Sous la direction de
Francis Fortin

Cybercriminalité

Entre inconduite et crime organisé

PRESSES
INTERNATIONALES
POLYTECHNIQUE

Cybercriminalité – Entre inconduite et crime organisé
Francis Fortin (Sous la direction de)

Cet ouvrage a été réalisé à l'initiative de la Sûreté du Québec

Coordination éditoriale : Luce Venne-Forcione,
Révision et correction d'épreuves : Nicole Blanchette
Mise en pages : Danielle Motard
Couverture : Cyclone Design

Pour connaître nos distributeurs et nos points de vente, veuillez consulter notre site Web à l'adresse suivante : www.pressespoly.ca

Courriel des Presses internationales Polytechnique : pip@polymtl.ca

Nous reconnaissons l'aide financière du gouvernement du Canada par l'entremise du Fonds du livre du Canada pour nos activités d'édition.

Gouvernement du Québec – Programme de crédit d'impôt pour l'édition de livres – Gestion SODEC.

Dépôt légal : 1er trimestre 2013
Bibliothèque et Archives nationales du Québec
Bibliothèque et Archives Canada

ISBN 978-2-553-01647-9
Imprimé au Canada

Chapitre

1

Problèmes relatifs à la définition et à la mesure de la cybercriminalité

Pierre-Éric Lavoie[1]
Francis Fortin[2]
Sarah Tanguay[3]

La cybercriminalité reste un concept mal défini, une sorte de « puzzle formé de pièces hétéroclites produisant une image distordue dans laquelle il est de plus en plus difficile de différencier la réalité de la fiction » (Leman-Langlois, 2006). Le terme « cybercriminalité », en se taillant une place dans le langage et l'imaginaire collectif, s'est transposé en une réalité culturellement et analytiquement floue, alimentée par diverses sources de qualité variable telles que les médias journalistiques, les experts en informatique, les représentations cinématographiques et romanesques, et le vécu et les ouï-dire de la masse citoyenne. Ce terme forme alors, par sa nature imprécise et impropre, une faible base pour la recherche, la collecte de données et l'intervention. En fait, cette lacune à l'égard de la clarté définitionnelle représente un problème de premier

1. Candidat à la maîtrise, École de criminologie de l'Université de Montréal.
2. Chercheur associé, Centre international de criminologie comparée, et candidat au doctorat, École de criminologie de l'Université de Montréal.
3. Ministère de la Sécurité publique.

plan, car elle impacte toutes les facettes de la prévention et de la régulation de la cybercriminalité (Ford et Gordon, 2006).

1.1 Motivations derrière l'emploi du terme « cybercrime »

Avant même d'aborder ce que représente le concept de la cybercriminalité, il importe de se questionner *a priori* sur les raisons derrière la nécessité du terme. L'existence du terme n'est pas consécutive aux caprices passagers d'une civilisation néophyte à l'égard de l'emploi d'une nouvelle technologie. Si tel était le cas, le lexique criminel français contiendrait des expressions telles que « criminalité des transports motorisés » ou « criminalité téléphonique ». Un vol demeure un vol, qu'il soit réalisé à l'aide d'un véhicule ou non, et l'intimidation reste de l'intimidation, qu'elle soit faite de vive voix ou par téléphonie. Toutefois, des actions similaires placées dans le contexte du cyberespace donnent naissance à de nouveaux termes, à l'exemple du « *cybertheft*[4] » ou de la « cyberintimidation ». Pourquoi existe-t-il ce besoin d'employer le préfixe « cyber », ou, au minimum, d'afficher au premier plan la présence d'une composante informatique lorsqu'un crime est commis dans le cyberespace? Sous l'étiquette de la cybercriminalité se retrouvent plusieurs actes différents qui forment à première vue un tout hétéroclite. Outre la dimension informatique, la cyberintimidation et la création de logiciels malveillants ont très peu de choses en commun lorsqu'on considère uniquement l'acte. Toutefois, en toile de fond, il est possible de noter quelques éléments qui justifient l'unification de comportements déviants, de prime abord différents, sous la bannière de la cybercriminalité.

1.1.1 Besoin d'une « cyberexpertise »

La cybercriminalité se démarque de la criminalité de type « traditionnel » par l'introduction d'un élément virtuel dans la scène de crime. À la partie matérielle du crime s'ajoute une composante immatérielle

4. Terme anglais n'ayant, pour le moment, aucune correspondance française et qui désigne, dans la plupart des cas, le vol de données personnelles ou financières à l'aide d'un réseau informatique.

qui vient complexifier la nature de l'acte. Ainsi, les repères physiques traditionnels se fondent avec des preuves numériques, intangibles et hautement techniques. Cela dit, cette configuration force le mariage entre les connaissances issues des techniques traditionnelles du métier de policier et les compétences constitutives du domaine informatique. Or, l'union de ces deux expertises n'est pas à la portée de tous les corps policiers; des compétences particulières, qui ne se retrouvent pas dans la culture policière traditionnelle, nécessitent le travail d'unités spécialisées, de « policiers de l'autoroute informatique », dont le personnel comble l'un et l'autre des domaines de connaissances. Le jumelage de la criminalité et de l'informatique instaure, en effet, une nouvelle configuration de la scène de crime qui amène plusieurs défis d'adaptation pour les forces de l'ordre. Évidemment se dresse d'abord l'obstacle de la connaissance. Tout dépendamment de ses objectifs et de ses effectifs, une unité spécialisée dans la lutte contre la cybercriminalité devra se doter de connaissances dans trois domaines particuliers :

