

**PROJET DE RECHERCHE PRÉSENTÉ DANS LE CADRE
DE L'OBTENTION DE LA BOURSE POSTDOCTORALE
DU CICC POUR L'ANNÉE 2010**

**PAR
CAROLINE VALLET**

MOTIFS DU STAGE POSTDOCTORAL

Ayant effectué un certificat en criminologie et un autre en sciences criminelles à l'Université de Panthéon-Assas à Paris II, ainsi que des études juridiques en droit criminel comparé, il semblait tout à fait logique que je continue mes recherches dans cette optique. L'idée d'explorer d'un point de vue plus criminologique l'évolution de la cybercriminalité et les nouveaux comportements développés par les nouvelles technologies de l'information correspond à mes préoccupations actuelles.

Mes études en droit criminel m'ont permis de comprendre certaines problématiques que je souhaiterais étudier lors d'un postdoctorat au Centre internationale de criminologie comparée (CICC). D'ailleurs, j'ai effectué la plupart de mes études en droit comparé ce qui justifie, en outre, mon choix.

En étant au CICC, je vais pouvoir mieux comprendre comment évoluent la cybercriminalité et ses nouveaux phénomènes de manière plus empirique. J'aimerais ainsi étudier ses nouveaux comportements que génère ce média pour dégager de éventuelles solutions et des moyens pour diminuer les risques potentiels de préjudices visiblement accentués par les internautes eux-mêmes. Le CICC semble être le lieu parfait pour mener à bien mon projet de recherche.

PROJET DE RECHERCHE

1) Problématique

Le réseau Internet, comme tout autre nouvelle technologie, possède une double face, une positive et une autre négative. En ce qui concerne la première, les internautes ont découvert un merveilleux moyen pour établir des relations sociales, professionnelles, voire amoureuses. Pour cela, ils ont tendance à exposer de manière assez exhibitionniste leur vie privée sans prendre de réelles précautions. Ils étalent ainsi toutes leurs pensées les plus intimes, leurs photographies personnelles ainsi que tous les événements de leur vie quotidienne. Ce phénomène peut se faire aussi bien de manière volontaire, telle que par exemple sur les sites populaires de *Facebook* ou de *MySpace*, que de manière involontaire, comme l'internaute qui fait une demande d'emploi sur un quelconque site d'embauche. Cet étalage s'explique notamment par le fait que les internautes pensent pouvoir facilement contrôler leurs données personnelles diffusées sur Internet. Or, il n'en est rien. En effet, ils ont tendance à oublier que ce vecteur est à vocation publique et mondiale.

Ces nouveaux comportements entraînent inévitablement certains risques plus ou moins prévisibles (D. PEPPERS et M. ROGERS). Cette exposition de la vie privée de chacun sur le réseau Internet, qui n'est que l'utilisation de sa liberté d'expression garantie par l'article 2 b) de la *Charte canadienne des droits et libertés*, possède deux facettes : « l'avantage des nouvelles technologies de l'information est de rendre visible, et son désavantage, ce qui est paradoxal, également de rendre visible » (S. COLL). Autrement dit, cette nouvelle tendance permet inévitablement la transparence de l'individu qui permet, d'une part, un meilleur contrôle des comportements adoptés sur Internet et, d'autre part, l'utilisation à mauvais escient des données personnelles ainsi mises à la disposition du public. Par conséquent, les cybercriminels y trouvent une véritable source d'inspiration pour commettre de nouveaux méfaits. Ils ont, en effet, accès sans difficulté à une masse importante de données personnelles d'un grand nombre de personnes sans prendre de véritables risques, contrairement au monde réel. En outre, des particuliers peuvent, en raison de la simplicité d'utilisation d'Internet et des risques

minimes pris du fait notamment de l'anonymat, commettre des infractions en récoltant facilement des données personnelles. En effet, les criminels ne sont plus forcément des professionnels. La confiance dont font preuve les utilisateurs du réseau en exposant leurs renseignements personnels, est clairement décelable malgré le manque de contrôle et de sécurité (W. CAPELLER; N. DAIGLE). Ils augmentent particulièrement leurs risques d'être victime. Pourtant, cela n'effraie pas les internautes qui continuent à faire preuve de transparence sur Internet.

