notamment quant à la limite d'âge qui donne droit à la protection. Un certain nombre de pays ont utilisé l'expression «mineurs», comme l'Argentine et l'Autriche. La plupart des pays utilisent «enfant» comme la Croatie, le Danemark, la Finlande, l'Italie, la Russie, la Turquie et les Etats-Unis. La Belgique et le Luxembourg utilisent les deux notions, « mineurs » et « enfants ». La Pologne vise plutôt l'âge réel, se référant à des enfants de 15 ans ou moins. Il faut noter que le Conseil de l'Europe permet de fixer l'âge à 16 ans. La Convention des Nations Unies relative aux droits de l'enfant définit l'enfant comme «toute personne âgée de moins de 18 ans» (article 1). Certains pays abordent la question de la pornographie juvénile produite par des mineurs. L'Autriche ne criminalise pas la pornographie faite avec le consentement de l'enfant et pour l'usage de l'enfant. La Croatie utilise la limite de «moins de 14 ans» pour étendre la non-responsabilité. Il existe une importante controverse et parfois des pressions en faveur de la criminalisation de ce qu'on appelle le «sexting», c'est-à-dire des mineurs qui envoient des messages de texte sexuellement explicites, parfois accompagnés de photos tout aussi explicites, à d'autres mineurs. La question de l'élément moral revêt également des nuances différentes, selon les pays. Certains pays exigent que la personne qui accède à la pornographie juvénile le fasse en connaissance de cause. Pour l'Argentine, c'est un crime d'accéder «sciemment» à la pornographie juvénile, de la transmettre, de l'exporter, et de la détenir. L'Autriche, la Croatie, le Danemark et les Etats-Unis suivent la même approche. Certaines juridictions exigent à la fois l'intention d'entrer dans un site de pornographie juvénile et sachant que de telles images

sont là: la Belgique, le Luxembourg et la Suède. La Pologne et l'Italie ne pénalisent pas le fait d'accéder simplement à de la pornographie juvénile. En Russie, "la simple possession " n'est pas criminalisée. La possession de la pornographie juvénile au Japon constitue une infraction uniquement si c'est à des fins de diffusion. L'Allemagne exige l'intention de l'auteur d'accéder à de la pornographie juvénile en tenant compte à la fois de l'âge de l'enfant et du caractère pornographique du matériel affiché. La possession par négligence de la pornographie juvénile n'est pas punissable en droit pénal allemand. Il existe aussi des différences intéressantes quant à l'intervention judiciaire. Dans certains pays, comme le Brésil, l'Italie, le Japon et la Pologne, les juges sont relativement impuissants à intervenir. Dans d'autres pays, les juges ont pleine autorité pour ordonner la suppression, la confiscation etc. comme en Autriche, Belgique, Allemagne, Luxembourg, Danemark et Turquie. Aux États-Unis, il n'existe aucune disposition légale permettant aux juges d'ordonner la suppression de matériel pornographique infantile.

Enfin, la pédopornographie virtuelle est un sujet majeur de débat et d'action juridique. Dans certains pays, comme l'Argentine, la Turquie, le Japon et les États-Unis, ce n'est pas une infraction. De la même façon en Autriche lorsque l'image est uniquement à usage privé. C'est en revanche une infraction en Belgique, Luxembourg, Brésil, Danemark, Finlande, Italie, Pays-Bas, et Suède. En Allemagne, la pédopornographie virtuelle s'inscrit dans le cadre du Code pénal, mais le matériel doit donner l'impression d'activités «réelles» de «vrais enfants». Un vif débat public sur la nécessité de légaliser la pédopornographie virtuelle afin d'offrir une alternative aux pédophiles a eu lieu fin 2012/début 2013 aux Pays-Bas. Aux États-Unis, en Avril 2002, la Cour Suprême américaine dans *Ashcroft v Free Speech Coalitio*n, 535 US 234 (2002) a constaté que la loi sur la prévention de la pornographie juvénile était inconstitutionnelle. Bien qu'il demeure illégal de faire, montrer ou posséder des photos sexuellement explicites d'enfants, la Cour a conclu qu'il n'y avait aucune raison impérieuse d'interdire la fabrication, l'exposition ou le stockage de photos, qui semblent simplement être des enfants. Deux catégories de pornographie qui étaient illégales en vertu de la loi sont maintenant légales: les images sexuellement explicites d'enfants qui semblent plus jeunes que leur âge réel, et les images sexuellement explicites d'enfants produits par ordinateur. Dès lors qu'aucun enfant réel n'est impliqué dans la production de ces images, la Cour suprême américaine estime qu'elles sont protégées par la liberté d'expression. Cependant, la pornographie juvénile virtuelle peut être un crime si elle est obscène, c'est-à-dire en l'absence de "LAPS "(acronyme anglais), à savoir, si elles n'ont aucune valeur littéraire, artistique, politique ou scientifique.

