La cybercriminalité: état des lieux et perspectives d'avenir

Fernanda Prates, Frédérick Gaudreau et Benoît Dupont[1]

Publié dans : Institut Canadien d'Études Juridiques Supérieures (sous la direction de), *Droits de la personne : La circulation des idées, des personnes et des biens et capitaux*, Éditions Yvon Blais, Cowansville, 2013, pp. 415-442.

[1] Adresse de correspondance: benoit.dupont@umontreal.ca.

Introduction

Internet fait désormais partie intégrante de nos vies, tant au niveau personnel que professionnel. Une enquête menée auprès de 50.000 personnes dans 46 pays montre en effet que l'Internet est devenu le média le plus utilisé pour plus de la moitié des internautes dans le monde, 61% d'entre eux s'y rendant quotidiennement, alors qu'ils sont 54% à faire de même avec la télévision, 36% avec la radio et 32% avec les journaux papier (TNS Sofres, 2010). Selon l'Union internationale des télécommunications, en janvier 2011, 2,08 milliards d'individus utilisaient Internet sur la planète, alors qu'ils étaient seulement 1,03 milliard en 2005 (ZDNet France). Au Québec, en décembre 2011, 78,9% des adultes ont utilisé Internet au moins une fois par semaine, contre 74,4% en décembre 2010 (CEFRIO, 2011a). Le nombre toujours grandissant d'acteurs présents dans l'univers virtuel demande d'ailleurs le renforcement du modèle de gouvernance multipartite soutenu par l'ICANN[2] pour assurer ainsi que les points de vue de ces multiples acteurs (les gouvernements, la société civile, les entreprises et la communauté technique) soient pris en considération (ICANN, 2011).

Bien que l'absence d'une compilation uniforme des données canadiennes sur les cybercrimes empêche de définir de façon précise l'ampleur du phénomène, cet article a pour objectif de décrire les changements les plus significatifs survenus ces dernières années dans le domaine. Après avoir présenté quelques chiffres relatifs à l'utilisation de l'Internet au Canada et dans certains pays européens, nous verrons les difficultés liées à l'élaboration d'une définition opérationnelle de la cybercriminalité, avant d'aborder les coûts estimés de cette dernière. Une réflexion plus spécifique suivra, qui nous permettra d'analyser plus en détail la nature de certains crimes à partir des statistiques et de la législation canadienne en vigueur. Nous conclurons en tirant des constats portant sur les actions nécessaires à la prévention et à la répression efficace de la cybercriminalité.

1. L'omniprésence d'Internet

L'utilisation de l'Internet par les Canadiens est en constante progression. Selon la dernière enquête canadienne sur l'utilisation d'Internet, en 2010, 79% des ménages avaient accès au réseau Internet et presque tous les ménages (96%) disposaient d'une connexion haute vitesse (Statistique Canada, 2011a). Le Québec accompagne la tendance canadienne avec 73% des ménages ayant accès à l'Internet en 2010 (Statistique Canada, 2011a). Un rapport récent montre qu'en septembre 2011, 80,4 % des Québécois de plus de 18 ans ont utilisé Internet au cours des sept derniers jours, ce qui indique une augmentation de 5% par rapport à septembre 2010, alors que le taux d'internautes réguliers était de 75,4% (Cefrio, 2011b). Au quotidien, 60 % des internautes québécois privilégient les médias sociaux pour consulter du contenu, 44 % pour interagir avec d'autres utilisateurs et 42 % pour entretenir leur profil personnel. En ce qui concerne les caractéristiques des internautes, on observe que les adultes dont le revenu familial dépasse 60.000 $ par année figurent parmi les utilisateurs les

[2] *Internet Corporation for Assigned Names and Numbers.*

plus assidus avec un taux de connexion de 94,5%. Sur le plan professionnel, ce sont les étudiants (100 %), les professionnels (96,8 %), et les cols blancs (88,2 %) qui utilisent le plus régulièrement Internet (Cefrio, 2011b).

La progression du nombre d'utilisateurs ainsi que la fréquence d'utilisation de l'Internet semblent liées entre autres au phénomène des médias sociaux. Une étude récente indique à ce sujet que 73 % des internautes québécois utilisent des réseaux sociaux (tels que Facebook, LinkedIn, MySpace ou Twitter) en moyenne près de 6 heures par semaine (Cefrio, 2011c). On constate également que 52% des internautes québécois entretiennent un profil sur les médias sociaux, dont 20 % tous les jours et 22 % au moins une fois par semaine (Cefrio, 2011c). Les internautes de 18 à 24 ans sont les plus présents sur les médias sociaux, un peu plus de la moitié d'entre eux utilisant ces services quotidiennement et 38% d'entre eux entretenant un profil aussi tous les jours. C'est également ce groupe d'âge qui passe plus d'heures par semaine sur les réseaux sociaux, soit 8h30 alors que pour l'ensemble des utilisateurs, cette moyenne est de 6 heures par semaine. Bien qu'il existe une coupure générationnelle entre les usagers des réseaux sociaux, il semblerait que les utilisateurs plus âgés y sont de plus en plus présents. On observe à ce propos que parmi les internautes québécois, 69% réalisent au moins une activité sur les médias sociaux entre 45 à 54 ans, ce taux passant à 55% chez les 55 à 64 ans et à 39% chez les 65 ans et plus (Cefrio, 2011c).

L'augmentation de l'utilisation de l'Internet est également observée en Europe. En France par exemple, 74% des ménages avaient accès à l'Internet en 2010 (Data Publica, 2010). De plus, 92% des Français accèdent à l'Internet tous les jours : 60% d'entre eux le font pour accéder à leur messagerie de courrier électronique tandis que 13% le font pour accéder à leur réseau social (TNS-Sofres 2010). Le commerce électronique continue à se développer en France, puisque 41% de la population a eu recours à ce type de services en 2009 contre 38% en 2008, ce qui représente 22 millions de consommateurs (CREDOC, 2009). L'accroissement de l'utilisation de l'Internet mobile connaît aussi un progrès remarquable depuis quelques années. En effet, selon une étude récente, l'utilisation de l'Internet mobile a doublé en seulement un an pour atteindre 5 millions d'utilisateurs en 2009. La proportion de la population qui dispose d'un téléphone intelligent et l'utilise pour consulter Internet est de 13% en 2009. Entre 2008 et 2009, ce taux est passé en France de 12% à 19% chez les adolescents et de12% à 27% chez les 18-24 ans (CREDOC, 2009).

Cette popularité n'est pas sans risques. En effet, le cyberespace favorise la perpétration d'infractions, notamment par sa dimension internationale, sa facilité d'utilisation, la possibilité de diffuser de l'information en tout genre à une multitude de personnes à un coût quasi nul et le relatif anonymat dont les utilisateurs bénéficient (Sûreté du Québec, 2009). On observe alors qu'avec la hausse des internautes, il y a également hausse des signalements qui est constatée par les services d'application de la loi, ces derniers ayant enregistré un accroissement du nombre des plaintes reçues en cette matière. Une étude récente montre à ce sujet que 431 millions

d'adultes auraient été victimes de la cybercriminalité dans le monde en 2010[3] (Norton Cybercrime Report, 2011).

2. Les coûts estimés de la cybercriminalité

Il est difficile d'estimer les coûts de la cybercriminalité, et ce, pour plusieurs raisons. Soulignons d'abord que ce type de délits est rarement signalé aux organismes d'application de la loi. De plus, les méthodes d'évaluation des coûts directs et indirects peuvent également être variables. Certaines études calculent par exemple uniquement la mise en place de systèmes de sécurité et la réparation des dommages directs à la suite d'une attaque, tandis que d'autres recherches incluront les coûts indirects des attaques comme le manque à gagner causé par la perte de clients. Mentionnons aussi que, puisque la définition du concept de cybercriminalité n'est pas universelle et que les études dans ce domaine portent sur des juridictions différentes, les résultats de celles-ci peuvent diverger. Quoique les coûts soient difficiles à évaluer, certains s'y risquent. Ces évaluations touchent les individus, les entreprises et les gouvernements (Sûreté du Québec, 2009).