1. Le champ informatique : Ceci inclut le savoir technique sur les différents matériels informatiques (*hardware*), la maîtrise de plusieurs logiciels et la possession de compétences en programmation.
2. Le domaine de la réseautique : Ici, les connaissances spécialisées incorporent le fonctionnement des réseaux, des différentes méthodes d'intrusion et d'attaque, des systèmes de sécurité informatique et de la détection d'intrusion.
3. La sphère juridique : L'équipe devra posséder un bagage d'acquis sur les lois nationales, mais aussi internationales, relatives à la cybercriminalité et sur les bonnes pratiques en matière d'enquête et de collecte de preuves.

Ces connaissances aboutissent subséquemment à différents savoir-faire qui se traduisent en actions permettant de prévenir, de restreindre et de sanctionner la cybercriminalité. Dans ce sens, une équipe anticybercriminalité est appelée à réaliser plusieurs activités uniques à son champ d'action dont, entre autres, le pistage des traces laissées par le cybercriminel sur les réseaux, l'identification d'une personne qui se cache derrière un pseudonyme numérique, le décryptage de données sensibles ou compromettantes et la collecte et la préservation de preuves numériques. La lutte contre la cybercriminalité requiert donc un bagage de connaissances différent de celui qui sert à combattre la criminalité

traditionnelle, nécessitant une approche professionnelle distincte et concentrée sur l'aspect informatique. Sous cet angle, il n'est pas surprenant qu'une unité anticybercriminalité doive traiter de crimes de natures différentes, dont l'unique lien est la composante informatique, ce qui justifie en partie la réunion de différentes déviances électroniques hétérogènes en une seule catégorie unificatrice.

1.1.2 Criminalité internationale

Comme l'avance Wall (2007a), le crime est une notion définie nationalement. Les lois qui président à la cybercriminalité sont restreintes à un territoire et, conséquemment, ne s'appliquent que dans le pays où elles sont adoptées (Brenner et Schwerha, 2004). Cependant, les réseaux virtuels effacent la frontière physique qui sépare le délinquant et la victime, attribuant à la cybercriminalité une réalité qui dépasse les frontières juridiques et politiques. Ainsi, dans la fusion de la criminalité et d'Internet se sont accrues les situations où l'accusé et la victime existent au sein de deux régions juridiques différentes. Cette situation entraîne d'évidentes problématiques pour les systèmes judiciaires du globe dont les uniques maîtres sont les États souverains qui les gouvernent.

Conséquemment, les nations doivent miser sur la coopération internationale si elles désirent faire reculer la cybercriminalité. Mais exécuter avec succès une démarche de coopération transfrontalière s'avère plus complexe que d'exprimer le simple désir de faire front commun devant les crimes informatiques. Divers obstacles nuisent à la collaboration pleine et entière entre les nations. En premier lieu, on retrouve les tensions politiques et diplomatiques qui existent entre différents pays et qui minent toutes volontés coopératives. Pourtant, même lorsque le climat politique et diplomatique est bon, il reste toujours plusieurs embûches telles que la langue, les coûts, la distance et les fuseaux horaires. Néanmoins, les problèmes les plus saillants proviennent des incompatibilités juridiques. En effet, les lois construites par une nation sont le reflet de sa constitutionnalité, de ses politiques, de sa morale et de ses valeurs, de ses principes religieux, de sa culture. *Ipso facto*, des pays condamnent certains actes comme des crimes alors que d'autres ne les jugent aucunement. Surviennent alors des situations où un individu commet une action parfaitement légale à l'intérieur de son pays, mais contrevient ce faisant aux lois d'un pays qui est hôte de l'acte (Marion, 2010). Or, il

n'est guère concevable qu'un pays puisse contraindre un de ses propres citoyens à se soumettre aux lois d'un autre pays. Dans le cas contraire, certaines valeurs, telle la liberté d'expression, seraient alors anéanties sous le joug de la nation la plus restrictive au point de vue des droits du cybercitoyen. Cette problématique s'est présentée lorsque le virus « I Love You » a infecté une grande partie du Web en 2000. Les créateurs du virus, des citoyens philippins, n'ont fait l'objet d'aucune sanction, bien qu'ils aient enfreint les lois de plusieurs régions juridiques du globe, puisque la zone juridique à laquelle ils étaient soumis ne disposait pas, à l'époque, de lois interdisant la création de virus informatiques (Marion, 2010). Il se dessine toutefois une tendance. De plus en plus de suspects sont extradés aux États-Unis pour y subir leur procès. Cette pratique a même fait l'objet de critiques de la part des autorités russes. Le ministre des Affaires étrangères a affirmé, à la suite de l'affaire Vladimir Zdorovenin, suspecté d'avoir commis plusieurs cybercrimes, que « malheureusement, ce n'est pas la première fois que les services spéciaux américains organisent la détention de nos ressortissants dans les pays tiers, souvent pour des raisons douteuses et par des méthodes provocatrices » (IANS, 2012). Cette pratique est tout aussi marginale que contestée.

