Rapport évolutif

Réseaux sociaux sur Internet et sécurité de la vie privée

Monica Tremblay, M. Sc.
Anthropologue

Laboratoire d'étude
sur les politiques publiques
et la mondialisation

Analyse des impacts de la mondialisation sur la sécurité - Rapport 9
Septembre 2010

ENAP
L'Université de l'administration publique

INTRODUCTION

Les sites de réseau social font partie du quotidien de bien des individus répartis un peu partout sur la planète. Un des plus connus, Facebook, dépassait le cap des 500 millions d'utilisateurs, en juillet 2010, soit l'équivalent de la population de l'Union européenne. Sur ces sites, les utilisateurs dévoilent, comme bon leur semble, des informations relatives à leur vie privée. Le phénomène est certes fort intéressant, mais parallèlement à l'engouement qu'il suscite, il soulève des inquiétudes en matière de sécurité et de vie privée.

La protection des renseignements personnels[1] et de la vie privée[2] suscitent des inquiétudes à l'heure où la circulation de l'information peut se faire en un clic de souris, d'un bout à l'autre du monde. On craint pour la sécurité des personnes et le respect de leur vie privée, voire de leur liberté. Des informations peuvent être recueillies à des fins criminelles ou malveillantes. Dès que l'information est lancée sur Internet, il devient difficile d'en garder le contrôle.

Le Québec, sa population et ses organisations tant privées que publiques, n'échappent pas à l'engouement des sites de réseau social (SRS), pas plus qu'aux préoccupations qu'ils font naître. Comme le rappelait le Président de la Commission d'accès à l'information du Québec, en mai 2010 lors des Journées des réseaux institutionnels de la Francophonie dans une conférence portant sur *La protection des droits dans un contexte de mondialisation*, « les renseignements diffusés sur les SRS sont accessibles comme s'ils étaient affichés dans un lieu public ». Un grand nombre de personnes peut en prendre connaissance sans que nous en soyons informés. Cela augmente donc le risque que des informations personnelles soient utilisées à tort entraînant ainsi des conséquences fâcheuses. Peu d'études permettent d'avoir une idée de l'ampleur du non-respect des lois de protection des renseignements personnels.

Les organisations gouvernementales, les entreprises, les ONG, tendent de plus en plus à utiliser les moyens mis à leur disposition sur Internet afin d'entrer en relation avec leur public. Les SRS s'avèrent donc une avenue intéressante, mais cette possibilité s'accompagne de questions et soulève des enjeux sur l'utilisation des renseignements personnels et la protection de la vie privée.

Ce rapport traite du phénomène des SRS et de leur impact en matière de vie privée. Il offre des précisions sur ces sites, notamment à propos des avantages et inconvénients de leur utilisation au regard de la sécurité et de la vie privée. Il montre ensuite de quelle manière les organisations internationales et nationales se penchent sur le phénomène et les préoccupations qu'il provoque. On expose enfin les moyens déployés par les autorités responsables de la protection de la vie privée afin de contrer les risques en la matière.

1. WEB 2.0, MÉDIAS SOCIAUX ET SITES DE RÉSEAU SOCIAL

Les sites de réseau social (SRS) s'inscrivent dans ce qui est communément qualifié de web 2.0. Cette appellation sert à désigner des outils qui permettent à l'internaute de mettre en ligne des données (vidéo, musique, texte, image), de dialoguer avec d'autres internautes et de donner son opinion sur divers sujets. Ces outils sont généralement offerts gratuitement à l'internaute. Ils sont financés par des revenus publicitaires. Les médias sociaux tels que forums, blogues, wikis, réseaux sociaux en sont des exemples.

Avec ces nouveaux outils, l'internaute a modifié son approche de l'Internet. Il ne se satisfait plus de recueillir des informations, d'obtenir des services précis en posant des questions à une organisation par l'entremise du courrier électronique ou en effectuant des transactions en ligne. Il peut maintenant rendre publique son opinion, la partager avec d'autres internautes ou avec les entreprises et organisations publiques avec qui il traite. L'internaute a la possibilité de participer à la création des informations qui se trouvent sur Internet. N'importe quel musicien peut se filmer, mettre sa vidéo sur MySpace ou YouTube et partager avec tout internaute quelques techniques de son art.