Selon le dernier rapport de l'entreprise de sécurité Norton, le coût mondial de la cybercriminalité en 2010 est estimé à 388 milliards de dollars. L'évaluation est basée sur des renseignements recueillis auprès de plus de 12.000 victimes réparties dans 121 pays et elle inclut la valeur du temps perdu à cause de la cybercriminalité (274 milliards de dollars) aussi bien que le coût de la résolution des problèmes causés aux usagers (114 milliards) (Norton Cybercrime Report, 2011). En ce qui concerne le Canada, le même rapport évalue le coût net de la criminalité à 5,6 milliards CAD. Cela regroupe la valeur du temps perdu pour les victimes (4,7 milliards $ CAD) autant que le coût direct lié à la cybercriminalité, comme l'argent volé et le coût de résolution des crimes (840 millions $ CAD)[4]. De plus, en 2009, le vol d'identité et les courriels frauduleux ont coûté aux internautes canadiens 59 millions de dollars, ce qui correspond à une hausse de 77% par rapport à l'année 2005, ce qui démontre une forte croissance annuelle des coûts associés à la cybercriminalité au cours des dernières années (Bureau de la Concurrence, 2010).

L'Europe semble suivre la même tendance. En France par exemple, on estime que la cybercriminalité aurait fait 9,4 millions de victimes en 2010, générant une perte approximative de 1.722 millions d'euros (872 millions en pertes directes et 850 millions en temps perdu à résoudre les incidents) (Norton Cybercrime Report, 2011). En Belgique, la cybercriminalité aurait fait 1,4 million de victimes, engendrant une perte de 347,5 millions d'euros en 2010, dont 160 millions seraient attribuables à la seule résolution du problème et 187,5 millions découleraient du temps perdu à

[3] Enquête réalisée auprès de 19.636 individus dans 24 pays.

[4] Remarquons que les études réalisées par les principaux acteurs du marché de la sécurité informatique doivent être prises avec précaution car celles-ci peuvent être biaisées en fonction de l'intérêt des parties (Ghernaouti-Hélie, 2010). Pour une analyse critique de la méthodologie employée par certaines recherches dans le domaine, voir Florêncio & Herley, 2012.

résoudre les incidents (Norton Cybercrime Report, 2011). Finalement, « d'un point de vue social, il existe des coûts qu'on ne peut pas quantifier. S'il est toujours possible d'estimer les pertes au niveau économique, on ne peut pas en faire autant des victimes de pornographie juvénile ou de leurre, par exemple. Ces personnes ont subi des atteintes à leur intégrité et peuvent rester stigmatisées toute leur vie » (Sûreté du Québec, 2009, p. 13).

3. Définition de la cybercriminalité

Au cours de la dernière décennie, la cybercriminalité est devenue une préoccupation majeure pour les organisations gouvernementales et du secteur privé, et elle donne lieu à une multiplication des études, que ce soit dans le domaine informatique, juridique ou criminologique. Malgré une croissance exponentielle, la courte histoire de ce phénomène fait que la notion même de la cybercriminalité demeure encore lacunaire et hétérogène. À l'heure actuelle, nous n'avons pas en effet atteint un consensus sur la signification de la cybercriminalité. Ce flou terminologique est renforcé par l'absence d'un cadre législatif uniforme définissant la cybercriminalité. Pour faire face à ce déficit, les organisations intéressées ont adopté certaines définitions pratiques pour rendre compte de cette forme particulière de délinquance.

L'Office fédéral de la police suisse par exemple comprend la cybercriminalité comme « de nouvelles formes de criminalité spécifiquement liées aux technologies modernes de l'information, et de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels » (Chawki, 2006, p. 8). En France, le Ministère de l'intérieur emploie le terme cybercriminalité pour désigner « l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet » (Ministère de l'Intérieur, 2010). Selon ce ministère, ce terme désigne à la fois les atteintes aux biens (comme la fraude bancaire et le piratage informatique) et les atteintes aux personnes (comme la pédophilie, les injures à caractère racial et les atteintes à la vie privée). Cependant, l'absence de définition légale précise n'est pas sans poser de problèmes dans ce pays. Citons par exemple que le concept d'atteintes aux systèmes de traitement informatisé de données (Code Pénal art. 323) 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 » (Sûreté du Québec,, 2009, p. 16). Le Canada fait face également à l'absence de définition légale en ce qui concerne la cybercriminalité. Face à cette lacune, les organismes canadiens d'application de la loi semblent se rallier à la définition proposée par le Collège canadien de police, laquelle décrit la cybercriminalité comme étant « la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principal » (Valiquet, 2011). Dans le même sens, depuis 2007, le Programme de déclaration uniforme de la criminalité englobe dans ses données les indicateurs de la cybercriminalité. Les cybercrimes sont alors classés en deux catégories, à savoir, celle où l'ordinateur est l'objet de l'infraction (comme le piratage ou l'utilisation illicite de systèmes informatiques) et celle où l'ordinateur constitue l'instrument principal de perpétration de l'infraction (comme la distribution ou la vente de pornographie infantile sur Internet et la fraude de vol d'identité perpétrée via Internet) (Ministère de la Sécurité Publique, 2007). Il serait intéressant

vérifier tout de même l'ampleur effective de cette tendance à l'uniformisation parmi les corps policiers canadiens. Une recherche menée en 2002 a ainsi mis en lumière l'absence de consensus au sein des organisations policières à ce sujet (Statistique Canada, 2002). Au Québec, en suivant la définition proposée par l'Office de la langue française, on parlera de délit informatique lorsque l'ordinateur est utilisé pour faciliter l'infraction, tandis que la cybercriminalité est définie comme la « criminalité informatique associée au cyberespace, qui recouvre l'ensemble des infractions pénales pouvant être commises au moyen du réseau Internet » (Office québécois de la langue française, 2009).

Malgré certaines spécificités, on peut dégager certains points communs des définitions citées précédemment. On retient à cet effet que la majorité des définitions adoptées par les organisations intéressées décrit la cybercriminalité selon une perspective utilitariste. Ainsi, les cybercrimes seraient divisés en deux grandes catégories. La première, constituée par les délits assistés par ordinateur, englobe les cas où l'ordinateur est l'instrument même de la perpétration du délit. Dans ces affaires, les organismes d'application de la loi seraient confrontés à des délits qui existaient préalablement à l'avènement de l'informatique, comme la pornographie juvénile, la fraude ou le harcèlement. La deuxième catégorie, composée des délits informatiques « purs », englobe les infractions où l'ordinateur constitue l'objet du crime. Il s'agit alors d'une criminalité nouvelle, liée surtout aux réseaux informatiques et notamment à l'Internet. Citons par exemple le piratage informatique et la propagation malveillante de virus informatiques (Statistique Canada, 2002 ; Sûreté du Québec, 2009; Valiquet, 2011).

Par ailleurs, certains auteurs ont essayé de définir la cybercriminalité à partir de son évolution au cours de la dernière décennie, en identifiant notamment les changements apportés par l'Internet. À partir de ce modèle, Lapointe (2000) a élaboré la typtologie suivante: « 1) Usages problématiques : usages d'Internet n'étant pas criminalisés, mais qui s'avèrent problématiques pour une personne morale ou physique; 2) Crimes traditionnels : infractions qui existaient déjà avant l'arrivée d'Internet; 3) Crimes innovateurs : infractions qui n'existaient pas avant le développement de l'informatique et d'Internet et qui ne peuvent être réalisés que dans cet univers virtuel » (*in* Sûreté du Québec, 2009, p.18). Dans ce chapitre, on considèrera l'ordinateur aussi bien comme un outil que comme une cible, mais nous discuterons aussi des usages problématiques d'Internet, d'anciens crimes ayant évolué pour s'adapter à la technologie, et de « nouveaux crimes » n'existant pas avant l'avènement de la micro-informatique et de l'Internet (Sûreté du Québec, 2009).