Certains pays, par manque d'effectifs, par absence de moyens financiers, par déficience des lois ou pour toute autre raison, n'ont tout simplement pas la capacité de lutter contre la cybercriminalité sur leur territoire. Ces lieux deviennent conséquemment des havres de sécurité pour les cybercriminels, leur offrant la possibilité de lancer des attaques informatiques contre d'autres régions juridiques sans que ces dernières puissent légalement riposter. Succinctement, le caractère international de la cybercriminalité présente plusieurs obstacles à la contre-attaque légale et réduit conséquemment l'efficacité des instances judiciaires et policières. Le fait que ces organismes existent dans un système focalisé naturellement sur la sécurité intérieure diminue les réflexes coopératifs et contraint les États à des efforts supplémentaires lorsqu'il est question de criminalité informatique.

1.1.3 Configuration différente de l'action de sécurité

Les enquêtes collaboratives internationales, dans la mesure même où elles sont possibles, sont coûteuses en temps, en argent et en efforts. Ainsi, seuls les actes particulièrement graves mériteront un tel traitement.

Les réseaux internationaux de pornographie juvénile, les sites qui distribuent massivement des œuvres protégées par le droit d'auteur et les fraudes à grande échelle représentent des situations qui motivent une opération transnationale. Toutefois, un segment important de la cybercriminalité est constitué de crimes de faible gravité, provenant de l'étranger, dont les conséquences sont mineures pour la victime. Des fraudes de quelques centaines de dollars, des virus qui engendrent des pertes de temps et d'argent, des pirates qui prennent possession du compte d'un utilisateur : de tels actes sont désagréables pour la victime, mais ne causent pas, en apparence, de dommages à long terme.

Nonobstant, la cybercriminalité de faible gravité est très fréquente. Presque tout internaute peut affirmer avoir déjà été victime d'un tel crime ou, du moins, connaître quelqu'un qui en a été affecté. Par ailleurs, la faible gravité de ces crimes n'est pas en mesure de justifier les coûts engendrés par une enquête internationale et les malfaiteurs demeurent impunis. Se constitue ainsi une situation où se maintient une vague de crimes irritants, dont les impacts individuels sont négligeables, mais qui représentent toutefois des dommages importants à l'échelle de la société, contre lesquels les organismes officiels de la lutte contre la criminalité peuvent difficilement protéger la population. Conséquemment, cet aspect de la cybercriminalité requiert que les systèmes informatiques et les données de l'utilisateur soient protégés des menaces du cyberespace, mais aussi que l'utilisateur soit conscient du concept des vulnérabilités informatiques (Ford et Gordon, 2006).

Pour combler l'inefficacité de la justice et des forces de l'ordre à contrer certains aspects de la cybercriminalité, une reconfiguration partielle de l'action de sécurité s'est opérée machinalement. Sans être le résultat d'une action sociale planifiée, cette reconfiguration a pour origine la préservation des intérêts du secteur privé et la solidarité émanant des communautés virtuelles. Cette action de sécurité improvisée est axée particulièrement sur une stratégie défensive, misant sur la prévention et la fortification des dispositifs de sécurité afin que le cybercriminel ne parvienne pas à actualiser ses intentions nuisibles. L'action communautaire relève principalement de l'éducation préventive. Des utilisateurs qui se communiquent entre eux les pièges à éviter, des blogueurs qui décrivent les schèmes déployés par les fraudeurs, des internautes qui signalent les liens dangereux : tous contribuent à sensibiliser les internautes aux dangers du Web et à rendre la navigation plus sécuritaire.

D'un autre côté, la loi du marché et les présages de profits stimulent les intérêts privés à sécuriser le réseau mondial. Entretenir la confiance des utilisateurs et fournir un sentiment de sécurité est crucial pour obtenir la clientèle des internautes. Ainsi, les commerçants en ligne auraient de la difficulté à trouver preneurs s'ils ne pouvaient garantir des paiements sécuritaires. Les concepteurs de logiciels d'exploitation ne pourraient préserver la viabilité de leurs produits s'ils ne fournissaient pas des mises à jour permettant d'éliminer les failles détectées. Les sites d'échanges sociaux auraient du mal à conserver leur communauté s'ils s'avéraient incapables de modérer les comportements déviants de certains utilisateurs. La sécurisation d'Internet peut elle-même être lucrative en soi, comme peuvent l'attester les concepteurs d'antivirus et les consultants en sécurité informatique. Dans ces conditions, les instances officielles du contrôle de la criminalité voient leur rôle réduit dans le paysage global de la cybersécurité. Malgré leur efficacité en matière de criminalité de haut niveau, l'inadaptation de la police et des tribunaux à la petite criminalité informatique fait en sorte que, devant celle-ci, l'entreprise privée et l'action communautaire forment la principale ligne de défense.