Le concept de « vie privée » s'est donc nettement transformé (V. GAUTRAIS; D. PEPPERS et M. ROGERS). En effet, lui qui étant auparavant basé sur le secret, voilà qu'il tend vers son opposé. Le législateur, avec ces changements de comportements, a dû intervenir afin de prendre en compte ces nouveaux risques susceptibles d'engendrer de nouvelles victimes. C'est ainsi que de nouvelles infractions ont été créées, comme par exemple celle de l'usurpation d'identité, ou envisagées, telles que la cyberintimidation (*Projet de loi C-355*). Mais il est également important de signaler que cette tendance à l'exhibition de la vie privée a contribué au développement d'infractions de droit commun. Il s'agit par exemple de la fraude, de l'utilisation de l'image d'un individu sans son autorisation et des infractions à caractère sexuel comme la pédopornographie (art. 163.1 C.Cr.) et le leurre (art. 172.1 C.Cr.). D'ailleurs, les jeunes semblent les premières victimes de ses infractions vu qu'ils sont les principaux utilisateurs d'Internet mais également parce qu'ils représentent les personnes les plus vulnérables dans la société ainsi que les personnes âgées. Il semble donc clair que les personnes vulnérables, dans le monde réel ou virtuel, restent les cibles favorites des délinquants. C'est pour ces différentes raisons qu'il est intéressant de se poser la question suivante à savoir quel est le rapport entre l'exposition de plus en plus importante de la vie privée grâce au réseau Internet et le développement de certaines formes de cybercriminalité? Autrement dit, la transparence des données personnelles telles que diffusées sur les réseaux sociaux n'est-elle pas un facteur de risque? N'est-ce pas un facteur accentué de victimisation?

Notre étude traite d'un sujet d'actualité qui suscite indéniablement l'engouement des pouvoirs publics ainsi que des internautes. Toutefois, leurs objectifs étant différents, voire même contradictoires. En effet, l'un souhaite nettement répondre aux attentes de sécurité demandées alors que les autres préfèrent continuer à rendre leur vie privée

publique. Autrement dit, les utilisateurs, le plus souvent jeunes, préfèrent livrer ses données personnelles plutôt que de se préoccuper des risques que cela peut produire. D'ailleurs, la plupart sont conscients qu'ils s'exposent à certains dangers. Une gestion du risque est donc effectuée (P. LANDREVILLE et G. TROTTIER). Mais, il semblerait que la facilité procurée par Internet et son aspect ludique l'emportent sur les risques potentiels auxquels ils peuvent s'exposer. Ce choix est surprenant puisqu'il est clair que dans le monde réel, il en irait différemment. Effectivement, les gens se protègent beaucoup plus dans la vraie vie que dans le monde virtuel. Pourquoi cette différence? Est-ce que la vie privée a moins de valeur sur Internet que dans le monde réel? Est-ce qu'elle peut exister réellement sur ce média à vocation publique? Dans tous les cas, nous sommes confrontés, d'un côté, aux risques engendrés par ce dévoilement de la vie privée, en particulier intime et, d'un autre côté, aux mécanismes de protection mis en place et de plus en plus demandés par la société. Un paradoxe s'entrevoit aisément.

2) Objectifs

Notre travail consiste à démontrer le fait que les internautes en dévoilant leur vie privée sur Internet, notamment sur les réseaux sociaux, s'exposent à de nombreux risques comme celui d'augmenter celui d'être victime d'une infraction. C'est ainsi que nous essayerons de mettre en exergue le fait que cette exposition de la vie privée contribue aux développements de certaines infractions.

