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

3

Crimes sur le Web 2.0[1]

Benoît Dupont[2]
Pierre-Éric Lavoie[3]
Francis Fortin[4]

L'avènement des sites de socialisation en ligne (MySpace, Facebook, YouTube, Flickr, etc.) est perçu comme un développement technologique si important par les observateurs d'Internet que nombre d'entre eux assimilent l'émergence de ces applications à la transition vers Internet de deuxième génération. Bien qu'on s'accorde généralement sur les caractéristiques dominantes de ces sites, notamment leur interactivité, leur connectivité et leur dimension sociale, les définitions du Web 2.0 restent imprécises, ce qui fait dire à d'autres qu'il s'agit là d'un simple effet de mode cherchant à distinguer de manière exagérée l'évolution naturelle d'Internet (Dupont et Gautrais, 2010).

Pourtant, force est de constater que les sites de socialisation sont devenus en quelques années (ou même en quelques mois dans certains cas) des

1. Cette recherche a été entreprise grâce au soutien financier du Conseil de recherches en sciences humaines du Canada et du Programme des chaires de recherche du Canada, ainsi qu'en partenariat avec la Sûreté du Québec.

2. Directeur du Centre international de criminologie comparée, Université de Montréal.

3. Candidat à la maîtrise, École de criminologie, Université de Montréal.

4. Chercheur associé, Centre international de criminologie comparée, et candidat au doctorat, École de criminologie de l'Université de Montréal.

moyens de communication incontournables pour les internautes, qui consacrent de nombreuses heures chaque semaine à leur consultation et à la mise à jour de leur profil personnel. À l'échelle mondiale, 67 % des internautes appartenaient à un site de socialisation en ligne en décembre 2008, avec des pics au Brésil (80 %), en Espagne (75 %) et en Italie (73 %) [Nielsen, 2009]. On remarque toutefois des variations importantes d'une tranche d'âge à une autre, les adolescents et les jeunes adultes étant presque deux fois plus adeptes de ces sites que la population de plus de 30 ans (Lenhart, Purcell, Smith et Zickuhr, 2010). La progression de la fréquentation de ces sites les rend maintenant plus populaires que les sites de courrier électronique (Gmail, Hotmail, Yahoo Mail, etc.) et même que le moteur de recherche Google. Les changements de comportement concernent également le temps passé en ligne : les usagers des sites de socialisation leur consacrent environ 10 % du temps total accordé à Internet, avec un pourcentage de croissance annuelle de 63 % (566 % pour Facebook) qui reflète la perte de vitesse d'autres catégories de sites (Nielsen, 2009).

Cette croissance exponentielle ne reflète pas seulement le remplacement d'une technologie par une autre. Elle a également donné lieu à des questionnements de la part de l'opinion publique et d'organismes gouvernementaux concernant la sécurité du Web 2.0. Les principales inquiétudes visent la divulgation excessive d'informations personnelles à laquelle ces sites exposent leurs usagers (Denham, 2009), l'exposition des internautes les plus jeunes à des risques accrus d'être contactés par des prédateurs sexuels qui pourraient utiliser ces sites pour sélectionner leurs victimes, et l'exploitation par les fraudeurs et les pirates informatiques de la confiance qu'accordent les usagers aux contenus de ces sites.

Peu d'informations sont disponibles à l'heure actuelle sur les risques criminels spécifiquement associés au développement du Web 2.0, à l'exception des comptes-rendus d'incidents isolés publiés dans les médias. Afin de remédier à cette situation, un projet de recherche financé par le Conseil de recherches en sciences humaines du Canada et mené en partenariat avec la Sûreté du Québec a été lancé en 2008 par la Chaire de recherche du Canada en sécurité, identité et technologie. Les objectifs de ce projet sont de comprendre la nature particulière des risques associés au Web 2.0, d'analyser la réponse judiciaire qui y est apportée à l'heure actuelle et d'explorer les mécanismes de régulation existants et potentiels pour y faire face.