4. Crimes contre l'intégrité de la personne

4.1. Pornographie juvénile

Depuis le milieu des années 1990, le développement du cyberspace a profondément modifié le visage de la pornographie juvénile. En 2008, 420 infractions de pornographie juvénile ont été enregistrées au Québec, tandis qu'en 2007 ce nombre a été de 255, ce qui équivaut à une augmentation de 65 % dans un intervalle d'un an.

Cette croissance pourrait s'expliquer par une plus grande accessibilité au matériel pornographique, mais aussi par l'intensification de la répression policière envers cette forme de criminalité. En 2008, la police a enregistré 191 infractions de distribution de pornographie juvénile, 189 infractions de possession de pornographie juvénile, 30 infractions de production de pornographie juvénile et 10 infractions de pornographie juvénile dont la nature n'a pas été précisée (Sécurité Publique, 2010). Soulignons que parmi les délits cités, les infractions de possession de pornographie juvénile ont connu la plus forte augmentation en 2008 (117 %), avec 102 infractions de plus qu'en 2007. Les délits de production et de distribution de pornographie juvénile ont connu pour leur part une hausse non négligeable de 36 % et 47 % respectivement (Sécurité Publique, 2010).

La pornographie juvénile est définie à l'article 163.1 du Code criminel comme étant la production, la promotion, la distribution et la possession de pornographie juvénile, ainsi que l'accès à cette pornographie. En 2005, certaines précisions ont été apportées à la législation canadienne par l'entremise de la Loi C-2[5]. En plus d'ajouter des peines minimales à la pornographie juvénile, cette loi a élargi la définition de la pornographie juvénile, en y ajoutant les enregistrements sonores et écrits. La loi a également interdit la promotion et la publicité de la pornographie juvénile (Sûreté du Québec, 2009). Finalement, depuis mars 2011, la loi C-22 impose aux fournisseurs d'accès à Internet l'obligation de rapporter tout incident concernant la pornographie juvénile (Valiquet, 2011).

4.2. Leurre

Certaines recherches ont déjà observé que les jeunes Canadiens adoptent des conduites pouvant augmenter leurs risques de devenir victimes d'exploitation sexuelle en ligne (Juristat, 2009). Les prédateurs, quant à eux, exploitent cette « aisance avec laquelle ils peuvent entrer en contact avec les jeunes» (Sûreté du Québec, 2009, p.62). Dans ce contexte, il n'est pas surprenant qu'on observe depuis les dernières années un accroissement du nombre de cas déclarés de leurre au Canada, phénomène qui semble lié également à l'amplification des efforts policiers dans la matière. L'Enquête sociale générale sur la victimisation menée en 2009 auprès des 19.422 ménages canadiens a démontré que 2% des répondants ont déclaré qu'au moins un de leurs enfants avait été leurré ou avait reçu des avances sexuelles sur Internet. Au Québec, on constate une augmentation significative du nombre de cas signalés aux autorités policières depuis les dernières années. En 2002, deux cas ont été signalés à la police alors qu'en 2009, ce chiffre est passé à 135 affaires signalées, surpassant ainsi les cas d'inceste (97 plaintes), de voyeurisme (82 plaintes) et d'agression sexuelle armée (56 plaintes) survenus dans cette même année (Sécurité Publique Québec, 2011).

En ce qui concerne le cadre législatif régissant l'infraction de leurre, en 2002 le Code criminel canadien a été modifié pour inclure, entre autres, l'interdiction à tout adulte de communiquer au moyen d'un ordinateur avec une personne mineure dans le but

[5] Projet de loi C-2 sur la protection des enfants et d'autres personnes vulnérables (Ministère de la Justice, 2005).

d'avoir des rapports sexuels. En 2008, les peines maximales imposables à cette infraction ont été revues à la hausse. Présentement le quantum de cette peine est de 10 ans, le double de ce qu'avait prévu le législateur en 2002, (Juristat, 2009).

4.3. La cyberintimidation

La cyberintimidation constitue « un acte d'intimidation impliquant l'utilisation de nouvelles technologies, afin de porter préjudice ou d'intimider autrui » (Bureau d'intervention en matière de harcèlement sexuel, 2009*)*. Le développement du réseau Internet a non seulement accru les moyens d'intimidation, mais il a aussi aggravé les impacts de cette activité sur les victimes. Au Canada, selon l'Enquête sociale générale de 2009 sur la victimisation, 7% des internautes adultes ont été victimes de cyberintimidation à un moment ou à un autre de leur vie. En Belgique, une étude réalisée en 2008 auprès de jeunes internautes (12-18 ans) de la communauté francophone révèle que six jeunes sur dix (66,7%) ont été la cible de harcèlement par Internet tandis que quatre jeunes sur dix (41,2 %) admettent s'être déjà rendus coupables d'une ou de plusieurs formes de cyberharcèlement (Walrave *et al.,* 2009*)*. En ce qui concerne le Québec, un sondage réalisé en 2007 auprès de 2.474 jeunes étudiants montre que 70% des répondants ont été victimes de cyberintimidation, parmi lesquels 76% disent avoir été injuriés et 38% affirment avoir été menacés en ligne (Jeunesse J'écoute, 2007). En revanche, une recherche réalisée par l'un d'entre nous auprès de 1.100 internautes montre que la cyberintimidation n'est pas si fréquente au Québec. En effet, seulement 0,5 % des répondants ont déclaré y avoir été confrontés à ce problème au cours des 12 derniers mois, ce qui correspond à 29.700 incidents annuels au Québec. Ce nombre réduit pourrait découler de la méthodologie de l'enquête, qui ciblait les utilisateurs adultes d'Internet, pour qui les relations en ligne seraient « plutôt caractérisées par des relations de civilité et de respect », contrairement aux internautes plus jeunes (Dupont, 2008, p. 22).

Par rapport à la législation canadienne, certaines dispositions du Code Criminel sont susceptibles d'être appliquées à des dossiers de cyberintimidation. Il s'agit des infractions telles que le harcèlement criminel (art. 264(1)); proférer des menaces (art. 264.1) ; émettre un faux message (art. 372(1)); l'extorsion (art. 346(1)); la supposition intentionnelle de personne (art. 403) et l'intimidation (art. 423). Finalement, la cyberintimidation peut également être assujettie à la Loi canadienne sur les droits de la personne, qui sanctionne la haine et la discrimination basée sur la race, l'origine ethnique, la couleur, la religion, le sexe, l'orientation sexuelle, le statut marital ou familial et les handicaps physiques ou mentaux (Sûreté du Québec, 2009).

5. Crimes économiques

5.1. Le piratage informatique

Le piratage informatique constitue une intrusion ou une utilisation non autorisée d'un système informatique. Depuis les dernières années, le piratage informatique évolue rapidement au Canada. Une enquête réalisée en 2011 (Statistique Canada, 2011b) montre à cet effet que 65% des internautes interrogés ont été victimes d'une infection

par un virus, un logiciel espion ou un logiciel publicitaire. Cette menace ne se limite pas cependant aux internautes. Une étude[6] récente (Telus-Rotman, 2011) montre qu'au Canada, le tiers des menaces recensées en sécurité des technologies de l'information visent des données financières. En France, une recherche récente montre qu'en 2010, 626 attaques contre des systèmes de traitement automatisé des données ont été répertoriées par la police, plus du tiers se référant à des accès avec altération du fonctionnement et modification ou suppression des données (Bauer, 2011). Au Québec, le Bureau de coordination des enquêtes sur les délits informatiques de la SQ a répertorié 154 incidents de piratage informatique et 82 incidents d'autre nature impliquant néanmoins une facette « piratage » entre 2004 et 2012. De plus, une recherche réalisée auprès de 1.100 internautes québécois révèle que 4,5 % des répondants ont été « victimes de ce phénomène chaque année au Québec, ce qui correspond à 267.000 incidents de piratage ou d'intrusions chez des particuliers » (Dupont, 2008, p.5). L'étude montre également que certains facteurs comme l'âge, le sexe et la fréquence d'utilisation de l'Internet peuvent augmenter la probabilité d'être victime d'un acte de piratage ou d'une intrusion informatique.