La cohésion qui motive l'emploi de l'expression « cybercriminalité » ne provient donc pas de la nature des actes qui la composent, mais plutôt des problématiques que la régulation de ces différents actes engendre. Il devient ainsi plus pragmatique de combiner des crimes contre la personne, des fraudes, des vols, des crimes sexuels sous une étiquette unificatrice qui mettra en valeur la composante informatique et permettra une action concentrée et organisée. « Cybercriminalité » est conséquemment un terme artificiel, créé dans une vision purement utilitariste et faisant fi des classifications naturelles de la criminalité. C'est d'ailleurs en lien avec cet aspect artificiel que naissent les différends relatifs à la définition du terme. En effet, de nature, l'acte criminel se classifie selon le geste commis. Par exemple, le fait de s'approprier un objet ou de l'argent appartenant à autrui est un vol. Dans le cadre de la cybercriminalité, le geste posé devient secondaire à la relation qu'il entretient avec les technologies informatisées. Dans l'exemple précédent, le vol n'est plus aussi important que sa relation avec l'informatique. Cette relation donne toutefois lieu à diverses interprétations. Est-ce que le vol d'un ordinateur représente un acte de cybercriminalité? Un vol réalisé à l'aide d'informations obtenues par voie informatisée constitue-t-il de la criminalité informatique? Ainsi, depuis l'apparition du terme il y a

quelques décennies, de nombreuses interprétations de la relation entre « crime » et « informatique » ont été mises de l'avant et débattues.

1.2 Définition de la cybercriminalité : l'absence de consensus accepté et les différentes approches définitionnelles

Bien que l'usage du terme « cybercriminalité » soit présent dans le langage populaire et professionnel, la portée du terme demeure nébuleuse. Le problème en est d'abord un de contenant. Quel rôle doit jouer l'ordinateur dans la concrétisation du crime pour que l'acte devienne un cybercrime? Toute refonte de la notion du contenant influencera à son tour la définition du contenu. Ainsi, si seuls les actes commis par un moyen informatique contre un système ou un réseau informatisé sont considérés comme de la cybercriminalité, le contenu sera limité à la piraterie, à la création de logiciels malveillants, aux attaques DDOS (Déni de service distribué, de *Distributed Denial-of-Service*) et à toute autre criminalité numérique portant atteinte à l'intégrité des données informatiques. Le manque de consensus quant au contenant et au contenu de la cybercriminalité entraîne des problèmes pour l'intervention locale et internationale. C'est ainsi que les Nations unies ont déclaré en 1999 que les problèmes entourant la coopération internationale, lorsqu'il est question de criminalité informatique, résultent en partie du manque de consensus quant aux différents types d'actes qui doivent être inclus au sein du groupe et des lacunes d'une entente globale sur la définition légale de la cybercriminalité (Alkaabi, Mohay, McCullagh et Chantler, 2011).

Plusieurs tentatives ont été effectuées afin d'offrir une définition et une classification de la cybercriminalité qui soient plus appropriées pour un usage théorique et pratique (Carter, 1995; Brenner, 2004; Leman-Langlois, 2006), mais une définition consensuellement acceptée reste hors de portée. Cette confusion s'étend également en matière de sécurité intérieure, alors que les différents services policiers ne possèdent pas de définition officielle unanimement reconnue. Au Canada, un rapport de Statistique Canada (2002) révèle que la plupart des services de police canadiens ne disposent pas d'une définition officielle de la cybercriminalité ou alors utilisent une définition propre à leur service.

Un des éléments renforçant le flou relatif à la définition est la tendance à désigner, sous une même expression, tous les équipements – de nature matérielle, logicielle ou micrologicielle (*firmware*) – permettant l'acquisition automatique, le stockage, la manipulation, le contrôle, l'affichage, la transmission ou la réception de données (Ferry et Neveu, 2005). Comme le souligne Tanguay (2009), cette forme d'imprécision est également présente du point de vue juridique, ainsi que le témoigne le droit français. En effet, le concept d'« atteintes aux systèmes de traitement informatisé de données » (Ferry et Neveu, 2005) a reçu une interprétation jurisprudentielle très large et concerne autant le réseau France Télécom que le réseau Cartes bancaires, un disque dur, un radiotéléphone ou un ordinateur isolé. Avec la constante évolution et la miniaturisation des technologies, les technologies informatiques fusionnent avec les objets de la vie courante. En quelques années, les téléphones cellulaires ont évolué en de puissants mini-ordinateurs. Devant le rythme effréné des progrès technologiques, il devient alors nécessaire de correctement définir et délimiter le terme « système de traitement informatisé de données » (Tanguay, 2009).

Ceci étant, force est de constater que ce terme a été utilisé « à toutes les sauces » et sert d'étendard sous lequel se rallie un ensemble de sous-catégories variables, elles-mêmes définies de diverses façons. Historiquement, l'emploi de l'expression « cybercriminalité » faisait référence aux crimes se déroulant spécifiquement sur les réseaux, particulièrement Internet. Néanmoins, le terme a graduellement perdu ce sens pour devenir un synonyme général de la criminalité informatique (Alkaabi, Mohay, McCullagh et Chantler, 2011). Dans la pratique courante, la cybercriminalité réfère à une notion aux définitions multiples, le plus souvent déployées de manière générique, afin de désigner toute forme d'inconduite possédant, de près ou de loin, un lien avec les technologies informatiques ou réseautiques. Pour ajouter à la confusion, plusieurs autres synonymes sont employés pour décrire les crimes impliquant l'ordinateur. Ces expressions similaires sont parfois utilisées de façons interchangeables, parfois employées pour décrire un sous-ensemble particulier de crimes informatiques. Ainsi, en français, on retrouve des expressions telles que « délits informatiques », « crimes technologiques », « déviances sur Internet », « criminalité numérique », « délinquance virtuelle ». Cette situation se répète dans la langue anglaise alors que les expressions « *computer related crime* », « *computer crime* », « *Internet*

crime », « *e-crime* », « *digital crime* », « *technology crime* », « *high-tech crime* », « *online crime* », « *electronic crime* », « *computer misuse* » et « *cybercrime* » renvoient toutes à la criminalité impliquant l'ordinateur (Alkaabi, Mohay, McCullagh et Chantler, 2011).