Ce chapitre livre les résultats préliminaires concernant le premier volet de l'étude, c'est-à-dire la nature et la distribution des risques dans l'univers du Web 2.0.

3.1 Méthodologie

Les organisations policières ne recueillent pas à l'heure actuelle de statistiques permettant de mesurer la prévalence des comportements criminels et déviants associés au Web 2.0. Afin de pouvoir néanmoins mener des analyses qui dépassent la simple dimension anecdotique, une base de données a été créée. Elle est constituée d'affaires rapportées dans les médias du monde entier qui respectent les deux critères suivants :

- elles concernent des comportements criminels ou déviants relatifs à des atteintes aux biens, aux personnes ou à leur réputation. Pour des raisons qu'il serait trop long de détailler ici, les violations au droit de la propriété intellectuelle comme l'utilisation ou la diffusion sans autorisation d'œuvres protégées par le droit d'auteur ne sont pas incluses dans notre échantillon;
- elles impliquent une composante technique relevant du Web 2.0, qu'il s'agisse de sites de réseautage social, d'échange de vidéos ou de blogues (ce critère est évalué à partir de la liste des 40 principales entreprises du secteur).

Cette base de données est alimentée depuis octobre 2008 de manière automatisée par l'application Yahoo Pipes[5], qui identifie, filtre et centralise les informations correspondant aux deux critères mentionnés au paragraphe précédent. Cette application en ligne gratuite permet aux utilisateurs de créer des scripts ou des routines de traitement des données provenant de sources Web diverses qui facilitent considérablement la collecte d'informations, puisqu'il n'est plus nécessaire de consulter manuellement et de façon répétitive une multitude de sites Internet de référence dont les contenus changent fréquemment, comme les sites de la presse généraliste ou les blogues. Le recours à cet outil a permis de surveiller en permanence 87 sources (47 en anglais et 40 en français) parmi lesquelles figurent des médias généralistes (comme *La Presse*, *Le Devoir*, Radio-Canada), des sites

5. pipes.yahoo.com/pipes/.

spécialisés dans les nouvelles technologies (entre autres Branchez-vous et Silicon.fr) et des blogues consacrés à la délinquance en ligne (Computer crime, The dead kids of MySpace, etc.).

Les articles sélectionnés par Yahoo Pipes sont ensuite examinés individuellement afin d'en vérifier la pertinence et d'en coder le contenu dans une base de données administrée grâce au logiciel SPSS (*Statistical Package for the Social Sciences*). Les variables associées à chaque événement comprennent la date de l'événement, sa localisation géographique, les types de comportements observés, les entreprises ou services impliqués ainsi que les informations démographiques sur les auteurs et les victimes.

L'échantillon comprend 683 cas (796 suspects et 540 victimes) recueillis sur une période de 14 mois (6 octobre 2008 au 12 décembre 2009)[6]. Bien entendu, si cette approche permet de mieux connaître les comportements associés à une technologie récente, elle n'en demeure pas moins soumise aux limites qu'implique l'origine des informations utilisées. En effet, les comptes-rendus des médias ne reflètent pas seulement la réalité d'un phénomène. Ils sont également le résultat d'un processus de sélection et d'analyse de la part des journalistes et des salles de rédaction, qui ne sont tenus à aucune obligation de représentativité statistique. Dans ce contexte, certains comportements jugés comme particulièrement inquiétants auront tendance à faire l'objet d'une couverture disproportionnée, alors que d'autres comportements pourtant tout aussi problématiques, mais moins médiatisés, seront délaissés ou traités en quelques entrefilets.

Néanmoins, en l'absence de sources alternatives de données, cette méthodologie constitue une excellente façon d'analyser de manière systématique la nature des crimes associés au Web 2.0 et les dynamiques sociales et technologiques qui s'y rapportent.