Dans le Code criminel canadien, certains articles ciblent explicitement le piratage informatique : Article 342.1 - Utilisation non autorisée d'ordinateur, Article 342.2 - Possession de moyens permettant d'utiliser un ordinateur, Article 430 (1.1) - Méfait concernant des données, Article 327 - Possession de moyens permettant d'utiliser des installations ou d'obtenir un service en matière de télécommunication, Article 184 - Interception des communications et Article 191 – Possession. Présentement, seules la propagation ou la tentative de propagation d'un virus informatique ou d'autres dispositifs malveillants constituent des infractions. Selon Valiquet (2011), pour ratifier la Convention européenne sur la cybercriminalité, le Canada devrait analyser la possibilité de modifier le Code criminel pour y inclure de nouvelles infractions comme la création, l'importation, la vente, la mise à disposition ou la possession d'un virus ou d'un autre dispositif malveillant dans le but de commettre un cybercrime.

5.1.2. Les *Botnets*

Les *botnets* existent depuis environ dix ans et ce phénomène est en constante augmentation. Une étude menée par Damballa (2010) montre que les *botnets* deviennent de plus en plus efficaces, seulement dix d'entre eux étant responsables de 57% des cas d'infection en 2010. Selon le rapport, le nombre de victimes aurait augmenté de 657% sur la seule période de l'année 2010 (Damballa, 2010). Le Canada n'est pas à l'abri de ce fléau. Un rapport récent montre à ce sujet que le nombre de sites d'hameçonnage (*phishing*) a augmenté de 319% au Canada durant l'année 2010. L'étude montre également qu'entre septembre 2010 et avril 2011 le nombre de réseaux *botnets* au pays a augmenté de 53% (Websense, 2011). En France, la situation ne semble pas très différente. Le rapport annuel de l'entreprise Cisco (2011) montre à cet effet qu'entre 2009 et 2010, la France fut le pays développé le plus touché par la

[6] Étude menée auprès de plus de 600 spécialistes en sécurité des TI au pays, englobant les organismes gouvernementaux, les sociétés cotées en bourse et les entreprises privées.

hausse du volume de spam, qui est de plus en plus fréquemment envoyé par le biais de *botnets*, cette augmentation étant de 115,3% pour la seule année 2010 (Cisco 2011).

Pour l'instant, Le Canada ne possède pas une législation particulière concernant l'utilisation des *botnets*. Toutefois, le Code criminel canadien encadre en partie cette nouvelle criminalité. Mentionnons trois articles principaux. Le premier article est l'article 342.1 du Code Criminel, qui concerne directement la criminalité informatique, l'article 342.2 quant à lui peut être invoqué contre un pirate informatique qui tenterait de se doter de *botnets*. Finalement, un pirate informatique pourrait aussi être accusé de méfaits concernant des données s'il exploite un *botnet* pour lancer une attaque par déni de service, un acte criminel réprimé par l'article 430 (1.1) du Code criminel canadien (Sûreté du Québec, 2009). En ce qui concerne le *spam*, le Canada a adopté en décembre 2010 sa loi antipourriel. Cette loi met en place un régime de réglementation et de sanctions administratives pécuniaires concernant le *spam*, l'hameçonnage, les contacts électroniques non sollicités, le vol d'identité, les logiciels espions, les virus et les réseaux d'ordinateurs zombies.

5.2. Usurpation et vol d'identité

Même si le vol d'identité n'est pas un phénomène nouveau, le développement de l'informatique en général, et notamment de l'Internet, eut un impact important sur le *modus operandi* des fraudeurs, ainsi que sur l'ampleur de cette pratique. Au Canada, en 2010, le Centre d'appel antifraude a reçu des signalements de fraude d'identité de la part de 18.146 victimes exposées à des pertes d'environ dix millions de dollars. En 2008, ce nombre était de 12.309 victimes. De plus, un sondage réalisé auprès de 3.000 consommateurs montre que 6,5% des répondants ont été victimes d'une forme de vol d'identité dans l'année précédente, ce qui équivaut à 1,7 millions de consommateurs. Au Québec, cette problématique prend également de l'ampleur. Une étude révèle qu'un peu plus de 5 % des répondants avaient été victimes de vol d'identité, ce qui permet d'estimer à 240.000 le nombre de victimes pour la période 2006-2007, avec un total de 338.000 incidents. L'étude démontre également que la technique du clonage des cartes représente le moyen le plus fréquent utilisé par les fraudeurs avec 40 % des cas, suivie par la corruption d'employés avec 15 % des cas identifiés (Dupont, 2008).

Quoique le Code criminel visait déjà la majorité des infractions liées au vol d'identité, il présentait certaines lacunes importantes qui ont été comblées par l'entrée en vigueur de la loi S-4, en janvier 2010. En effet, avant la loi S-4, le Code ne s'appliquait pas à la collecte, à la possession ou au trafic illicite de renseignements personnels pour un futur usage criminel (sauf par rapport aux cartes de crédit et aux mots de passe des ordinateurs). La loi S-4 a créé alors trois nouvelles infractions, à savoir : l'obtention et la possession de renseignements sur l'identité dans l'intention de les utiliser de façon trompeuse, malhonnête ou frauduleuse pour commettre un crime; le trafic de renseignements sur l'identité, et la possession ou le trafic illégal de documents d'identité émis par le gouvernement qui renferment les renseignements d'une autre personne. Ces nouvelles infractions sont toutes assujetties à des peines maximales de cinq ans d'emprisonnement. De plus, la loi a prévu la possibilité pour le

juge d'ordonner au prévenu de dédommager la victime d'un vol d'identité (Valiquet, 2011).

5.3. La fraude

La fraude est habituellement désignée comme une sollicitation sous de faux prétextes pour obtenir de l'argent. La dématérialisation des transactions en ligne engendre des opportunités de fraudes toujours plus nombreuses. Selon une recherche menée auprès des internautes canadiens, 4 % des internautes ont déclaré avoir été victimes de fraude bancaire dans les 12 mois précédant l'enquête. De plus, environ 14 % des répondants ayant effectué des achats en ligne au cours des 12 mois précédant l'enquête se sont heurtés à un problème causé soit par une erreur ou par des moyens frauduleux, pour au moins une des transactions effectuées. Près de 4 internautes sur 10 mentionnent également avoir fait l'objet d'au moins une tentative d'hameçonnage[7] (Statistique Canada, 2011b). Une étude réalisée au Québec révèle à son tour que 0,7% des répondants ont été victimes de fraudes sur les sites d'encan[8], que 0,4% des répondants ont été victimes de la fraude nigériane[9] et que 0,5% de l'échantillon signale avoir été victime de la fraude par loterie[10] (Dupont, 2008). Le nombre réduit de victimes au Québec pourrait s'expliquer en partie par la langue, puisque les sites et courriels frauduleux sont habituellement destinés à une clientèle anglophone (Dupont, 2008 ; Statistique Canada, 2011b). En France, 33.905 infractions liées à la fraude par Internet ont été repérées par les forces de l'ordre en 2010. Les données montrent que plus 80% de ces infractions se réfèrent à des escroqueries et abus de confiance tandis que le 20% restant inclut les falsifications et l'usage frauduleux des cartes de crédit, mais ces chiffres restent très fragmentaires, comme le souligne le responsable des statistiques de la délinquance (Bauer, 2011).