En outre, nous souhaitons démontrer que les internautes et plus particulièrement les jeunes ont tendance à s'exposer plus facilement aux risques et en connaissance de cause la plupart du temps ce qui les rend, par ailleurs, plus vulnérables. Ils font d'Internet la vitrine de leur vie.

Enfin, nous voulons comprendre pourquoi les utilisateurs d'Internet s'exposent plus facilement à des risques sur Internet? Ce réseau a-t-il un aspect plus rassurant et confiant que la vie réelle, pouvant alors expliquer cet étalage de détails privés?

3) Méthodologie

Pour vérifier nos hypothèses, nous allons utiliser différentes méthodes pour collecter les documents pertinents. La première est traditionnelle puisqu'il s'agit de l'observation documentaire. C'est ainsi que nous allons analyser aussi bien des documents juridiques que non-juridiques tels que criminologiques, politiques ou sociologiques. Pour ce faire, nous allons étudier des textes législatifs de différents pays en nous limitant toutefois à 3 ou 4 afin de confronter les pays de droit civil à ceux de common law; les décisions judiciaires; les rapports gouvernementaux ou non; les recommandations; les pratiques professionnelles; les articles de doctrines; les monographies et autres recueils. Il sera également intéressant de prendre en compte certains articles de presse, de périodiques, de revues, de colloques et de séminaires. Par conséquent, la plupart des documents proviendront de plusieurs sources qui seront essentiellement officielles. De plus, l'étude de statistiques sera également un élément important à analyser pour mener à bien notre recherche.

Enfin, la seconde méthode s'effectuera par le biais d'entretiens qui viendront soit corroborer notre thèse, soit, au contraire la réfuter. Dans tous les cas, ils vont venir s'assurer du bien fondé de nos conclusions mais également, des grands axes choisis dans notre recherche. Les répondants seront *a priori* des policiers traitant de la cybercriminalité, des procureurs de la Couronne ainsi que des particuliers utilisant habituellement les réseaux sociaux.

4) Échéancier

Vu que le stage postdoctoral s'effectue sur une année, nous pensons que les premiers mois serviront à vérifier certaines de nos hypothèses de départ à partir de l'observation documentaire. Les premiers résultats obtenus pourraient aboutir à la rédaction d'un article afin de les exposer.

La deuxième étape serait de répondre clairement à nos interrogations par les entretiens et l'usage de statistiques pour, peut être, formuler de nouveaux concepts. Un autre article pourrait être rédigé.

Pour enfin, faire une seconde série d'entretiens, pour appuyer notre recherche et ainsi la terminer afin d'exposer et comparer, dans un dernier article, les résultats obtenus tout au long de notre étude.

La mise en place d'une conférence sur ce thème pourrait également être envisagée dans le but de confronter les différents points de vue sur ce sujet d'actualité.

5) Références

Législation

Charte canadienne des droits et libertés, partie I de la *Loi Constitutionnelle de 1982* [annexe B de la *Loi de 1982 sur le Canada* (1982, R.-U., c. 11)].

Code criminel, L.R.C. (1985), c. C-46, mod. par L.R.C. (1985), c.2 (1^{er} supp.).

Code pénal français, 104^e édition, Paris, Dalloz, 2007.

Convention sur la cybercriminalité, STE n°185, Budapest, 23 novembre 2001, en ligne sur : [Site du Conseil de l'Europe <http://conventions.coe.int/Treaty/FR/Cadreprincipal.htm>](http://conventions.coe.int/Treaty/FR/Cadreprincipal.htm)

Loi modifiant le Code criminel (protection des enfants et d'autres personnes vulnérables) et la Loi sur la preuve au Canada, L.C. 2005, c.32.

Projet de loi C-27 : Loi modifiant le Code Criminel, (vol d'identité et inconduites connexes), Ministre de la Justice, l'hon. Robert Douglas Nicholson, 39^{ème} législature, 2^{ème} session, 16 oct. 2007 – 7 sept. 2008, en ligne sur : <http://www.parl.gc.ca/legisinfo/index.asp?Language=F&query=5333&Session=15&List=toC>.