3.2 Crimes et déviances observés sur le web 2.0

La classification des comportements criminels et problématiques recensés dans la base de données comprend sept grandes catégories qui

6. La différence entre le nombre de cas et le nombre d'individus impliqués est attribuable au manque d'informations disponibles sur l'identité des auteurs et des victimes dans certaines affaires rapportées dans les médias.

touchent aussi bien les personnes que leurs biens ou leur réputation. Comme le montre le tableau 3.1, les crimes contre la personne, qu'ils soient de nature sexuelle ou qu'ils impliquent des actes de violence ou des menaces, représentent plus de la moitié (56,2 %) des événements analysés. Cependant, cette donnée doit être interprétée avec prudence. En effet, on peut aisément imaginer que les médias vont privilégier dans leur couverture des incidents particulièrement graves ou choquants afin d'attirer l'attention de leur lectorat sur les risques bien réels inhérents à ces nouveaux outils de communication.

Tableau 3.1 Distribution des affaires par type de crime ou de risque

	Fréquence	Pourcentage
Crimes sexuels	272	39,8 %
Atteintes à la personne (violences et menaces)	112	16,4 %
Attaques informatiques	112	16,4 %
Fraudes	67	9,8 %
Atteintes aux biens	35	5,1 %
Contenus problématiques	72	10,5 %
Autres	13	1,9 %
Total	683	100 %

Les crimes les plus fréquemment recensés sont les crimes sexuels. On retrouve dans cette catégorie une majorité significative de cas dont les victimes sont des personnes mineures (57,2 % de la catégorie « crimes sexuels »). On peut d'ores et déjà préciser qu'elle comprend des cas d'agression sexuelle (contre des mineurs avec ou sans usage de la contrainte ainsi que contre des majeurs), de pornographie juvénile, de prostitution (aussi bien adulte que juvénile) ou encore de comportement indécent en ligne. L'importance relative des crimes sexuels dans notre échantillon ne doit pas surprendre dans la mesure où les services offerts par les sites du Web 2.0 consistent principalement en la mise en relation d'individus par le biais de plateformes de socialisation en ligne, et que ces derniers sont encouragés à partager avec leurs « amis » des aspects plus ou moins intimes de leur vie, ainsi que des photos pouvant les représenter dans des poses équivoques. Par contre, il est aussi indispensable de relativiser ces données, puisqu'un service comme Facebook

revendiquait au début de l'année 2010 pas moins de 400 millions d'utilisateurs actifs (13 millions au Canada) et que MySpace, son compétiteur direct, comptait environ 125 millions d'usagers à la même période. De plus, selon un récent sondage, environ 73 % des adolescents américains actifs en ligne (soit plus de 90 % de l'ensemble de la population adolescente) fréquentaient un site de socialisation en ligne (Lenhart, Purcell, Smith et Zickuhr, 2010). Considérant un tel bassin d'utilisateurs, dont une grande proportion est composée de mineurs, on semble donc loin d'assister à l'épidémie de crimes sexuels anticipée par les autorités juridiques américaines à la fin de l'année 2007 (Alexander, 2008).

La deuxième catégorie de crimes en importance concerne les autres atteintes à la personne. On y retrouve d'abord des actes de violence physique qui comprennent des meurtres et des tentatives de meurtre (21 cas), des voies de fait ou des vols avec violence. Dans les cas de meurtres et de voies de fait, les outils du Web 2.0 jouent principalement un rôle accessoire. Les parties entretiennent en effet fréquemment un conflit préalable qui est exacerbé par des informations ou des commentaires diffusés sur les sites de socialisation en ligne. On recense également de nombreux cas de violence conjugale dans lesquels la jalousie est alimentée par l'utilisation que font les conjoints du Web 2.0. Dans le cas des vols avec violence, le Web 2.0 est utilisé par les délinquants comme outil de planification permettant d'identifier leurs victimes et de gagner leur confiance. On retrouve également dans cette catégorie des cas de menaces nominatives proférées sur Internet ainsi que des cas d'incitation à la haine envers un groupe social ou ethnique particulier. Les cas de harcèlement et d'intimidation semblent en revanche moins présents dans notre échantillon, bien que des sondages menés auprès des jeunes utilisateurs aient mis en lumière la prévalence de ce type de comportement[7]. Le cas d'intimidation le plus médiatisé est certainement celui de Megan Meier, cette adolescente de 13 ans qui a mis fin à ses jours après avoir découvert que le petit ami qu'elle pensait avoir rencontré sur MySpace et qui l'accablait de commentaires humiliants était en fait la mère d'une ancienne camarade de classe (Maag, 2007).