Parallèlement, bien qu'il n'existe pas de définition législative de la cybercriminalité ou de concepts apparentés en droit canadien, la majorité des définitions adoptées par les organisations intéressées décrit la cybercriminalité ou les délits informatiques avec une vision utilitariste. À cet égard, Statistique Canada spécifie que la cybercriminalité constitue « la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale » (Statistique Canada, 2002). Ainsi, lorsque l'ordinateur est un « instrument de perpétration », il est question de crimes qui existaient avant l'arrivée de l'informatique, mais qui, depuis, ont migré vers la technologie. À cette catégorie se greffent des actes tels que la pornographie juvénile, le harcèlement et la fraude. Lorsque l'ordinateur est « objet » du crime, il est à propos de parler de « nouveaux crimes ». Ces actes se voient attribuer le qualificatif « nouveaux » puisqu'ils ne disposent d'aucun équivalent non informatique. Le piratage, la création et la dissémination de virus, les crimes virtuels et le vandalisme de pages Web ne sont possibles que dans un monde où l'informatique et Internet existent. Selon cette vision, la cybercriminalité représente à la fois l'accroissement et la sophistication de comportements déviants existants et l'émergence de nouvelles formes d'activités illégales (Rush, Smith, Kraemer-Mbula et Tang, 2009). Pour d'autres auteurs, seule la dimension « nouveaux crimes » mérite l'appellation de « cybercrimes ». Ainsi, Wall (2007a) écrit :

> Les cybercrimes sont des activités criminelles ou dommageables, de nature informationnelle, mondiale et apparentée aux réseaux, et doivent être distingués des crimes qui utilisent simplement les ordinateurs. Ils sont le produit des technologies de réseaux qui ont transformé la division des efforts criminels afin de donner naissance à des opportunités criminelles et à des formes de crimes entièrement nouvelles, qui typiquement impliquent l'acquisition ou la manipulation de l'information et ses valeurs à travers des réseaux mondiaux pour obtenir des gains. (traduction libre)

Sous un autre angle, certains penseurs ont tenté de définir la cybercriminalité en mesurant les répercussions de l'informatisation sur l'évolution

de la criminalité au cours de la dernière décennie. Cette évolution s'est traduite de deux façons : d'une part, par la facilitation de la commission de crimes préexistants et, d'autre part, par l'apparition de nouvelles infractions qui ciblent les systèmes informatiques, leurs périphériques ou les données qu'ils contiennent.

Plus précisément, certains auteurs ont adopté une vision plus globale et ont essentiellement tenté d'identifier les changements qu'Internet et, par extension, l'utilisation généralisée de la micro-informatique ont amenés dans les paramètres du crime. En prenant le Code criminel pour classifier les événements criminels reliés à Internet, Lapointe (1999) a élaboré la typologie suivante :

1. Usages problématiques : Usages d'Internet n'étant pas criminalisés, mais qui s'avèrent néanmoins problématiques pour une personne morale ou physique.
2. Crimes traditionnels : Crimes qui existaient avant l'arrivée d'Internet et que l'on retrouve encore dans nos rues.
3. Crimes innovateurs : Crimes qui n'existaient pas avant le développement de l'informatique et d'Internet et qui ne peuvent être réalisés que dans cet univers virtuel.

Il est intéressant de voir que certains usages considérés jadis comme problématiques, par exemple le leurre, ont été ajoutés au Code criminel canadien. Ce sont maintenant de nouveaux crimes avec des paramètres qui leur sont propres. L'inclusion prochaine des pourriels dans le Code criminel canadien montre que la scène cybercriminelle est encore en constante évolution et que la séparation des usages problématiques des autres catégories n'est pas absolue sur une base temporelle. Grâce aux nouvelles technologies, certains autres crimes ont connu un déplacement ou un nouvel envol, comme la pornographie juvénile. En effet, l'ordinateur facilite la prise, le stockage, l'édition et le transfert des photos, et change ainsi la donne quand vient le temps d'aborder la pornographie juvénile contemporaine. L'idée qu'Internet ait créé de nouvelles infractions est confirmée par Gautrais (2007), qui soutient ce qui suit : « La criminalité informatique regroupe deux types de conduites : celles qui ne rappellent en rien les attitudes réprimées par le droit traditionnel et les autres qui, en revanche, ne sont que de nouvelles versions des crimes qui existaient bien avant l'avènement de l'Internet. »

D'autres tentatives de définitions ont mis l'accent sur les différents rôles que peut jouer l'ordinateur dans l'activité déviante. Selon Adomi (2008), la cybercriminalité décrit l'ensemble des crimes perpétrés sur les réseaux de télécommunications, dans lesquels les ordinateurs ou les réseaux jouent le rôle d'outils, de cibles ou de scènes de crime. D'une manière plus détaillée, il est possible d'exposer au moins cinq rôles différents que peuvent interpréter les technologies informatiques dans une activité criminelle :