Cette évolution des applications disponibles et de la relation de l'internaute à l'Internet a également des répercussions sur le marketing et la publicité. La publicité devient plus ciblée, plus personnalisée et s'adapte davantage au contexte de navigation de l'usager, utilisateur occasionnel ou régulier, par exemple. Pour ce faire, une bonne connaissance du profil de la clientèle est nécessaire. Ce besoin de connaissance des usagers fait naître la crainte d'une atteinte possible à la vie privée, notamment lorsque des SRS autorisent des tiers à obtenir les renseignements sur ceux-ci[3].

Compte tenu de la grande diversité de médias sociaux et des particularités de chacun, ce rapport cible uniquement les réseaux sociaux.

1.1 Caractéristiques des sites de réseau social

Un site de réseau social est

> un service web qui permet à une personne (1) de créer un profil public ou partiellement public au sein d'un système délimité, (2) de dresser la liste des autres utilisateurs avec lesquels elle est en relation, et (3) de voir et de parcourir sa liste de relations et celle d'autres utilisateurs du système (Boyd et Ellison *in* Barrigar, 2010 :4).

Ces sites structurent et révèlent des réseaux sociaux établis ou en développement. Ils relient des individus désirant partager leurs intérêts, leurs activités et certains renseignements. Ils offrent aussi un moyen aux individus de communiquer et d'interagir entre eux de manière virtuelle, à l'aide de différents outils en ligne (messagerie instantanée, blogues, etc.). Ils se distinguent ainsi des sites de réseautage social en ce qu'ils ne servent pas principalement à créer de nouveaux liens.

Dans les SRS, les informations sont versées de manière volontaire, selon le désir et le choix de l'utilisateur - contrairement aux organisations publiques ou privées qui recueillent des renseignements personnels afin d'offrir un service ou d'assurer leur sécurité et, dans certains cas, celle de l'État. Chacun est libre d'adhérer ou pas à un réseau social et d'y dévoiler les informations qu'il juge pertinentes aux personnes de son choix. Les informations peuvent être divulguées à tous les Internautes participant au réseau ou réservées à un groupe restreint.

Malgré la liberté de chacun d'adhérer ou non à un SRS et de diffuser l'information qu'il lui plaît, les administrateurs de ces sites doivent s'engager à protéger les renseignements personnels et la vie privée de leurs participants. Généralement, ces derniers sont informés de l'utilisation qui sera faite des données, grâce à la publication de politiques de confidentialité. Les SRS offrent aussi à leurs utilisateurs des options permettant de protéger leur vie privée, à divers degrés. De plus, les lois et politiques en vigueur dans de nombreux pays visant à protéger la vie privée des personnes s'appliquent également. De telle sorte que

les règles de collecte, de conservation, d'accès, de divulgation, d'archivage et de destruction des données peuvent faire l'objet d'enquête par les autorités responsables de la protection de la vie privée. Néanmoins, des risques d'atteinte à la vie privée des utilisateurs semblent subsister.

1.2 Les acteurs des sites de réseau social

Toutes sortes d'individus, de provenances diverses, font partie des sites de réseau social. Il est possible d'y retrouver presque n'importe quelle personne, indépendamment de sa situation ou de son statut dans la société. Les SRS permettent d'entrer en contact avec de nombreuses personnes et d'avoir accès à leurs informations en autant qu'elles fassent partie d'un même réseau social.

Selon une étude internationale de Nielsen (2009) sur l'utilisation des réseaux sociaux, 67% des internautes d'Autriche, du Brésil, du Chili, du Danemark, d'Espagne, de France, d'Italie, du Royaume-Uni et des États-Unis se trouvent sur un « site de socialisation en ligne ». Ce qui signifie, par exemple, qu'un individu peut communiquer au même moment, une même information, avec une personne en Italie et une autre au Brésil.