Projet de loi C-355, Loi modifiant le Code criminel (cyberintimidation), 2^e session, 40^e législature, 57-58 Elizabeth II, première lecture le 1^{er} avril 2009.

Projet de loi n°1697 d'orientation et de programmation pour la performance de la Sécurité intérieure, Assemblée Nationale, 13^{ème} législature, 27 mai 2009, en ligne sur : http://www.assemblee-nationale.fr/13/dossiers/lopsi_performance.asp.

Monographies et recueils

AUSTIN Lisa, Arthur COCKFIELD et Patrick A. MOLINARI, *Technology, privacy and justice = Technologies, vie privée et justice*, Montréal, Canadian Institute for the Administration of Justice = Institut canadien d'administration de la justice, 2006.

BAUDRY Patrick, Claude SORBETS et André VITALIS (dir.), *La vie privée à l'heure de médias*, Pessac : Presses universitaires de Bordeaux, 2002.

BECK Ulrich, *La Société du risque - Sur la voie d'une autre modernité*, Paris, Flammarion, 2003.

BECOURT Daniel, *Image et vie privée*, Paris, L'Harmattan, 2004.

BLANCHARD Marc-André et Florence LUCAS, «Divertir la liberté d'expression», dans Service de la formation permanente, Barreau du Québec, vol. 208, *Développements récents en droit du divertissement*, Cowansville, Éditions Yvon Blais, 2004, p.31 -59.

BORRILLO Daniel et Danièle LOCHAK (dir.), *La liberté sexuelle*, Paris, PUF, 2005.

CAPELLER Wanda, « Un net pas très net – Réflexions sur la criminalité virtuelle », dans, Angel SANCHEZ DE LA TORRE et al., *Le droit et l'immatériel*, Archives de philosophie du droit, CNRS, Tome 43, Paris, Sirey éd., 1999, pp. 167-185.

DUBOS Olivier et Jean-Pierre MARGUENAUD (dir.), *Sexe, sexualité et droits européens : enjeux politiques et scientifiques des libertés individuelles*, Paris, Éditions A. Pedone, 2007.

DUCLOS Denis, « Puissance et faiblesse du concept de risque », (1996) 46 *L'année sociologique*, n°2, pp.309-337.

ERICSON Richard V. et Kevin D. HAGGERTY, *Policing the Risk Society*, Toronto, University of Toronto Press, 1997.

HOUZIAUX Alain (dir.), *La liberté sexuelle jusqu'où?*, Paris, Les Éditions de l'atelier/Les Éditions Ouvrières, 2005.

LEPAGE Agathe, *Libertés et droits fondamentaux à l'épreuve de l'Internet : Droits de l'internaute, Liberté d'expression sur l'Internet, Responsabilité*, Paris, Litec, 2002.

MARTIN Daniel et Frédéric-Paul MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, PUF, 2001.

PINI Joseph et autres, *Le sexe, la sexualité et le droit*, Paris, Édition Pierre Téqui, 2002.

POULLET Yves, Cécile de TERWANGNE et Paul TURNER, *Vie privée : nouveaux risques et enjeux = Privacy : new risks and opportunities*, Namur, CRID, Facultés universitaires Notre-Dame de la Paix de Namur, E. Story-Scientia, 1997.

Articles de périodiques, de revues et de presse

DEBET Anne, «Internet et vie privée : la protection et la liberté du mineur internaute», *Comm. com. électr. déc.* 2005. n°40, 11-17.

DUFIEF Vincent, « La vie privée sacrifiée sur l'autel des réseaux sociaux », 20 novembre 2007, *Écrans, Libération*, en ligne sur : <<http://www.ecrans.fr/La-vie-privee-sacrifiee-sur-l-2606.html>>.

FRANCESCON I., « Les nouvelles techniques d'information et de communication et leur exploitation à des fins illicites. L'exemple des activités touchant à la pornographie dure dans l'Internet », (1996) *Revue Internationale de criminologie et de police technique* 61-68, n°1.