Les attaques informatiques utilisant le Web 2.0 comme vecteur privilégié sont aussi fréquentes dans notre échantillon que les actes de

7. Voir par exemple Beran et Li (2005) pour le Canada et Ybarra et Mitchell (2007) pour les États-Unis.

violence (à l'exclusion des crimes sexuels) et les menaces. Le Web 2.0 constitue en effet un environnement technologique très attrayant pour les pirates informatiques. En premier lieu, il leur procure un important bassin de victimes potentielles du fait de la très grande popularité des sites de socialisation en ligne. Ensuite, la nature ouverte de ces sites permet à chacun de leurs utilisateurs de diffuser du contenu audiovisuel ou logiciel qui n'est que rarement contrôlé. Cela conduit à un transfert de responsabilité aux usagers en matière de sécurité, qui sont souvent incapables de juger de la dangerosité ou de l'innocuité de certains contenus. Enfin, les utilisateurs de ces sites sont connectés les uns aux autres par des liens de confiance qui facilitent également la propagation des programmes malveillants. En effet, si les virus et les vers informatiques trouvaient déjà sur le réseau Internet un mode de propagation privilégié (par courriel notamment), les plateformes de socialisation en ligne constituent un environnement propice à la contagion rapide de victimes sous couvert d'échanges d'applications anodines provenant d'amis ou de proches. Le ver « Koobface » (anagramme de Facebook) est certainement le plus connu de ces programmes malveillants. Apparu en 2008 et ayant « colonisé » depuis d'autres sites du Web 2.0 comme MySpace, Twitter ou Bebo, il se diffuse en incitant ses cibles à cliquer sur un lien censé conduire à une vidéo particulièrement intéressante ou compromettante. Le fait de cliquer sur ce lien entraîne en réalité le téléchargement sur l'ordinateur de la victime d'une application malveillante qui va continuer à se propager par le biais des membres du réseau social de cette dernière, tout en permettant au délinquant d'utiliser l'ordinateur compromis pour diffuser des pourriels, mener des attaques par déni de service ou voler des identifiants personnels. On estime que « Koobface » aurait contaminé plus de trois millions de machines (Cisco, 2009), ce qui dénote une forme de crime à très grande échelle qui se distingue quantitativement des crimes contre la personne, où il est possible d'identifier des victimes individuelles. Les chiffres qui figurent dans notre étude doivent donc être interprétés à la lumière de ces caractéristiques.

Les fraudes et les atteintes aux biens arrivent respectivement en quatrième et cinquième positions dans notre classement des types de crimes rapportés par les médias avec respectivement 9,8 % et 5,1 % des affaires recensées. Les cas de fraude se présentent sous la forme classique des fraudes nigérianes ou des fraudes par avance de fonds, où les délinquants font miroiter à la victime des gains importants en échange

d'une mise de départ dont cette dernière ne reverra jamais la couleur. Le Web 2.0 permet cependant de personnaliser les approches en exploitant les informations personnelles dévoilées par les victimes sur leurs profils Facebook ou MySpace. De nombreux fraudeurs prennent ainsi le contrôle du profil de leurs victimes sur les sites de socialisation en ligne (à l'aide d'une application malveillante décrite dans le paragraphe précédent) et lancent un appel à l'aide aux membres du réseau de ces dernières en leur expliquant qu'ils se sont fait dérober toutes leurs possessions lors d'un voyage à l'étranger et qu'ils ont besoin du virement rapide de quelques centaines ou milliers de dollars pour pouvoir rentrer chez eux. Une requête similaire provenant d'un inconnu sera certainement ignorée, alors que les chances augmentent considérablement pour le fraudeur si elle émane d'un individu familier par le biais d'un canal privilégié de communication (dans la mesure où on a déjà approuvé ce profil au préalable).