La fraude est définie dans l'article 380 du Code criminel comme étant le fait de frustrer le public ou une personne d'une valeur quelconque, par la supercherie, le mensonge ou d'autres moyens dolosifs. L'article 342.1(1)a) du Code pourra également servir de fondement à une mise en accusation puisqu'il se réfère à l'obtention

---

7 Il s'agit des « courriels frauduleux de quelqu'un se faisant passer pour un représentant d'une organisation fiable et légitime demandant des renseignements personnels » (Statistique Canada 2011b).

8 Cette fraude « consiste pour le fraudeur à promettre à sa victime la livraison d'un bien à un prix défiant toute concurrence. Une fois le paiement reçu par le fraudeur, celui-ci disparaît ou fait parvenir à sa victime un produit ne correspondant pas aux spécifications initiales » (Dupont, 2008).

9 Fraude qui « consiste à faire croire au destinataire d'un courriel que l'expéditeur est en possession de fonds importants auquel il ne peut accéder sans son assistance. Le fraudeur propose à la victime de toucher un pourcentage de ces fonds en échange de son aide (Dupont, 2008).

10 Dans ce cas, « la victime reçoit un courriel lui annonçant qu'elle a gagné un prix important, mais qu'elle doit acquitter des frais juridiques ou fiscaux pour permettre le versement des fonds. Une fois l'avance de fonds consentie par la victime, les fraudeurs disparaissent » (Dupont, 2008).

frauduleuse des services d'ordinateur. Mentionnons également qu'en décembre 2010 une nouvelle loi (C-2830) a mis en place des sanctions administratives et pécuniaires concernant le pourriel, ainsi que les « menaces connexes provenant de contacts électroniques non sollicités, dont le vol d'identité, l'hameçonnage, les logiciels espions, les virus et les réseaux d'ordinateurs zombies » (Valiquet, 2011).

6. Crimes contre la collectivité

6.1. Propagande haineuse

Dans un rapport préparé par le gouvernement canadien, une activité motivée par la haine est définie comme « tout acte, matériel ou organisation qui véhicule des préjugés contre des groupes identifiables [...] entre autres, la diffusion de matériel préconisant la haine» (Nelson et Kiefl, 1995). Au Canada, selon l'Enquête sociale générale réalisée en 2009, près d'un internaute sur six (16%) a déclaré être déjà tombé sur du contenu faisant la promotion de la haine envers un groupe particulier. Mentionnons également que d'après cette enquête, près des deux tiers (65 %) des crimes haineux déclarés par les répondants étaient, selon eux, motivés par la race ou l'origine ethnique, et 16 %, par la religion (Statistique Canada, 2011b). En 2009, les services de police canadiens[11] ont déclaré 1.473 crimes de haine. Ce nombre a augmenté de 42 % par rapport à 2008 (Statistique Canada, 2011c). Au Québec, les données déclarées par des services de police montrent une hausse des crimes motivés par la haine entre 2008 et 2009. En 2008 le nombre de crimes déclarés a été de 94 incidents, tandis qu'en 2009 ce nombre est passé à 198 incidents déclarés, ce qui correspond à un accroissement de 110,6% sur une année (Statistique Canada, 2011c)

Le crime de propagande haineuse est prévu dans le Code criminel du Canada dans deux passages : les articles 318 et 319. L'article 318 sanctionne l'encouragement au génocide alors que l'article 319 punit l'incitation publique à la haine. En ce qui concerne la propagande diffusée sur l'Internet, l'article 320.1 autorise les tribunaux à ordonner que la propagande haineuse accessible au public soit supprimée des systèmes informatiques.

7. Perspectives d'avenir : Les nouvelles technologies et leurs implications en matière de cybersécurité

Le monde de l'informatique est en constante mutation. De nouvelles technologies ne cessent d'apparaitre et de créer de nouvelles possibilités et de nouveaux risques. Pour faire face à ces innovations, le combat contre la cybercriminalité doit être en mesure d'anticiper les technologies émergentes afin analyser leurs implications sur la cybersecurité (Dupont, 2012). Parmi ces technologies émergentes, nous soulignons notamment l'informatique dans les nuages (*cloud computing),* la massification des données, l'Internet des objets et l'Internet mobile, qui font de plus en plus partie du quotidien des utilisateurs (Dupont, 2012).

[11] Desservant 87 % de la population.

L'informatique dans les nuages a connu une croissance impressionnante dans les dernières années. Ce service de stockage à distance de données représentera, selon certaines estimations, entre 20% et 30% du marché informatique en 2020 (Dupont, 2012). Les revenus mondiaux reliés à ce service, qui s'élevaient à 68,3 milliards de dollars en 2011, devraient doubler dans les prochaines années pour atteindre 148 milliards en 2014 (Foresight Horizon Scanning Centre, 2010). Cette nouvelle technologie n'est pas toutefois sans poser de risques. En effet, l'architecture même de ce service d'hébergement crée une vulnérabilité accrue aux actes de malveillance car les utilisateurs de l'infonuagique n'ont pas de contrôle sur les mesures de sécurité déployées par les fournisseurs de services. Cette décision, qui revient exclusivement à ces derniers, peut varier sensiblement puisqu'ils ne disposent pas tous des mêmes capacités de protection que les *leaders* du marché, comme Google, Microsoft ou Amazon (Dupont, 2012). Dans cette configuration, la confidentialité des données devient plus difficile à assurer. Étant donné la capacité de stockage inhérente à cette technologie, on constate également que la gravité des dommages subis par ce type de système est plus élevée que dans des configurations traditionnelles, en raison de la quantité de données sous leur responsabilité. On se rappellera à ce sujet qu'au printemps 2011, la compagnie Sony a été la cible d'une attaque pirate qui a mené au vol des données personnelles de plus de 100 millions d'utilisateurs de son portail interactif PlayStation Network. La vulnérabilité d'un tel système est d'ailleurs confirmée par les pirates mêmes. Selon un sondage réalisé en 2010 par l'entreprise Fortify Software auprès de 100 répondants à l'occasion de la conférence DefCon dédiée au piratage informatique, plus de 96% des pirates interrogés ont affirmé que l'informatique dans les nuages multiplie les opportunités de piratage et 45% d'entre eux affirment avoir déjà essayé d'exploiter les vulnérabilités de ces systèmes. De plus, 89% des répondants soulignent que la sécurité n'est pas suffisamment assurée par ces services (Fortify, 2010).

L'augmentation drastique dans les dernières années du volume de données produites et partagées par les utilisateurs du Web a donné lieu à ce qu'on appelle la massification des données (ou *big data* en anglais). Ces « données massives » constituent des fichiers de données contenant un volume gigantesque d'informations. Selon l'entreprise IDC, le volume des données numériques produites et traitées connaîtra une croissance exponentielle dans les prochaines années. Si, en 2011, la quantité mondiale d'informations créées et échangées sur des supports numériques équivalait à 1,8 zettabits, elle serait en effet multipliée par vingt d'ici 2020 pour atteindre 38 zettabits (Dupont, 2012). Cette production colossale d'information engendre cependant des problèmes importants au niveau de la vie privée des usagers, alors que de grandes entreprises commencent à commercialiser les données de leurs clients. Mentionnons par exemple que certaines institutions financières commercialisent déjà certaines données (p.ex. magasins fréquentés et produits achetés) reliées aux transactions par carte de paiement de leurs clients (Banerjee *et al.*, 2011). Dans le même sens, un fournisseur hollandais de solutions de localisation par GPS a également vendu les données des déplacements de ses usagers à des agences gouvernementales (Lasar, 2011). Ce marché secondaire des données massives expose ainsi les usagers à un risque croissant d'intrusions indésirables, d'autant plus que le croisement de fichiers de « données massives permet de désanonymiser des

fragments d'information en apparence anodins » (Acquisti *et al.*, 2011). Face à ce nouvel environnement, de nouvelles mesures pour assurer la vie privée des usagers devront êtres mises en place, car à l'avenir les mécanismes traditionnels de contrôle seront inadaptés face à cette technologie (Dupont, 2012).