Au Canada au cours de l'année 2009, selon l'enquête annuelle réalisée par la firme de sondage Ipsos Reid, 56% des internautes ont un profil sur un site de réseau social (89% des personnes ont accès à Internet au Canada et 82% au Québec). Le plus populaire d'entre eux est, sans surprise, Facebook qui réunit 85% de ces adeptes de réseau social.

Outre les individus, différentes organisations, notamment les entreprises, peuvent souhaiter s'afficher sur les SRS. Il en va de même pour les organisations publiques et les organisations non gouvernementales. Ce moyen de communication permet de joindre en quelques secondes des centaines de personnes. Cela crée un environnement intéressant pour les entreprises qui désirent faire de la promotion, peu importe où elles se trouvent sur la planète. Elles le font parfois en créant une page sur un SRS que les utilisateurs consultent ou en diffusant de la publicité sur les réseaux. Les attraits des SRS sont bien entendu différents pour les organisations et les individus.

2. ATTRAITS ENVERS LES SITES DE RÉSEAU SOCIAL

2.1 Pour les individus

De manière générale, les médias sociaux procurent des avantages aux utilisateurs. Les sites de réseau social (SRS) ne font pas exception. Ils apparaissent désormais comme un moyen de communication presque incontournable pour les internautes. Ils permettent aux parents, amis et collègues d'avoir plus d'interactions à l'aide de messages instantanés, de blogues et des informations diffusées dans leur description ou « profil », notamment des photos et des vidéos. L'avantage qu'ils présentent dans le maintien des relations est généralement apprécié, particulièrement des étudiants (Krasnova *et al*, 2010). Ils peuvent informer rapidement plusieurs amis de leurs activités quotidiennes.

Avec les SRS, les distances n'existent plus. Retrouver des personnes et rester en contact avec elles d'un bout à l'autre de la planète est aisé. Les SRS permettent aussi de regrouper des utilisateurs autour de préoccupations communes : partager des connaissances, acheter des biens ou des services, ou encore organiser en ligne leur vie sociale ou politique. Ils peuvent aussi

s'avérer un outil pratique afin de planifier un voyage personnel ou d'affaires. Ainsi, outre les relations entre véritables amis, les SRS autorisent aussi à tisser des liens avec de purs inconnus parce qu'ils sont amis d'amis, etc. qui partagent des intérêts communs. Cette réalité est d'ailleurs la source de plusieurs problèmes relatifs à la vie privée ou même à la diffamation.

Réseaux sociaux populaires

Il existe de nombreux sites de réseau social, chacun avec ses particularités. Les plus populaires sont brièvement présentés en encadrés dans ce document, selon les données disponibles le 25 août 2010.

Classmates - Créé en 1995. Il est le premier site de réseau social. Il permet de retrouver et de reprendre contact avec d'anciens camarades de classe. L'inscription est gratuite et autorise la création du profil personnel, mais la communication entre membres requiert des frais annuels. Conçu aux États-Unis, le site a maintenant des ramifications au Canada, en France sous le nom de **trombi**, en Autriche, en Allemagne et en Suède : **stayFriends**. L'information est conservée aux États-Unis et par conséquent la protection des données est régie par les lois américaines. Difficile de connaître le nombre de membres.

LiveJournal - Créé en 1999. Ce site de communication oscille entre le blogue et le réseau social. Il permet à ses membres d'établir leur profil, de créer des journaux web et dresser une liste d'amis avec qui ils peuvent partager ces informations. Principalement utilisé aux États-Unis, en Russie, au Royaume Uni et au Canada. LiveJournal Inc. compte 27 413 305 de membres dont 17 millions sont réellement actifs.

Copains d'Avant - Créé en 2001. Service du site L'Internaute Magazine, il est le premier site de réseau social français. Il permet de retrouver et de reprendre contact avec d'anciens camarades de classe. Les personnes inscrites définissent leur profil et peuvent envoyer des courriels, consulter les profils et faire des recherches par mots clés. Une autorisation est demandée à l'utilisateur si une personne qui n'est pas dans son réseau immédiat lui envoie un courriel. Les données sont protégées par la Directive européenne de 1995. Compte 12 millions de membres.