Enfin, les contenus problématiques figurent dans notre base de données (10,5 % des incidents) pour deux types de risques qu'ils font peser sur les individus et les organisations. D'abord, les sites de socialisation en ligne constituent des outils privilégiés de dévoilement de la vie privée dont les retombées ne sont pas encore pleinement maîtrisées par leurs usagers et qui peuvent par conséquent donner lieu à des abus dommageables. L'exemple le plus symptomatique à ce titre est certainement celui de John Sawers, le nouveau chef du MI6 – les services très secrets de Sa Majesté – dont la vie privée (y compris son adresse résidentielle, celle de ses trois enfants et celle de ses parents) a été exposée à l'été 2009 sur Facebook par sa propre épouse. Celle-ci avait négligé de régler correctement les paramètres d'accès à son profil qui était par conséquent consultable par tous, conduisant à une transparence non seulement embarrassante, mais également dangereuse, pour un espion (Evans, 2009). Outre la révélation d'informations privées sur soi, plusieurs affaires concernent également des atteintes à la vie privée d'autrui, comme cette infirmière qui discutait sur sa page MySpace du profil médical de certains de ses patients (Sanchez, 2008). Dans un second temps, le Web 2.0 favorise la collision des sphères privées et professionnelles. Cela se traduit par exemple par des usagers qui partagent avec leurs « amis » l'opinion parfois peu flatteuse qu'ils ont de leur employeur, s'exposant ainsi à des mesures disciplinaires ou à un congédiement. Un autre type d'affaire rencontré est celui dans

lequel l'employé d'une organisation ou d'une administration nuit par ses propos racistes ou diffamatoires à la réputation de cette dernière, remettant ainsi en question sa légitimité.

3.3 Distribution des événements selon les sites du Web 2.0

Une deuxième stratégie de classification des incidents recensés dans notre étude consiste à examiner les sites du Web 2.0 les plus fréquemment associés aux incidents qui figurent dans notre base de données (tabl. 3.2). Le site de petites annonces Craigslist[8] arrive en première position avec 37,3 % des affaires (N = 255), suivi par MySpace (28,3 %, N = 193) et Facebook (15,8 %, N = 108). Twitter et YouTube, deux autres sites extrêmement populaires, ne représentent quant à eux que 8,2 % (N = 56) et 3,5 % (N = 24) de l'échantillon respectivement.

Ce « palmarès » ne peut cependant être interprété sur la seule base de la fréquence d'apparition des sites dans la base de données. En effet, un examen plus approfondi de la distribution des incidents laisse apparaître de grandes disparités.

Ainsi, certains sites comme Craigslist ou MySpace sont particulièrement exposés aux crimes sexuels. Mais alors que les victimes sont principalement de jeunes adultes dans le cas du site d'annonces (moyenne d'âge de 18 ans), la moyenne d'âge est de seulement 15 ans sur la populaire plateforme de socialisation en ligne. Facebook et Twitter semblent pour leur part être confrontés à des problématiques d'attaques informatiques : pour des raisons différentes (nombreuses applications non vérifiées disponibles sur Facebook et technique de raccourcissement et de masquage des liens sur Twitter), ces deux services offrent aux pirates informatiques des plateformes technologiques qui se prêtent parfaitement à la diffusion de logiciels malveillants. YouTube, exclusivement consacré au partage de vidéos en ligne, concentre enfin la moitié des incidents le concernant sur des cas de contenu problématique.