1. Les crimes physiques qui prennent l'ordinateur pour cible : l'acte criminel cible les composantes physiques de l'ordinateur.
2. Les crimes physiques où l'ordinateur est accessoire à l'acte : un ou plusieurs ordinateurs ont été utiles, mais pas nécessaires, pour commettre l'acte criminel.
3. Les crimes physiques où l'ordinateur est essentiel à l'acte : un ou plusieurs ordinateurs ont été requis pour réaliser l'activité déviante, laquelle n'aurait pu être accomplie sans ceux-ci.
4. Les abus informatiques : sur la scène virtuelle, utilisation d'un ordinateur dans le but de causer du tort à des individus, à des groupes ou à des organisations, d'une façon qui peut violer des procédures ou des guides de conduite, mais qui ne viole pas de lois existantes (McQuade, 2006, p. 10-16).
5. Les crimes purement informatiques : utilisation d'un ou de plusieurs ordinateurs dans le but de commettre un acte, par l'entremise d'un réseau, visant à nuire à l'intégrité d'un système informatique ou réseautique.

Au Québec, on note dans les définitions de l'Office québécois de la langue française (OQLF) les distinctions qui représentent deux axes de changement au cours des dernières décennies. D'abord, lorsque l'ordinateur est utilisé pour faciliter le crime, on préférera parler de délit informatique (OQLF, 2009) : « Acte illicite perpétré par le moyen de l'informatique, ou ayant pour cible le système informatique ou l'un de ses éléments. » Ce type de crime pouvait donc exister avant Internet. Cette définition de l'OQLF inclut quatre sous-catégories (OQLF, 2009) :

1. le vol et le sabotage du matériel tel que les claviers, imprimantes, écrans, supports, etc.;

2. la fraude informatique et le sabotage immatériel (détournement de fonds, antiprogrammes, etc.);
3. les indiscrétions et détournements d'information, lesquels sont au cœur même de l'espionnage commercial et industriel;
4. les détournements de logiciels par copie illicite.

Ensuite, on définit la cybercriminalité comme la « criminalité informatique associée au cyberespace, qui recouvre l'ensemble des infractions pénales pouvant être commises au moyen du réseau Internet » (OQLF, 2009). Cette définition a reçu le soutien de plusieurs chercheurs, particulièrement dans les réseaux informatiques.

L'objectif de ce chapitre se limitant à présenter les différents angles définitionnels de la cybercriminalité, il serait fallacieux d'affirmer qu'une approche est supérieure à une autre. En effet, ce livre serait le premier à transgresser les limites conceptuelles de l'une ou l'autre de ces définitions. La teneur plutôt pragmatique de ce livre implique une vision élargie du phénomène. Les auteurs ont choisi la voie de l'étude des problématiques pouvant être rencontrées par les personnes œuvrant dans le domaine de l'application de la loi. Cette analyse stratégique se décline en chapitres sur l'ordinateur en tant qu'outil et cible, mais aussi en chapitres traitant d'usages problématiques d'Internet, d'anciens crimes à la sauce technologique et de « nouveaux crimes » n'existant pas avant l'avènement de la micro-informatique et d'Internet.

1.3 Difficultés relatives à la mesure de la cybercriminalité

Le flou définitionnel entourant la notion de cybercrime entraîne plusieurs problèmes quant à la collaboration et à l'élaboration de plans d'action. Sans un langage commun, il est difficile de parvenir à diriger l'action vers les bonnes cibles. Sans consensus sur la définition, il devient ardu d'obtenir des statistiques universelles sur le phénomène et de produire ainsi une image claire de la déviance sur Internet. Mais les ennuis définitionnels ne sont pas l'unique raison de la complexité à jauger le phénomène cybercriminel. Plusieurs autres traits de la criminalité informatique nuisent à la mesure de cette déviance. Or, sans une bonne mesure, les actions entreprises à l'encontre de la cybercriminalité seront

accomplies à tâtons et seront fortement soumises aux perceptions et aux pressions sociales au lieu de s'appuyer sur une logique découlant de faits observés. Les paragraphes qui suivent présentent brièvement quelques causes de ces freins à la mesure efficiente de la criminalité informatique.

1.3.1 Faible taux de crimes informatiques rapportés à la police

Il est admis qu'une part importante de la criminalité connue de la police provient des dénonciations faites par les citoyens. Or, pour qu'un crime soit rapporté ou dénoncé, il faut que quelqu'un, quelque part, en ait conscience. En prenant place en partie dans un univers immatériel, la criminalité informatique élimine dans la plupart des cas la présence de témoins. Ainsi, la victime est souvent l'unique personne pouvant dénoncer le crime. Toutefois, diverses situations font en sorte que la victime optera, consciemment ou inconsciemment, pour ne pas rapporter le crime à la police. D'abord, la victime n'est pas toujours consciente du geste criminel commis à son égard. Certains cybercrimes sont en effet de nature furtive et se réalisent à l'insu des personnes touchées. Le vol de données personnelles, par exemple, est rarement détecté au moment de l'acte, puisque le « vol » ne prive pas le propriétaire légitime de son bien; le voleur s'enfuit avec une copie numérique des renseignements. Cette situation est particulièrement vraie pour les entreprises, où le nombre imposant de données emmagasinées, la complexité du réseau interne et le va-et-vient des employés sur les systèmes rendent difficile la détection des intrusions informatiques. Similairement, les logiciels espions et certains virus parviennent à s'infiltrer discrètement dans le système et échappent à l'attention de la victime.