La notion d'Internet des objets se réfère à une tendance croissante d'imbrication entre l'univers physique et numérique, par « le biais de capteurs et de senseurs intégrés aux objets qui nous entourent » (Dupont, 2012, p. 17). Cette nouvelle forme d'interconnexion a été rendue possible grâce à l'arrivée du protocole IPv6, un protocole réseau sans connexion qui dispose d'un espace d'adressage bien plus large que son prédécesseur, c'est-à-dire, le protocole IPv4. Il faut noter cependant que l'arrivé du protocole IPv6 apporte des défis importants en matière d'application de la loi, puisque durant la phase transitoire de IPv4 vers IPv6, il sera pratiquement et techniquement impossible de retracer certains internautes, dans la mesure où les fournisseurs de services ne disposeront pas de la technologie nécessaire pour lier les clients entre eux.

Cette nouvelle technologie facilite la surveillance du fonctionnement d'un nombre grandissant d'objets, comme les véhicules, les pacemakers, les compteurs électriques et même les réfrigérateurs. L'émergence de cette technologie fera que, dans les prochaines années, l'Internet ne se limitera plus aux réseaux numériques mais elle comprendra aussi des réseaux d'objets capables de communiquer entre eux et avec leurs contrôleurs (Hourcade *et al.,* 2009). En effet, Cisco prévoit qu'il y aura plus de 50 milliards d'objets connectés à Internet en 2020 (Evans, 2011). Parallèlement, on observe que l'augmentation du nombre d'objets connectés à Internet va vraisemblablement faire augmenter le nombre de cibles disponibles pour les pirates informatiques dans l'univers non virtuel. En 2010 par exemple, un employé d'une concession automobile du Texas a piraté une centaine de voitures en accédant à distance au système d'immobilisation des véhicules, utilisé en cas de non paiement des mensualités (Poulsen, 2010). On peut constater ainsi que, étant donné la nature même de cette nouvelle technologie, ses implications ne se limiteront peut-être pas à l'univers numérique seul, mais qu'elles engloberont également une problématique importante au niveau de la sécurité physique des individus.

Le concept d'Internet mobile désigne les technologies permettant « l'accès complet ou allégé à l'Internet à l'aide d'appareils mobiles tels que des téléphones intelligents ou des tablettes informatiques » (Dupont, 2012, p. 20). Avec le développement récent du marché de la téléphonie intelligente, cette technologie a connu un accroissement important au fil des dernières années et, selon plusieurs estimations, cette tendance croissante se maintiendra dans les prochaines années. IDC prévoit par exemple que, pour l'année 2012, la vente d'appareils mobiles sera deux fois plus élevée (985 millions d'unités) que celle des ordinateurs classiques (400 millions d'unités) (Gens, 2011). Les implications de cette nouvelle technologie pour la cybersécurité sont multiples. Dans les prochaines années, l'infection des téléphones à l'aide d'applications malveillantes devrait connaître une augmentation, reflétant le fort taux d'adoption de l'internet mobile. Cette problématique est d'ailleurs déjà bien actuelle. L'entreprise de sécurité Norton a réalisé un sondage à ce propos, lequel démontre que

10% de la population adulte aurait déjà été victime de crimes reliés à l'utilisation de téléphones intelligents, et Symantec estimait en 2010 que les menaces à l'Internet mobile avaient connu une croissance de 42% par rapport à l'année précédente (Albanesius, 2011). Des problèmes au niveau des chaînes d'approvisionnement et de distribution sont également à prévoir. Par exemple, en 2010, 3.000 téléphones intelligents de la filiale espagnole de la compagnie Vodafone ont été infectés par le logiciel malveillant Mariposa pour être ensuite commercialisés par ses propres revendeurs agréés (Leyden, 2010).

8. Complexité et défis en matière d'application de la loi

La rapidité avec laquelle les nouvelles technologies se développent rend difficile la lutte contre la cybercriminalité. Au Canada, les organismes d'application de la loi font face à de nombreux défis reliés à la modernisation des infractions et des techniques d'enquête (Valiquet, 2011). Certains éléments peuvent cependant aider la lutte contre cette forme de criminalité. Le premier est l'exploitation de ce que nous pouvons appeler la « cybergéographie» (Sûreté du Québec, 2009). L'objectif étant de cartographier les réseaux informatiques, cette méthode permet d'identifier et de connaître les failles potentielles se trouvant dans les réseaux informatiques. En ayant ce portrait des failles informatiques, cela permettra aux décideurs de la sécurité de prioriser les brèches à colmater (Sûreté du Québec, 2009). Le second élément concerne la capacité de contrôler l'ensemble des espaces numériques pour donner aux décideurs en sécurité le pouvoir d'agir (Sûreté du Québec, 2009). Pour y parvenir, certains débats devront se tenir, notamment en ce qui concerne la portée de l'anonymat sur Internet. À ce sujet, certains services d'accès à l'Internet, comme les cybercafés, les bibliothèques publiques, les cartes d'accès Internet et les services de cellulaire prépayés sont perçus par les organismes d'application de la loi comme un obstacle à l'enquête policière. En effet, à l'heure actuelle, les télécommunicateurs ne sont pas tenus de vérifier l'identité des usagers de ces services, ce qui leur permet alors de rester anonymes (Valiquet, 2011).

Cette réflexion mène à la question des politiques à mettre en place pour lutter contre la cybercriminalité. Si la menace de la cybercriminalité se montre toujours grandissante, les gouvernements demeurent très en retard dans l'implantation de mesures de cybersécurité. Cela semble particulièrement vrai au Canada, où les procédures d'enquête sur les cybercrimes sont de moins en moins adaptées à cette forme de criminalité. Mentionnons par exemple le fait que le Canada n'impose pas aux fournisseurs de service Internet (FSI) l'obligation de signaler aux autorités la présence d'un contenu à caractère illicite, sauf lorsqu'il s'agit d'un incident concernant la pornographie juvénile, en vertu de la Loi C-22, adoptée le 23 mars 2011. Soulignons également qu'au Canada, il n'existe, à l'heure actuelle, aucune loi obligeant les télécommunicateurs à se doter d'appareils permettant l'interception des communications. Ils ne sont pas non plus contraints de recueillir ni de conserver des informations sur l'usage que font leurs abonnés de leurs services[12] (Valiquet, 2011).

[12] Le projet de loi sur l'accès légal (C-30), déposé le 14 février 2012 vise à obliger les fournisseurs de services Internet et de téléphonie cellulaire à dévoiler à la police - sans

Et pourtant, ce sont surtout les gouvernements qui devront investir dans la lutte contre la cybercriminalité. D'une part, cela passe évidemment par les budgets destinés aux organismes d'application de la loi. Par exemple, il est clair qu'une lutte efficace contre la cybercriminalité demande des formations spécialisées tant chez les policiers que chez les avocats et les juges. Cela demande donc un investissement supplémentaire, afin de fournir des outils intellectuels aux professionnels agissant dans le domaine (Sûreté du Québec, 2009). D'autre part, cela passe aussi par l'augmentation des postes budgétaires dévolus aux projets d'informatisation des secteurs gouvernementaux (Sûreté du Québec, 2009). En ce moment, bon nombre de projets informatiques sont établis par diverses organisations gouvernementales. Mais, trop souvent, la sécurité informatique devient l'enfant pauvre de ces projets. Cela insécurise bien évidemment les données fournies par les citoyens au gouvernement. Cette tendance est d'ailleurs démontrée dans une étude menée par Benoît Dupont et Benoît Gagnon (2008) : les trois secteurs les plus visés par la compromission de données sont, dans l'ordre, le secteur de l'éducation, de la santé et la fonction publique plus largement. Cela démontre donc qu'il y a urgence d'agir dans ce domaine.