8. Bien qu'il ait été fondé en 1995, bien avant l'explosion du Web 2.0, Craigslist est généralement associé à la deuxième génération de sites Internet en raison des innovations technologiques introduites dans son interface et de son esprit communautaire, qui permettent aux usagers de publier directement et gratuitement leurs petites annonces (Wolf, 2009).

Tableau 3.2 Distribution des incidents par site

	Type d'incident							
	Crime sexuel	Attaque informatique	Atteinte à la personne	Contenu problématique	Fraude	Atteinte aux biens	Autre	Total
Craigslist (N = 255)	42,7 %	0,4 %	20,8 %	0,8 %	20,4 %	11,8 %	3,1 %	100,0 %
MySpace (N = 193)	64,8 %	1,0 %	12,4 %	15,5 %	3,1 %	2,1 %	1,0 %	100,0 %
Facebook (N = 108)	15,7 %	32,4 %	22,2 %	21,3 %	7,4 %	0,9 %	0,0 %	100,0 %
Twitter (N = 56)	1,8 %	87,5 %	1,8 %	3,6 %	1,8 %	0,0 %	3,6 %	100,0 %
Autre (N = 35)	31,4 %	48,6 %	11,4 %	5,7 %	0,0 %	0,0 %	2,9 %	100,0 %
YouTube (N = 24)	4,2 %	25,0 %	20,8 %	50,0 %	0,0 %	0,0 %	0,0 %	100,0 %
Bebo (N = 7)	42,9 %	28,6 %	14,3 %	14,3 %	0,0 %	0,0 %	0,0 %	100,0 %
MyYear-book (N = 5)	100,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	0,0 %	100,0 %

Plusieurs conclusions préliminaires peuvent être tirées de ces données : d'abord, il n'existe pas de corrélation dans notre échantillon entre le nombre d'incidents recensés et le nombre d'usagers revendiqué par les divers services impliqués. Ainsi, Craigslist, qui compte « seulement » une cinquantaine de millions de visiteurs mensuels[9], arrive en tête des incidents répertoriés, alors que le mastodonte Facebook ne figure qu'en troisième position malgré ses 400 millions de membres et ses

9. www.crunchbase.com/company/craigslist.

120 millions de visiteurs mensuels[10]. Ce décalage résulte certainement du fait que chaque plateforme du Web 2.0 est exposée à des risques particuliers qui sont directement reliés à sa fonction principale ainsi qu'à la technologie mise en œuvre. Par ailleurs, le fait que les utilisateurs de Facebook doivent se servir de leur vrai nom, contrairement à ceux de MySpace ou de Craigslist qui peuvent recourir à des pseudonymes, a peut-être pour effet de contrôler le sentiment d'anonymat et d'impunité qu'on peut ressentir à tort ou à raison sur ces deux derniers sites. Il est aussi fort probable que la prééminence des crimes sexuels pour les deux services les plus fréquemment mentionnés (Craigslist et MySpace) reflète un biais médiatique particulièrement friand de faits divers assaisonnés à la sauce technologique.

3.4 Profil démographique des suspects et des victimes

Une troisième façon d'analyser les crimes associés au Web 2.0 consiste à examiner les caractéristiques des victimes et des suspects impliqués. Bien que les sources médiatiques ne mentionnent pas systématiquement les éléments démographiques comme l'âge ou le genre, nous avons pu recueillir ces données pour plusieurs centaines d'individus (fig. 3.1).