GRABOSKY Peter, Russell G. SMITH et Paul WRIGHT, « Nouvelles technologies, nouveaux délits », (4e trimestre 1998) 34 *Les Cahiers de la sécurité intérieure*, 13-29.

LANDREVILLE Pierre et Germain TROTTIER, « La notion de risque dans la gestion pénale », (2001) 34 *Criminologie*, n°1, pp. 3-8, en ligne sur : <<http://id.erudit.org/iderudit/004754ar>>.

LASCOURMES Pierre, « La précaution comme anticipation des risques résiduels et hybridation de la responsabilité », (1996) 46 *L'année sociologique*, n°2, pp.359-382.

LAUTMAN Jacques, « Risque et rationalité », (1996) 46 *L'année sociologique*, n°2, pp.273-285.

PRATT John, « Dangerosité, risque et technologie du pouvoir », (2001) 34 *Criminologie*, n°1, pp.102-121, en ligne sur : <<http://www.erudit.org/revue/crimino/2001/v34/n1/004756ar.pdf>>.

ROUILLÉ-MIRZA Ségolène et Éric BARBRY, « Nouveaux moyens de communication, protection des mineurs et mesures techniques », (2007) 37 *Légicom* 69-75, p.71.

VINCENT Catherine, « Vie privée sur Internet : la polémique Facebook », (20 Février 2009) *Le monde*.

WOLAK Janis, David FINKELHOR et Kimberly MITCHELL, « Trends in arrests of « online predators » », (30 mars 2009) *Crimes against children research center*, CV194_FINAL NJOV2, en ligne sur : <<http://www.unh.edu/ccrc>>.

Articles électroniques

BARBRY Éric, *La fin de l'anonymat sur Internet : La loi relative à la sécurité quotidienne a rappelé le principe général d'anonymisation. Mais la réalité est bien différente*, 11 juin 2002, en ligne sur : le Journal du Net <<http://www.journaldunet.com/juridique/juridique020611.shtml>>.

COLL Sami, *Révolution sexuelle et libération de l'information: affaiblissement ou renforcement du contrôle social?*, 14 avril 2009, en ligne sur : <<http://www.internetactu.net/2009/04/14/revolution-sexuelle-et-liberation-de-l%E2%80%99information-affaiblissement-ou-renforcement-du-contr%C3%B4le-social/>>.

CONGRÈS MONDIAL CONTRE L'EXPLOITATION SEXUELLE COMMERCIALE DES ENFANTS, *Mondialisation et incitation à consommer*, Yokohama, 2001, en ligne sur : <<http://www.csecworldcongress.org/fr/index.htm>>.

GAUTRAIS Vincent, « Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle », (hiver 2004) 9 *Lex Electronica* n°2, en ligne sur : <<http://www.lex-electronica.org/articles/v9-2/gautrais2.htm>>.

PEPPERS Don et Martha ROGERS, *The Societal Benefits of Data Sharing*, 20 janvier 2009, en ligne sur: <<http://www.1to1media.com/View.aspx?DocId=31350>>.

RÉSEAU ÉDUCATION-MÉDIAS, « Apprendre aux jeunes à protéger leur vie privée sur les sites commerciaux », en ligne sur : <http://www.education-medias.ca/francais/parents/internet/jeunes_vendre_parents/apprendre_jeunes_vie_privée_par.cfm>.

Rapports et documents

ALLIOT-MARIE Michèle, *Lutte contre la cybercriminalité*, Intervention de la Ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, 14.02.2008, en ligne sur : <http://www.interieur.gouv.fr/sections/a_l_interieur/le_ministre/interventions/lutte-cybercriminalite?print_page:int=1>.