ii. Tout autre objet où la criminalisation dépend de l'utilisation de l'information et de la communication (TIC)

a. Création et utilisation d'un véritable anonymat :

Comportement non criminalisé : Argentine, Belgique, Luxembourg, Danemark, Finlande, Allemagne, Italie, Japon, Suède et États-Unis.

Comportement criminalisé : Croatie

b. Cyber- intimidation (« bullying »)

D'une part, une partie des participants à la section II affirme que les infractions déjà «existantes» dans le Code pénal comme le harcèlement criminel, les menaces, l'intimidation, l'utilisation non autorisée d'un ordinateur, l'extorsion, le libellé diffamatoire et la pédopornographie couvrent déjà les comportements d'intimidation les plus graves, ce qui rend inutile une nouvelle législation spéciale.

A l'opposé, d'autres exigent que le Code criminel soit révisé et modifié pour mettre à jour certaines infractions existantes et lutter contre le harcèlement par voie de médias électroniques. Ils estiment également nécessaire de mettre à jour les pouvoirs d'enquête pour l'application de la loi, de sorte que tous les actes de cyber-intimidation perpétrés grâce aux nouvelles technologies puissent faire l'objet d'enquêtes et de poursuites. Beaucoup de codes pénaux contiennent déjà des dispositions qui interdisent l'envoi de faux messages par lettre, télégramme, téléphone, câble et radio ainsi que des appels téléphoniques indécents ou constitutifs de harcèlement. Tels que les Codes sont rédigés actuellement, ces infractions ne peuvent pas couvrir les situations de cyber-intimidation lorsque les messages sont envoyés par texte ou par courriel. Ainsi, il y a des pays où la cyber-intimidation est une incrimination spécifique, et d'autres où ce n'est pas le cas, avec parfois la justification que les lois actuelles sur les supports papier peuvent remédier à la situation avec quelques légères modifications.

« Cyber bullying » pas criminalisé : Argentine, Finlande (pas directement pénalisé, mais utilisation de diffamation possible), Danemark (pas de dispositions spécifiques, d'autres lois sont utilisées), Allemagne, Italie, Japon, Suède et Turquie. Il faut noter que la cyber-intimidation peut être incluse dans la commission d'infractions pénales existantes, comme en Allemagne, par exemple.

Criminalisé : Belgique, Luxembourg, Croatie, Pologne, Etats-Unis (lois des certains Etats)

c. Cyber- poursuite («stalking»)

Non criminalisé : Argentine, Finlande (pas de dispositions spécifiques, l'utilisation d'ordonnances restrictives est possible), Danemark (pas de dispositions spécifiques, d'autres lois sont utilisées), Italie, Japon, Pays-Bas (aucune infraction spécifique), Suède et Turquie. Dans certains de ces pays, comme au Japon, par exemple, d'autres dispositions du code pénal peuvent être utilisées pour mettre en oeuvre la cyber-poursuite.

Criminalisé : Belgique, Croatie, Allemagne, Luxembourg, Pologne, Etats-Unis (lois fédérales et étatiques)

d. Cyber- pansage

Non criminalisé : Argentine, Turquie, Japon, Suède

Criminalisé : Allemagne, Italie, Pays-Bas, Pologne, Etats-Unis (loi fédérale)

4. Violations des droits de propriété, y compris la propriété intellectuelle

La propriété, les actifs financiers et l'authenticité des documents sont les principaux intérêts protégés ici. La manipulation et l'interférence avec un système électronique ou informatique sont principalement destinées à produire des avantages financiers au bénéfice du pirate.