Dans d'autres cas, il se peut que la victime ne reconnaisse pas le caractère criminel du geste posé à son égard. Par exemple, une personne recevant des menaces en ligne peut décider que les actions de l'autre partie ne sont pas suffisamment sérieuses pour retenir l'attention de la police. Pareillement, pour certains, les dommages causés par un virus informatique ou autres victimisations mineures peuvent être assimilés à « l'expérience » de la navigation en ligne, soit un phénomène banal qui est fréquent sur Internet et qui relève principalement du hasard, d'une simple malchance. Dans certains cas, la victimisation peut même être débattue, comme c'est le cas de l'exposition non sollicitée à de la

pornographie. Le silence de la victime peut aussi être le fruit d'une attitude défaitiste alors que celle-ci se dit que la police ne pourra rien faire pour l'aider. La personne victimisée n'aura alors pas d'incitatif à rapporter le crime. Finalement, certaines victimes, particulièrement celles qui ont fait l'objet d'une supercherie, peuvent avoir honte d'être tombées dans un piège tendu par autrui. Les fraudes nigérianes sont des exemples de cas où les victimes peuvent hésiter à révéler leur victimisation de peur de subir un jugement négatif de la part des autres. Ainsi, pour diverses raisons, les victimes de criminalité informatique rapportent très peu leur victimisation à la police. En retour, cela affecte la capacité de la police à produire un portrait statistique du phénomène fidèle à la réalité. Il s'agit d'un autre exemple de ce que la criminologie nomme « le chiffre noir de la criminalité » et qui représente tous les crimes qui sont inconnus de la police, mais qui sont bien réels.

1.3.2 Priorités de l'entreprise privée

Dans l'univers des crimes informatiques, l'individu n'est pas le seul à faire figure de victime. L'entreprise privée détient également une part importante de la victimisation, particulièrement dans le domaine de la fraude. Tout comme les particuliers, l'entreprise privée n'est pas encline à divulguer sa victimisation à la police. En effet, un sondage réalisé par Ernst et Young (2003) sur la fraude commise contre le secteur commercial révèle que seulement un quart des affaires ont été renvoyées à la police. Pire, le taux de satisfaction relativement au travail policier chez ceux qui ont fait appel à la police ne s'élève qu'à 28 %, laissant présager que ces entreprises ne seront pas portées à répéter l'expérience.

Considérant les motivations et objectifs de l'entreprise privée, l'absence de contact avec le milieu policier est souvent délibérée. Dans le milieu des affaires, de sérieux doutes planent quant à la capacité de la police publique à effectuer des enquêtes informatiques efficaces, rapides et confidentielles. L'une des craintes premières des institutions est que l'enquête policière exposera publiquement la négligence de l'entreprise en matière de sécurité. Faire appel à la police équivaut donc souvent à risquer sa réputation, à mettre en jeu la confiance des clients et des partenaires, et à s'exposer à des pertes financières et à de graves dommages à l'image de marque. Nécessairement, une banque victime de fraude enverra l'image à ses clients qu'elle n'est pas en mesure de protéger leurs

avoirs. Une part de la clientèle risque alors de déserter ses rangs pour rejoindre une institution rivale, jugée plus compétente. Ainsi, la plupart du temps, les compagnies dont la cybervictimisation est révélée sur la place publique voient la valeur de leurs actions chuter (Kirbie, 2000). Conséquemment, cette peur des impacts négatifs provoqués par la mauvaise publicité réduit grandement la volonté du secteur commercial de mobiliser la police en cas de victimisation, lequel préfère poursuivre un modèle privé de justice, en faveur des intérêts égoïstes de l'entreprise, plutôt que de faire appel au système de justice public, agissant au service du bien collectif (Wall, 2007b).

Cette décision de traiter l'affaire à l'interne est aussi une question de rendement économique. Dans la plupart des situations, l'avenue policière ne permettra pas à l'entreprise privée de récupérer les pertes résultant de la victimisation. Pire, l'enquête publique, par sa lourdeur procédurale, diminue le rendement de l'entreprise en lui imposant des tâches et des restrictions contraires aux objectifs commerciaux. Par conséquent, faire appel à la police est un investissement en matière d'argent, de temps et d'efforts qui n'offre pratiquement aucun retour économique possible. Il s'agit d'un « mauvais investissement » (Smith, 2003), à proprement parler. Les objectifs de la police et du milieu économique sont, dans ces conditions, fondamentalement différents. Pour le milieu policier, une enquête réussie équivaut à une arrestation, à un dossier clos. Pour l'entreprise privée, un succès se définit par l'arrêt des victimisations. Aucun bénéfice ne sera retiré du blâme social du coupable. À court terme, la victimisation risque de disparaître avec l'arrestation du criminel, mais cette situation est généralement temporaire, le risque étant que le délinquant mis hors service soit remplacé, à moyen ou long terme, par d'autres individus. Corollairement, l'entreprise sera disposée à assumer la perte initiale de la victimisation et à déployer des moyens pour corriger les failles qui ont rendu l'incident possible. L'application de nouvelles mesures préventives ou l'amélioration de celles qui sont déjà en place tend donc à remplacer la signalisation de l'affaire au milieu policier.