BRETON Thierry, *Chantier sur la lutte contre la cybercriminalité*, Paris, Ministère de l'Intérieur, de la sécurité intérieure et des libertés locales, 2005, en ligne sur : <http://www.interieur.gouv.fr/rubriques/c/c2_le_ministere/c21_actualite/2005_04_13_dossier_presse_cybercriminalite/rapport_breton.pdf>

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *Internet et la collecte des données personnelles auprès des mineurs*, 12 juin 2001, présenté par Cécile ALVERGNAT, en ligne sur : <<http://www.cnil.fr/fileadmin/documents/approfondir/rapports/mineurs.pdf>>.

INSTITUT DE STATISTIQUE DE L'UNESCO, *Mesurer l'état et l'évolution de la société de l'information et du savoir : un défi pour les statistiques*, Sommet mondial sur la société de l'information (SMSI), Montréal, 2003, en ligne sur : site de l'UNESCO <http://www.uis.unesco.org/ev_fr.php?ID=5504_201&ID2=DO_TOPIC>.

OCDE, *Protection de la vie privée en ligne : orientations politiques et pratiques*, Paris, Organisation de coopération et de développement économiques, 2003.

THE BERKMAN CENTER FOR INTERNET ET SOCIETY AT HARVARD UNIVERSITY, *Enhancing Child Safety et Online Technologies : Final report of the Internet safety technical task force to the Multi-State working Group on Social Networking of State Attorneys General of the United States*, New York, Berkman Center for Internet & Society at Harvard University, 31 décembre 2008, en ligne sur : <<http://cyber.law.harvard.edu/pubrelease/isttf/>>.

THE NATIONAL CAMPAIGN TO PREVENT TEEN AND UNPLANNED PREGNANCY ET COSMOGIRL.COM, *Sex and tech: Results from a survey of teens and young adults*, 2008, en ligne sur: <www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf>.

Séminaires, Colloques, conférences et allocutions

DAIGLE Nathalie, *Un environnement sans confiance, c'est un arbre sans fruits - Comment contrôler la mise en œuvre des politiques de protection des renseignements personnels et cultiver la confiance dans les environnements électroniques*, Conférence *Confiance et environnements électroniques*, Chaire L.R. Wilson sur le droit des

technologies de l'information et du commerce électronique, Montréal, 20 novembre 2008, en ligne sur : <<http://www.chairelrwilson.ca/documents/Daigle.pdf>>.

GAUTRAIS Vincent, *Introduction générale : Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle*, Conférence *Vie privée et interconnexions : vers un changement de paradigme?*, Conférence organisée par le Programme international de coopération scientifique (CRDP / CECOJI), Ivry sur Seine, 5 juin 2003, en ligne sur:< <http://www.lex-electronica.org/articles/v9-2/gautrais2.pdf> >.

TRUDEL Pierre, « Vers de nouvelles approches pour garantir la protection de la vie privée dans un monde en réseaux », dans Colloque *Devenir, aujourd'hui, l'avocat de demain!*, Legal IT, Droit et technologies de l'information, Montréal, Éditions Yvon Blais, 21 avril 2008, pp.1-25.

Travaux, Mémoires et Thèses

BLANCHETTE François, *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, Mémoire de maîtrise, Montréal, Faculté de droit, Université de Montréal, 2001, en ligne sur : <<http://www.juriscom.net/uni/visu.php?ID=425>>.

HAMON Arnaud, *Une approche de la liberté d'expression sur Internet*, Mémoire de DEA Droit de l'homme et libertés publiques, Paris, Université de Paris X Nanterre, 2000, en ligne sur : Juriscom.net <<http://www.juriscom.net/uni/mem/14/presentation.htm>>.

JOLICOEUR Pénélope, *Conséquences d'une redéfinition du concept de vie privée sur l'environnement informationnel propre aux étudiants fréquentant une institution d'enseignement supérieur*, Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maître en Droit des Technologies de l'Information", Thèse (L. L. M.) --Université de Montréal, 2006.

JOUGLEUX Philippe, *La criminalité dans le cyberspace*, Mémoire de DEA Droit des Médias, Aix-Marseille, Faculté de droit et de science politique, Université de droit, d'économie et des sciences d'Aix-Marseille, 1999.