A. Fraude

Quand il s'agit de fraude, la plupart des pays pénalisent la fraude par Internet. Il existe quelques exceptions. Aux Pays-Bas, en dehors de la pornographie juvénile, il n'y a pas d'autres infractions connexes au contenu en fonction de l'utilisation des technologies d'information et de communication. Les infractions connexes au contenu sont considérées comme «technologiquement neutres». En Roumanie, outre la criminalisation des infractions contre les droits d'auteur, aucune autre responsabilité pénale n'est explicitement indiquée. La loi russe n'est pas non plus explicite à ce sujet. La législation suédoise n'interdit pas spécifiquement et ne pénalise pas la fraude perpétrée grâce à l'utilisation des technologies d'information et de communication. Au Japon, la fraude informatique a été introduite dans le Code pénal en 1987.

B. Violation des droits de propriété intellectuelle

La plupart des pays reconnait la violation des droits de la propriété intellectuelle. Certains, comme l'Autriche, adoptent et intègrent dans leur législation la directive européenne 2001/29/CE 3, par exemple dans les articles qui protègent les mesures techniques, programmes informatiques et l'étiquetage. Autrement, la Belgique, le Luxembourg et le Japon n'ont pas de dispositions spéciales pour les violations des droits de propriété intellectuelle sur et à travers l'Internet, mais il est convenu que les lois générales de propriété intellectuelle s'appliquent dans ce cas. Le Brésil n'incrimine, en général, aucun acte dans le monde virtuel. En dehors de la pornographie enfantine, les Pays-Bas ne pénalisent pas la commission d'un crime perpétré dans le monde virtuel en l'absence de personnes réelles impliquées. Selon la Cour suprême néerlandaise, les données ne sont pas des biens en raison d'une qualité essentielle des biens qui est que la personne qui les possède doit en perdre le contrôle au profit d'une autre personne qui, à son tour, en prend le contrôle. Les données numériques n'ont pas cette propriété parce qu'elles peuvent être contrôlées par deux ou plusieurs personnes à la fois. Toutefois, dans l'affaire *Runescape* (2012), la Cour suprême néerlandaise a jugé

que les objets virtuels sur un jeu d'ordinateur sont des biens qui peuvent faire l'objet d'un vol, pour autant qu'il s'agit d'un objet qui peut être soustrait au contrôle *de facto* d'une autre personne. Dans le cas *Runescape*, une personne réelle a commis le vol de biens virtuels au détriment d'une autre personne réelle.

La Roumanie pénalise les infractions contre les droits d'auteur. Aucune autre responsabilité pénale n'est explicitement indiquée.

La Russie a joint l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) en 1996. La loi russe a été mise à jour pour répondre aux normes internationales pour la protection juridique des droits d'auteur. Les articles 146 et 147 du Code pénal russe sont applicables aux cyber-infractions. La loi suédoise, au contraire, n'interdit pas spécifiquement et ne pénalise pas la fraude et la violation des droits de propriété intellectuelle commises par le biais des technologies de communications par Internet. Aux États-Unis, la fraude au moyen d'un ordinateur, la violation des droits de propriété intellectuelle et le trafic de biens et services contrefaits sont criminalisés.

C. Espionnage industriel

Un certain nombre de pays pénalise l'espionnage industriel (Danemark, Finlande, Italie, Japon) sur la base des dispositions générales (par exemple, la concurrence déloyale et les lois sur les droits d'auteur); la Pologne sur la base d'une protection de la propriété intellectuelle et des lois contre la concurrence déloyale; la Russie, pas spécifiquement mais sur la base des dispositions générales sur la collecte illégale de secrets commerciaux ; la Turquie ; la Suède ; et les Etats-Unis qui interdisent le vol de secrets commerciaux et l'espionnage industriel.

5. La criminalisation des actes commis dans le monde virtuel

Les actes commis dans le monde virtuel ouvrent de nouvelles frontières en droit pénal et mettent à l'épreuve les principes et les définitions traditionnelles, comme celle de «biens» (pour la pédopornographie virtuelle, voir ci-dessus). Le discours porte sur les blessures et dommages dans le monde virtuel qui exigent des remèdes dans le monde réel. Le débat est de savoir si le monde de l'Internet est assez spécifique pour exiger sa propre réglementation. Certains soutiennent qu'avant d'approuver des règles propres à l'Internet, la société doit comprendre pourquoi les activités sur l'Internet sont si différentes ou spéciales et par conséquent pourquoi elles justifient leurs propres règlementations spécifiques. L'une des questions les plus importantes porte sur les fondements et les sources du droit cybernétique. Certains considèrent le cyberespace comme nouveau, indépendant et à part, capable et autorisé à créer ses propres institutions et à articuler ses propres lois. D'autres ne voient pas comment et pourquoi les transactions sur Internet sont différentes des transactions transnationales du monde réel et pourquoi elles devraient être hors de la portée de la réglementation territoriale normale. En d'autres termes, en utilisant l'Internet ou les