Conclusion

La complexité inhérente à l'écosystème numérique appelle à une vision élargie de la cybersécurité. La cybercriminalité doit être comprise dans ce sens comme un phénomène sous-tendu par des dynamiques diverses. Pour s'avérer efficace, les stratégies de cybersécurité doivent alors développer des outils capables de cartographier les acteurs et les interactions pour ainsi évaluer les implications de ces transformations sur la cybersécurité (Dupont, 2012). Par ailleurs, la nature transnationale de la cybercriminalité demande une intégration des stratégies de gestion de risque par les acteurs gouvernementaux ainsi que leurs partenaires privés afin de déceler rapidement les risques, en limitant ainsi leur impact sur l'écosystème numérique (Dupont, 2012). L'expansion et la diversification de cet écosystème doivent s'accompagner d'ailleurs d'innovations institutionnelles et règlementaires afin d'adapter les capacités d'intervention et de coordination des gouvernements à des besoins nouveaux. Il est nécessaire également d'accentuer les initiatives de coordination et de transfert de connaissance entre les acteurs chargés de la prévention et de l'application de la loi afin d'accélérer et de standardiser le développement des capacités locales. Finalement, il est important d'intensifier les recherches empiriques sur les transformations de l'écosystème numérique. Cependant, puisque la cybercriminalité constitue un phénomène complexe, le recours exclusif à des spécialistes issus de l'informatique n'offre qu'une solution partielle. Il faudrait plutôt mettre en place des équipes multidisciplinaires (informaticiens, politologues, criminologues, spécialistes des communications, juristes, etc.) pour endiguer

---

mandat mais avec un encadrement serré – des données informatiques permettant d'identifier un individu qui aurait commis un crime ou qui est soupçonné d'avoir commis un crime. Les critiques à ce projet sont multiples, tant parmi l'opposition qu'au sein du gouvernement.

correctement le phénomène (Sûreté du Québec, 2009). Également, les alliances stratégiques[13] existant entre les services gouvernementaux, l'industrie et les milieux académiques doivent être renforcés, afin de soutenir les efforts de ces équipes multidisciplinaires (Sûreté du Québec, 2009).

[13] À titre d'exemple : www.ncfta.ca

Références

Acquisti, A., Gross, R. et F. Stutzman (2011), "Faces of Facebook : Privacy in the age of augmented reality", Black Hat 2011, 3-4 août, Las Vegas. Accessible en ligne à http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf, consulté le 26 décembre 2011.

Albanesius, C. (2011), "Cyber crime costs $114B per year, mobile attacks on the rise", PCmag.com, 7 septembre. Accessible en ligne à http://www.pcmag.com/article2/0,2817,2392570,00.asp, consulté le 28 décembre 2011

Bauer, A. (2011). La criminalité en France : Rapport de l'Observatoire national de la délinquance 2010. Accessible en ligne à http://www.inhesj.fr/fichiers/ondrp/rapport_annuel/synthese-rapport-2010.pdf, consulté le 10 décembre 2011.

Banerjee S., Bolze J., McNamara, J. et K. O'Reilly (2011), "How big data can fuel bigger growth", Outlook: The online journal of high-performance business, no. 3. Accessible en ligne à http://www.accenture.com/us-en/outlook/Pages/outlook-journal-2011- how-big-data-fuels-bigger-growth.aspx, consulté le 26 décembre 2011

Bureau de la concurrence (2010). Mois de la prévention de la fraude. Accessible en ligne à http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03218.html, consulté le 10 novembre 2011.

Bureau d'intervention en matière de harcèlement sexuel (2009). La violence sexuelle. Accescible en ligne à http://www.harcelement.uottawa.ca/sexuel/svw-defi-violencefr.html, consulté le 04 juin 2012

Cefrio (2011a). Utilisation d'Internet au Québec en décembre 2011. Accessible en ligne à http://blogue.cefrio.qc.ca/2012/01/utilisation-dinternet-au-quebec-en-decembre-2011, consulté le 10 janvier 2012.

Cefrio (2011b). Utilisation d'Internet au Québec en septembre 2011. Accessible à http://blogue.cefrio.qc.ca/2011/09/utilisation-dinternet-au-quebec-en-septembre-2011/, consulté le 15 décembre 2011.

Cefrio (2011c). L'engouement pour les médias sociaux au Québec. Netendances, volume 2, numéro 1.

Centrale des syndicats du Québec (2011). Cyberintimidation dans le milieu de l'éducation. Rapport final. Accessible en ligne à http://beta.csq.qc.net/fileadmin/CSQ/Internet/documents/portail_csq/documentation/education_formation/cyberintimidation/cyberintimidation_milieu_education.pdf, consulté le 20 décembre 2011.

Chawki, M. (2006). Essai sur la notion de cybercriminalité. Accessible en ligne à http://www.ie-ei.eu/bibliotheque/cybercrime.pdf, consulté le 20 décembre 2011.

Cisco (2011). Rapport annuel portant sur la sécurité sur Internet et la lutte contre la cybercriminalité. Accessible en ligne à http://experts-it.fr/files/2011/02/Cisco-2010-ASR.pdf, consulté le 03 janvier 2012.

Clusif (2009). Bots et Botnets. Accessible en ligne à http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2009-Bots-et-Botnets.pdf, consulté le 05 décembre 2011.

Credoc (2009). La diffusion des technologies de l'information et de la communication dans la société française. Accessible à http://www.arcep.fr/fileadmin/reprise/communiques/communiques/2009/slides-etude-credoc-2009.pdf, consulté le 11 décembre 2011.

Damballa (2010). The Command Structure of the Aurora Botnet : History, Patterns and Findings Bots et Botnets. Espace Menaces, CLUSIF. Accessible en ligne à http://www.damballa.com/research/aurora, consulté le 01 décembre 2011.

Davies, A. (2011). Résumé législatif du projet de loi C-28 : Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique. Service d'information et de recherche parlementaires. Bibliothèque du Parlement. Accessible en ligne à http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=c28&source=library_prb&Parl=40&Ses=3&Language=F, consulté le 15 décembre 2011.

Dupont, B. (2008). Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec. Accessible en ligne à http://www.securitepublique.gouv.qc.ca/fileadmin/Documents/statistiques/prevention/vol_identite/vol_identite.pdf, consulté le 10 décembre 2011.

Dupont, B. (2012) L'environnement de la cybersecurité à l'horizon 2022. Tendances, moteurs et implications, Sécurité Publique Canada, Ottawa.

Enisa (2011). Botnets: Detection, Measurement, Disinfection & Defence. Accessible en ligne à http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence, consulté le 05 décembre 2011.

Evans, D. (2011), The internet of things: How the next evolution of the internet is changing everything, Cisco Internet Business Solutions Group: San Jose.

Florêncio, D. Herley, C. (2012). Accessible en ligne à http://weis2011.econinfosec.org/papers/Sex,%20Lies%20and%20Cyber-crime%20Surveys.pdf, consulté le 10 mai 2012.

Fortify (2010). Defcon survey reveals vast scale of cloud hacking - and the need to bolster security to counter the problem. Accessible en ligne à https://www.fortify.com/news-and-events/press-releases/2010/2010-08-24.html, consulté le 01 décembre 2011.

Foresight Horizon Scanning Centre (2010), Technology and innovation futures: Technology annex, Department for Business Innovation & Skills: Londres.

Gens, F. (2011), Top 10 predictions – IDC predictions 2012: Competing for 2020, IDC: Framingham.

Ghernaouti-Hélie, S. (2010). *Comment lutter contre la cybercriminalité ?* Pour la Science, n° 391. Accessible en ligne à http://www.itu.int/cybersecurity/Articles/Ghernaouti_PLS391.pdf, consulté le 11 mai 2012.