Une rapide comparaison de l'âge des deux groupes montre que les suspects sont en moyenne plus âgés que les victimes de neuf ans, ce qui reflète certainement la proportion importante de crimes sexuels qui figure dans notre échantillon. Cette interprétation semble confirmée par l'examen de l'âge médian des victimes qui chute à 15 ans, ce qui signifie que la moitié des victimes recensées avaient 15 ans ou moins. Par contre, les suspects ne sont pas aussi âgés qu'on pourrait l'imaginer dans un tel contexte, ce qui est certainement attribuable à la jeunesse des utilisateurs de ces nouveaux médias. Ainsi, selon un sondage mené par le Pew Research Center, alors que 72 % des jeunes adultes (18 à 30 ans) américains utilisaient les sites de socialisation en ligne à l'automne 2009, la proportion d'utilisateurs tombait à 40 % chez les plus de 30 ans (Lenhart, Purcell, Smith et Zickuhr, 2010).

10. www.crunchbase.com/company/facebook.

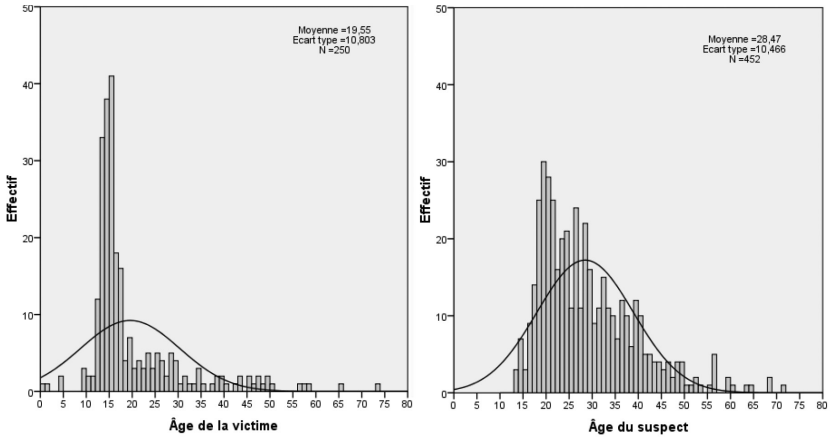

Figure 3.1 Nombre de victimes et de suspects impliqués dans les crimes associés au Web 2.0 selon l'âge

En ce qui concerne le genre, on observe que les incidents impliquent une majorité écrasante de suspects masculins (80 %) et de victimes féminines (73,4 %). Ces chiffres doivent cependant être interprétés avec prudence, car ils concernent majoritairement les crimes sexuels et les atteintes à la personne, pour lesquels le genre joue un rôle déterminant. Il est par contre beaucoup plus difficile de réduire les attaques informatiques ou les fraudes à des formes de crimes dirigés contre les femmes en particulier. Il n'en reste pas moins que cette disproportion entre la représentation des hommes et des femmes dans les crimes associés au Web 2.0 évoque une délinquance familière où l'innovation technologique joue un rôle accessoire dans un contexte malheureusement familier de violence.

3.5 Perspectives d'avenir

Ce chapitre a permis de présenter les résultats préliminaires d'une étude qui vise à mieux connaître les caractéristiques des crimes et des risques associés au développement de la deuxième génération d'applications Internet (le Web 2.0). Si les 15 premières années du Web ont été marquées par l'émergence des espaces numériques et la découverte de leur potentiel de diffusion de l'information, le Web 2.0 dénote l'intégration

des nouvelles technologies de l'information et de la communication dans chaque activité humaine, qu'il s'agisse du maintien de réseaux de socialisation étendus ou du partage d'expériences et de compétences personnelles avec autrui. À ce titre, la distinction entre les crimes traditionnels et les « cybercrimes » semble de moins en moins adaptée pour rendre compte de l'omniprésence d'Internet dans notre quotidien.

En effet, les analyses préliminaires menées sur une base de données qui s'enrichit chaque jour laissent entendre que les risques criminels et réputationnels dérivés du Web 2.0 transcendent la dichotomie classique entre crimes contre la personne et crimes numériques. De nombreux crimes contre la personne trouvent leur origine dans des liens tissés initialement en ligne ou sont déclenchés par des facteurs technologiques, alors que de plus en plus de fraudes et d'attaques informatiques s'appuient sur la confiance bien réelle existant entre des personnes appartenant aux mêmes cercles sociaux pour se propager et accroître leurs chances de réussite.