communications électroniques, fait-on un pas hors du monde «réel» dans un monde virtuel, ce qui est tout aussi vrai avec ses définitions, ses règles et les sanctions ? Doit-on sortir de son propre pays dans une juridiction mondiale ou, un jour, de l'espace, sans frontières et universelle, acceptant implicitement la compétence de tous les pays du monde? En outre, particulièrement complexes, nouvelles et stimulantes sont les situations criminelles impliquant des interactions Avatar-Avatar ou des actions de robots. Quoi qu'il en soit, de nombreux pays comme la Belgique, le Luxembourg, la Croatie, le Danemark, les Pays-Bas, la Suède et les Etats-Unis incriminent la pédopornographie virtuelle. D'autres types de violence virtuelle ne sont pas si souvent considérés comme des crimes. Par exemple, en Belgique et au Luxembourg la violence virtuelle n'est pas incluse. La violence ne peut exister qu'entre des personnes réelles ou contre des biens réels. Toutefois, le sabotage virtuel et le piratage virtuel sont criminalisés. Les « virtual graffiti » ne sont pas punissables. La Finlande n'a aucune disposition particulière pour les actes commis dans le monde virtuel. La diffamation et le harcèlement sexuel commis dans le monde virtuel sont reconnus comme des infractions dans certains pays comme la Suède, le Danemark, la Belgique et le Luxembourg. En Allemagne, la diffusion de matériel contenant des violences virtuelles ou fictives est criminalisée lorsque la violence est glorifiée ou minimisée, lorsque la dignité humaine est bafouée ou lorsqu'il s'agit de violences pornographiques. Pour inclure la violence virtuelle, l'objet de l'infraction a été étendu aux « êtres humanoïdes ». Le droit pénal allemand ne pénalise pas explicitement les graffiti virtuels. Quand il s'agit d'Avatars, ils ne sont pas protégés en eux-mêmes. Il doit exister un lien, par exemple dans le cas d'une insulte personnelle, avec une personne physique pour que l'infraction existe**.**

6. Les infractions de non-conformité

Les révélations récentes de Wikileaks et surtout d'Edward Snowden ont donné un aperçu de l'étendue des programmes gérés par certains gouvernements pour intercepter, enregistrer, écouter, stocker et analyser les communications personnelles et professionnelles des citoyens et des étrangers, mais aussi du niveau élevé de coopération entre les prestataires de services Internet (ISP), les forces de l'ordre et les agences de renseignement dans de nombreuses régions du monde. Certains fournisseurs de services logiciels et d'Internet (ISP) auraient même collaboré volontairement pour aider les organismes de police et d'espionnage à contourner leurs propres systèmes de cryptage, tout en affirmant qu'ils respectent et protègent la vie privée de leurs clients. Il en résulte un scepticisme considérable par rapport aux promesses de la vie privée et des garanties offertes au consommateur et au citoyen. Cela entretient le sentiment que ces politiques de confidentialité ne sont que des outils de marketing sans valeur et des promesses vides qui sont facilement contournées à des fins de renseignement et de police, mais également pour un gain financier grâce à

l'exploration des données et à la vente d'informations relatives à la commercialisation et au marketing. Les soi-disant «médias sociaux » constituent, en particulier, un référentiel massif de style de vie, de shopping, de voyages, d'informations sur les dépenses personnelles qui est extrait et vendu à plusieurs grandes entreprises pour mieux cibler leurs messages commerciaux sur la clientèle. Il en est de même des programmes de fidélité des compagnies aériennes, supermarchés et magasins, cinémas, librairies et autres.