Gouvernement du Canada (2011). La Loi canadienne anti-pourriel. Accessible en ligne à http://combattrelepourriel.gc.ca/eic/site/030.nsf/fra/h_00039.html, consulté le 10 décembre 2011.

Hourcade, J.-C., Neuvo, Y., Posch, R., Saracco, R., Sharpe, M. et W. Wahlster (2009), Future internet 2020 : Visions of an industry expert group, Commission Européenne: Bruxelles.

ICANN (2011). Rapport annuel. Accessible en ligne à http://www.google.ca/url?sa=t&rct=j&q=rapport%20annuel%20icann%202011&source=web&cd=1&ved=0CGAQFjAA&url=http%3A%2F%2Fwww.icann.org%2Ffr%2Fabout%2Fannual-report%2Fannual-report-2011, consulté le 12 mai 2012.

Jeunesse J'écoute (2007). La cyberintimidation: une nouvelle réalité´ pour les jeunes. Accessible en ligne à http://org.kidshelpphone.ca/media/21707/2007_cyber_bullying_report_full_fr.pdf, consulté le 04 juin 2012.

Jing Liu, Yang Xiao, Kaveh Ghaboosi, Hongmei Deng, Jingyuan Zhang (2010). Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. EURASIP Journal on Wireless Communications and Networking.

Juristat (2009). Leurre d'enfants par Internet. Accessible en ligne à http://www.statcan.gc.ca/pub/85-002-x/2009001/article/10783-fra.htm, consulté le 05 novembre 2011.

Lasar, M. (2011), "Dutch traffic cops use Tom Tom GPS data to nail speeders", Ars

Technica, 28 avril. Accessible en ligne à http://arstechnica.com/tech-policy/news/2011/04/dutch-traffic-cops-use-tomtom-gps-data-to-nail-speeders.ars, consulté le 26 décembre 2011.
Leyden, J. (2010), "Vodafone Spain admits 3,000 smartphones shipped with Mariposa", The Register, 19 mars. Accessible en ligne à http://www.theregister.co.uk/2010/03/19/voda_spain_mariposa_latest/, consulté le 27 décembre 2011.

Ministère de la Sécurité Publique (2007). Des modifications à venir dans le Programme de déclaration uniforme de la criminalité. Accessible en ligne à http://www.securitepublique.gouv.qc.ca/fileadmin/Documents/statistiques/prevention/programme_duc/bulletin_duc_mai-07.pdf, consulté le 10 novembre 2011.

Ministère de l'Intérieur (2010). Qu'est-ce-que la cybercriminalité?. Accessible en ligne à http://www.interieur.gouv.fr/sections/a_votre_service/votre_securite/internet/cybercriminalite/presentation-cybercriminalite/view, consulté le 02 janvier 2012.

Norton Cybercrime Report (2011). Accessible à http://www.symantec.com/content/fr/ca/home_homeoffice/html/cybercrimereport/, consulté le 10 janvier 2012.

Office québécois de la langue française (2009). Délit informatique [En ligne]. [http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp] (Consulté le 20 février 2009).

Observatoire de la Sécurité des Paiements (2010). Le rapport annuel d'activité 2010. Accessible en ligne à http://www.banque-france.fr/observatoire/rap_act_fr_10.htm, consulté le 20 décembre 2011.

Office de la langue française du Québec (2008). Accessible en ligne à http://www.oqlf.gouv.qc.ca/, consulté le 20 décembre 2011.

Panda Security (2011). Le marché noir de la cybercriminalité révélé. Accessible en ligne à http://blog.pandasecurity.fr/doc/Le_Marche_Noir_du_Cyber_Crime_FR.pdf, consulté 20 décembre 2011.

Poulsen, K. (2010), "Hacker disables more than 100 cars remotely", Wired Threat Level Blog, 17 mars. Accessible en ligne à http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/, consulté le 27 décembre 2011.

Sécurité Publique Québec (2010). Statistiques 2008 sur les agressions sexuelles au Québec. Accessible en ligne à http://www.securitepublique.gouv.qc.ca/police/publications-statistiques-

police/statistiques-agression-sexuelle/agressions-sexuelles-2008/3030.html, consulté le 15 novembre 2011.

Sécurité Publique Québec (2011). Statistiques 2009 sur les agressions sexuelles au Québec. Accessible en ligne à http://www.securitepublique.gouv.qc.ca/police/publications-statistiques-police/statistiques-agression-sexuelle/agressions-sexuelles-2009/5050.html, consulté le 20 décembre 2011.

Statistique Canada (2002). Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police. Accessible en ligne à http://publications.gc.ca/collections/Collection/Statcan/85-558-X/85-558-XIF2002001.pdf, consulté le 15 novembre 2011.

Statistique Canada (2010). La victimisation criminelle au Canada, 2009. Accessible en ligne à http://www.statcan.gc.ca/pub/85-002-x/2010002/article/11340-fra.htm, consulté le 01 novembre 2011.

Statistique Canada (2011a). Enquête canadienne sur l'utilisation d'Internet. Accessible à http://www.statcan.gc.ca/daily-quotidien/110525/dq110525b-fra.htm, consulté le 10 décembre 2011.

Statistique Canada (2011b). Les incidents autodéclarés de victimisation sur Internet au Canada, 2009. Accessible en ligne à http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11530-fra.htm, consulté le 10 décembre 2011.

Statistique Canada (2011c). Les crimes haineux déclarés par la police au Canada, 2009. Accessible en ligne à http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11469-fra.htm, consulté le 05 janvier 2012.

Sproule, S. & Archer, N. (2008). Measuring Identity Theft in Canada: 2008 Consumer Survey - Working Paper # 23. Accessible en ligne à http://merc.mcmaster.ca/working-papers/23.html, consulté le 20 décembre 2011.

Sûreté du Québec (2009). Analyse stratégique sur la cybercriminalité. Document non publié.

Telus-Rotman (2011). Communiqué de presse : Selon l'étude TELUS-Rotman sur la sécurité des TI de 2011, le piratage est devenu de plus en plus sophistiqué; une menace sur trois viserait des données financières. Accessible en ligne à http://about.telus.com/community/french/news_centre/news_releases/blog/2011/11/15/selon-l-%C3%A9tude-telus-rotman-sur-la-s%C3%A9curit%C3%A9-des-ti-de-2011-le-piratage-est-devenu-de-plus-en-plus-sophistiqu%C3%A9-une-menace-sur-trois-viserait-des-donn%C3%A9es-financi%C3%A8res, consulté le 05 janvier 2012.

TNS Sofres (2010). Digital Life. Accessible en ligne à http://2010.tnsdigitallife.com, consulté le 10 décembre 2011.

Valiquet, D. (2011). Cybercriminalité : les enjeux. Service d'information et de recherche parlementaires. Bibliothèque du Parlement. Accessible en ligne à http://www.parl.gc.ca/Content/LOP/ResearchPublications/2011-36-f.htm, consulté le 10 décembre 2011.

ZDNet France (2011). L'UIT recense 2 milliards d'utilisateurs d'Internet dans le monde. Accessible en ligne à http://www.zdnet.fr/actualites/l-uit-recense-2-milliards-d-utilisateurs-d-internet-dans-le-monde-39757795.htm, consulté le 15 décembre 2011.

Walrave, M; Demoulin, M; Heirman, W; Van der Perre, A. (2009). Cyberharcèlement : risque du virtuel, impact dans le réel. Observatoire des droits de l'Internet. Accessible en ligne à http://www.internet-observatory.be/internet_observatory/pdf/brochures/Boek_cyberpesten_fr.pdf, consulté le 10 novembre 2011.

Websense (2011). The Next Hotbed of Cybercrime Activity is… Canada? Accessible en ligne à http://community.websense.com/blogs/securitylabs/archive/2011/05/11/the-next-hotbed-of-cybercrime-activity-is-canada.aspx, consulté le 20 décembre 2011.