Friendster - Créé en mars 2002. Principalement utilisé en Asie. Il permet à l'Internaute, invité par un membre à l'aide d'un courriel, de créer son profil. Les contacts sont permis uniquement entre membres d'un même réseau. Depuis février 2009 ce site autorise les transferts d'argent entre ses utilisateurs, particuliers et entreprises, sans sortir du site. La transaction doit être validée sur son téléphone portable. Compte plus de 115 millions de membres.

Hi5 - Crée en 2003. Offre à l'internaute de définir son profil afin de rencontrer ses amis en ligne et se divertir. Pour être ajouté à la liste d'amis, une demande doit être faite par courriel. Le réseau comporte trois niveaux : les amis directs, les amis des amis, et les amis des amis des amis. Le profil d'un utilisateur peut être public ou seulement diffusé dans son réseau, c'est-à-dire aux 3 niveaux. Ce site permet de se doter d'un avatar (apparence que prend un internaute dans un univers virtuel). Dès sa création, ce site a visé un public international et s'avère populaire surtout auprès des hispanophones. L'accès aux renseignements personnels peut être configuré par l'utilisateur. Il compte plus de 50 millions de visiteurs uniques par mois.

LinkedIn – Créé en mai 2003. Ce site est destiné à enrichir le réseau professionnel de ses utilisateurs. Ces derniers établissent et mettent à jour la liste des personnes avec qui ils entretiennent des relations professionnelles. Comme Hi5 il utilise 3 niveaux afin de développer les relations. Ce réseau permet, entre autres, d'obtenir des informations sur des offres d'emploi. Il compte plus de 75 millions de membres dans plus de 200 pays.

Krasnova *et al* (2010), dans une étude portant sur les motivations de divulgation d'information sur les SRS, constatent que la personnalisation des présentations incite à participer aux réseaux en ligne. En général, les utilisateurs tentent de donner une bonne impression d'eux. Différentes études soulignent l'importance que les utilisateurs accordent à la gestion de leur identité et à leur réputation en ligne. En effet, chacun choisit les informations qu'il intégrera à son profil et celles qu'il ne souhaite pas diffuser. Torloting (2006), dans un ouvrage intitulé *Enjeux et perspectives des réseaux sociaux*, prétend que ces sites, outre la visibilité qu'ils offrent aux individus, leur permettent de gérer ce qu'il appelle leur « extimité » c'est-à-dire, contrôler l'intimité extériorisée dans ce lieu public en ligne.

Les SRS servent de divertissement. Pour plusieurs utilisateurs, ils s'avèrent un passe-temps qui aide à chasser l'ennui, relaxer et s'amuser.

Les SRS favorisent aussi la liberté d'expression, augmentent la diffusion d'opinions diverses et, par conséquent, peuvent s'avérer un moyen d'enrichir les débats politiques et sociaux (OCDE, 2007). L'utilisation d'un SRS s'avère un moyen de favoriser la participation plus directe des citoyens dans le débat public. Au Pays-Bas, le site SchaduwKamer, en lien avec le réseau social Hyves, permet aux jeunes de s'exprimer sur les initiatives politiques. Pour s'inscrire, les personnes doivent dévoiler pour qui elles ont voté lors des dernières élections. Dès lors, elles sont autorisées à donner leur avis et à se prononcer sur des projets de loi[4]. Cette expérience fera sans doute l'objet d'études; elle risque de soulever des interrogations en matière de protection de la vie privée, qu'il sera intéressant de suivre à long terme.

2.2 Pour les organisations

Selon certains gestionnaires, les SRS sont incontournables et indispensables aux entreprises. Ces réseaux constituent un média supplémentaire et peu coûteux de diffusion d'information, notamment parce que les internautes aident à véhiculer les informations (Balagué et Fayon, 2010). Le dernier sondage canadien de la firme Ipsos Reid (2010 :3) signale aussi qu'« À l'époque actuelle, une stratégie de médias sociaux est indispensable » [Trad. libre].