D'une façon générale, dans ce domaine, la défense nationale, la sécurité de l'Etat et l'ordre public sont présumés avoir la préséance sur la vie privée et les droits humains et civils. Tous les pays, à des degrés légèrement différents, exigent une coopération avec la police et d'autres agences d'espionnage ; la conservation des données, généralement pendant au moins 6 mois, parfois un an (Danemark) ; le blocage de communications à la demande des autorités ; et l'accès à des systèmes cybernétiques pour installer des dispositifs nécessaires pour la collecte en temps réel des données de trafic et pour la surveillance des données de contenu. Le refus peut entraîner des accusations d'outrage, l'arrestation, l'emprisonnement, des sanctions administratives ou des amendes. Les législations belge et luxembourgeoise ne pénalisent pas spécifiquement la non-coopération dans ces domaines. Toutefois, un juge peut exiger de certaines personnes la coopération et il y a des sanctions pénales en cas d'abstention. Au Japon, il existe des nombreuses infractions de non-conformité et le domaine de la cybercriminalité ne fait pas exception avec des amendes prononcées à titre de sanction. L'Allemagne exige également que les fournisseurs de services coopèrent avec les autorités et fournissent les renseignements demandés sans délai. En cas de refus, la police et les procureurs peuvent utiliser les différents outils réglementaires et coercitifs à leur disposition. Le fait de refuser les informations demandées peut constituer une infraction.

Aucune information sur cette question n'a été fournie par les rapports du Brésil, de la Turquie et de l'Argentine. La Russie n'a pas de dispositions spécifiques. Certains pays, comme la Finlande, limitent la punition pour non-conformité à des amendes. L'Italie envisage des sanctions administratives, même si le non-respect peut éventuellement devenir une infraction pénale. Aux États-Unis, des sanctions pénales sont prévues pour défaut de tenir des registres relatifs à la production du matériel sexuellement explicite. Dans la plupart des cas, les enquêteurs doivent présenter une assignation judiciaire. Le refus peut conduire à un outrage civil, à l'arrestation, à l'emprisonnement et des amendes. Un sujet de préoccupation croissante est l'obligation de déclarer la cybercriminalité connue. Selon le rapport polonais, les personnes qui ont des informations sur de la cybercriminalité punissable doivent aviser les autorités. Il existe en effet des pénalités en cas de non-déclaration. En général, les autres rapports nationaux n'abordent pas cette question, qui est cependant inévitable et qui devra finalement être étudiée.

Conclusion

Le droit pénal peut et doit jouer un rôle crucial dans la lutte contre le développement rapide, en constante évolution, des phénomènes liés au cyberespace, aux médias sociaux et aux communications électroniques à travers le monde.

À cet égard, il est essentiel de soulever ici la question des droits de l'homme, de la liberté d'expression, de l'expression artistique, de la domination culturelle du monde développé, des intérêts financiers dans le contrôle de la création, du marketing, de l'accès et de l'utilisation de l'information, de l'autoritarisme ou de ses vestiges qui permettent de limiter la liberté de communication, d'expression et le partage de l'information sous la menace de poursuites pour diffamation de fonctionnaires publics, le manque de respect pour les institutions de l'Etat , les forces armées, la police , etc.

Il est également important de tenir compte des différentes traditions juridiques quand il s'agit de la liberté d'expression ; des limites dans la manifestation de son opinion et de ses valeurs avant de déclencher des sanctions pénales ; l'utilisation de la censure pour museler les critiques et étouffer l'innovation; l'angle du profit qui peut motiver des puissants conglomérats privés de divertissement, de la musique, du théâtre, du cinéma, et des arts créatifs pour éradiquer l'expression artistique novatrice qui peut couper dans leurs profits ou contester leur domination culturelle, linguistique et artistique au niveau national ou mondial.

Il est clair que l'intervention du droit pénal peut aussi bien être positive, lorsqu'il s'agit de protéger des intérêts précieux et légitimes, que négative, quand elle appuie des régimes autoritaires et des valeurs ou pratiques culturelles et religieuses qui sont étouffantes et oppressantes.

Invoquer les «droits de l'homme» ne suffit pas à justifier des sanctions pénales ou la censure et les restrictions sur les expressions personnelles, politiques et artistiques. Ainsi, l'appel à la criminalisation doit être soigneusement réfléchi et équilibré. Au début l'Internet a été présenté comme le véritable marché libre des idées et des communications. Depuis lors, il y a eu un effort concerté de la part de régimes autoritaires et même démocratiques pour limiter, contrôler, exploiter, imposer le silence et punir certains documents et informations qui sont publiés et diffusés sur l'Internet. Il nous incombe d'évaluer les demandes assez contrastées prudemment, équitablement et clairement et de proposer des solutions et des approches équilibrées qui prennent en compte la diversité ainsi que les différences culturelles et religieuses, et qui sont infusées avec une dose judicieuse de défiance à toujours regarder le droit pénal et l'Etat comme l'unique solution à tous les problèmes.