Les statistiques criminelles jouent un rôle important dans la direction des activités policières. Elles permettent aux décideurs d'allouer les ressources limitées de la police de manière plus appropriée (Goodman, 2001). Il reste des efforts à faire pour préciser le pourtour des définitions du cybercrime, et ce, ne serait-ce que par pragmatisme. À défaut d'une définition claire et commune de la cybercriminalité et devant le faible

taux de crimes informatiques rapportés à la police, il est très difficile de produire un portrait clair de la réalité criminelle sur Internet. Le défi de rendre compte de cette situation complexe et variée avec le plus d'acuité possible est donc de taille. C'est ce que nous tenterons de faire dans les prochains chapitres.

Bibliographie

ADOMI, E. (2008). *Security and Software in Cybercafes*, Hershey, PA, Information Science Reference.

ALKAABI, A., MOHAY, G., McCULLAGH, A., et CHANTLER, N. (2011). « Dealing with the Problem of Cybercrime », dans I. Baggili (sous la direction de), *Digital Forensics and Cyber Crime*, Actes de l'Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Berlin, Springer, vol. 53, p. 1-18.

BRENNER, S., et SCHWERHA, J. (2004). « Cybercrime : A Note on International Issues », *Information Systems Frontiers*, vol. 6, nº 2, p. 111-114.

BRENNER, S. W. (2004). « U.S. Cybercrime Law : Defining Offences », *Information Systems Frontiers*, vol. 6, nº 2, p. 115-132.

CARTER, D. (1995). « Computer Crime Categories : How Techno-Criminals Operate », *FBI Law Enforcement Bulletin*, vol. 64, nº 7, p. 21.

ERNST & YOUNG FRAUD INVESTIGATION GROUP (2003). *Fraud: the Unmanaged Risk : 8th Global Survey*, Johannesburg, Global Investigations and Dispute Advisory Services.

FERRY, M., et NEVEU, M. (2005). « Les atteintes aux systèmes informatisés de données », *e-juristes.org* [En ligne] www.e-juristes.org/Les-atteintes-aux-systemes (consulté le 13 février 2009).

FORD, R., et GORDON, S. (2006). « On the definition and classification of cybercrime », *Journal in Computer Virology*, vol. 2, nº 1, p. 13-20.

GAUTRAIS, V. (2007). « Ententes de sécurité. Code criminel et utilisation d'Internet », *Chaire en droit de la sécurité et des affaires électroniques* [En ligne] www.gautrais.com/Code-criminel-et-utilisation-d (consulté le 13 mars 2011).

GOODMAN, M. (2001). « Making computer crime count », *FBI Law Enforcement Bulletin*, août [En ligne] findarticles.com/p/articles/mi_m2194/is_8_70/ai_78413303 (consulté le 14 février 2012).

IANS (2012). « Russia slams hacker's extradition to US », *IBN live*, 20 janvier [En ligne] ibnlive.in.com/news/russia-slams-hackers-extradition-to-us/222457-2.html (consulté le 14 février 2012).

KIRBIE, C. (2000). « Hunting for the Hackers : Reno Opens Probe Into Attacks That Disabled Top Web Sites », *The San Francisco Chronicle*, 10 février [En ligne] www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/02/10/MN72324.DTL (consulté le 14 février 2012).

LAPOINTE, S. (1999). *Vers l'organisation d'une cyberpolice au Canada et au Québec*, Mémoire de maîtrise, Faculté des Arts et des Sciences, École de criminologie.

LEMAN-LANGLOIS, S. (2006). « Le crime comme moyen de contrôle du cyberespace commercial », *Criminologie*, vol. 39, nº 1, p. 63-81 [En ligne] www.crime-reg.com/textes/cybercrime.pdf (consulté le 14 février 2012).

MARION, N. (2010). « The Council of Europe's Cyber Crime Treaty : An exercise in Symbolic Legislation », *International Journal of Cyber Criminology*, vol. 4, nºs 1 et 2, janvier-juillet 2010 / juillet-décembre 2010, p. 699-712 [En ligne] www.cybercrimejournal.com/marion2010ijcc.pdf (consulté le 14 février 2012).

MCQUADE, S. (2006). *Understanding and Managing Cybercrime*, Boston, MA, Allyn and Bacon.

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (2009). « Délit informatique », *Grand Dictionnaire terminologique* [En ligne] www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp (consulté le 20 février 2009).

RUSH, H., SMITH, C., KRAEMER-MBULA, E., et TANG, P. (2009). *Crime online : Cybercrime and illegal innovation*, NESTA, Rapport de recherche, juillet.

SMITH, R. (2003). « Investigating Cybercrime : barriers and solutions », *Australian Institute of Criminology*, 11 septembre.

STATISTIQUE CANADA (2002). *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, Centre canadien de la statistique juridique.

TANGUAY, S. (2009). « Définition de la cybercriminalité », dans F. Blanchard, F. Fortin, B. Gagnon et I. Ouellet (sous la direction de), *Analyse stratégique sur la cybercriminalité – 2009*, Montréal, Sûreté du Québec.

WALL, D. (2007a). *Cybercrimes : The Transformation of Crime in the Information Age*, Cambridge, Polity.

WALL, D. (2007b). « Policing Cybercrimes : Situating the Public Police in Networks of Security within Cyberspace », *Police Practice and Research*, vol. 8, nº 2, p. 183-205.