Il faut toutefois se garder de sombrer dans une peur irrationnelle au regard de ces transformations. En effet, si le nombre d'incidents que contient notre base de données peut sembler conséquent, il faut rappeler que les sites de socialisation en ligne jouissent d'une immense popularité et qu'ils comptent dans certains cas plusieurs centaines de millions d'usagers. Rien n'indique que la fréquentation de ces sites génère pour ces derniers (y compris les plus jeunes d'entre eux) des risques excessifs qui seraient individuellement et collectivement intolérables. Ainsi, pour ne prendre qu'un exemple, les inquiétudes relatives à la facilité avec laquelle les prédateurs sexuels pourraient identifier et contacter leurs victimes sur des sites comme MySpace donnent lieu à une frénésie réglementaire qui semble oublier que plus de 80 % des agressions sexuelles graves sur des enfants sont commises par des personnes connues (Hébert et coll., 2009).

Bibliographie

ALEXANDER, N. (2008). « Attorneys general announce agreement with MySpace regarding social network safety », *NAA Gazette*, vol. 2, nº 1 [En ligne] www.naag.org/attorneys_general_announce_agreement_with_myspace_regarding_social_networking_safety.php (consulté le 1er février 2010).

BERAN, T., et LI, Q. (2005). « Cyber-harassment : A Study of a New Method for an Old Behavior ». *Journal of Educational Computing Research*, vol. 32, nº 3, p. 265-277.

CISCO (2009). *Annual security report*, San Jose, Cisco Systems.

DENHAM, E. (2009). *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, Ottawa, Commissaire à la protection de la vie privée du Canada.

DUPONT, B., et GAUTRAIS, V. (2010). « Crime 2.0 : le web dans tous ses états! », *Champ Pénal : Nouvelle revue internationale de criminologie*, vol. VII [En ligne] champpenal.revues.org/7782 (consulté le 12 mars 2010).

EVANS, M. (2009). « Wife of Sir John Sawers, the future head of MI6, in Facebook security alert », *TimesOnline*, 6 juillet [En ligne] technology.timesonline.co.uk/tol/news/tech_and_web/article6644199.ece (consulté le 1er mars 2010).

HÉBERT, M., TOURIGNY, M., CYR, M., McDUFF, P., et JOLY, J. (2009). « Prevalence of childhood sexual abuse and timing of disclosure in a representative sample of adults from Quebec », *The Canadian Journal of Psychiatry*, vol. 54, nº 9, p. 631-636.

LENHART, A., PURCELL, K., SMITH, A., et ZICKUHR, K. (2010). *Social media and mobile internet use*, Washington, D.C., Pew Research Center.

MAAG, C. (2007). « When the bullies turned faceless », *The New York Times*, 16 décembre [En ligne] www.nytimes.com/2007/12/16/fashion/16meangirls.html (consulté le 3 février 2010).

NIELSEN (2009). *Global faces and network places : A Nielsen's report on social networking's new global footprint*, New York, Nielsen Company.

SANCHEZ, J. (2008). « MySpace gripe about patient sparks federal privacy complaint », *Ars Technica*, 7 décembre [En ligne] arstechnica.com/tech-policy/news/2008/12/myspace-gripe-about-patient-sparks-federal-privacy-complaint.ars (consulté le 1er mars 2010).

WOLF, G. (2009). « Why Craigslist is such a mess », *Wired Magazine*, vol. 17, septembre [En ligne] www.wired.com/entertainment/theweb/magazine/17-09/ff_craigslist?currentPage=all (consulté le 2 mars 2010).

YBARRA, M., et MITCHELL, K. (2007). « Prevalence and frequency of Internet harassment instigation : implications for adolescent health », *Journal of Adolescent Health*, vol. 41, nº 2, p. 189-195.