Selon la Commission européenne, la création de SRS ne requiert pas d'investissements massifs. Il apparaît en ce sens facile pour une entreprise d'investir ce marché pouvant lui apporter des avantages concurrentiels. Les SRS offrent une nouvelle façon de faire des affaires, notamment en permettant aux entreprises d'interroger facilement les consommateurs à propos de leurs produits. De plus, les SRS influencent aussi les méthodes de recrutement de personnel et de publicité. Le site LinkedIn est un réseau professionnel qui permet notamment d'être informé d'offres d'emploi. Les SRS sont des bases de données qui peuvent permettre aux entreprises de cibler les internautes lors d'une campagne commerciale, selon leurs intérêts. Il faudra néanmoins que les SRS et les organisations trouvent la manière d'exploiter ces informations personnelles de la manière la moins intrusive possible.

Les organisations gouvernementales peuvent également bénéficier de ces avantages. Selon l'agence responsable de l'utilisation des SRS au sein du gouvernement de la Caroline du Nord (États-Unis), la présence sur les réseaux sociaux est perçue comme une preuve de communication transparente. D'ailleurs, les informations partagées sur ces sites constituent de l'information publique au sens de la loi d'accès à l'information de cet État. Être présent sur un SRS permet

de plus d'améliorer l'interaction entre une organisation publique et les citoyens. Un document du Central Office of Information (COI), du Royaume-Uni, sur l'attrait des médias sociaux en général, précise qu'ils favorisent une meilleure communication avec les citoyens en allant à leur rencontre là où ils se trouvent; là où ils sont à la fois producteurs et consommateurs d'information, ajoutent Balagué et Fayon (2010). On peut de ce fait obtenir plus rapidement la réaction du public. Cela permet aussi d'améliorer la compréhension de certains problèmes et d'y trouver réponse. Selon le COI, le recours à des sites non gouvernementaux afin de communiquer avec les citoyens donne de la crédibilité à la volonté d'interagir avec ceux-ci.

Plusieurs organisations gouvernementales en divers endroits du monde ont commencé à adhérer aux SRS en créant une « page », profil de leur organisation, laquelle peut-être suivie par les utilisateurs du réseau et proposée à d'autres utilisateurs. C'est notamment le cas du gouvernement de Russie. Le ministère des Affaires étrangères du Canada et le ministère des Relations internationales du Québec par l'entremise de son programme Québec Sans Frontières, ont eux aussi créé des pages sur Facebook. Au gouvernement du Québec, certains ministères et organismes réfléchissent à la façon dont ils exploiteront les SRS. Facebook courtise notamment les gouvernements avec sa page *Facebook et Gouvernement* qui vise à recueillir les meilleures pratiques gouvernementales.

Beaucoup d'organisations publiques ont actuellement recours à Twitter[5] afin d'échanger des informations avec d'autres utilisateurs; c'est entre autres le cas d'organisations policières canadiennes et québécoises et des gouvernements de France, du Royaume-Uni, des États-Unis, et de l'Alberta.

Il en va de même pour diverses entreprises, institutions d'enseignement et organisations non gouvernementales. Les sites web des organisations offrent de plus en plus la possibilité aux internautes de les « suivre » sur un SRS afin d'avoir les dernières nouvelles, dès que possible.

Pour les organisations, les SRS servent donc à établir une relation avec le monde extérieur, afin d'obtenir ou de diffuser des informations. Les réseaux sociaux présentent aussi des bénéfices pour le fonctionnement interne de l'organisation. Ils offrent notamment le moyen de renforcer le sentiment d'appartenance à l'organisation. Par exemple, certaines entreprises suggèrent à leurs employés de devenir adeptes de leur page sur un SRS.

Pour une organisation, le recours aux réseaux sociaux permet une circulation transversale des informations. Le document du COI rappelle qu'il s'agit d'une occasion de favoriser les discussions et les relations entre les employés, le partage de connaissances et de pratiques. L'apport de commentaires spontanés peut faire progresser le déroulement du travail, des projets, etc[6]. Aussi, les SRS permettent ainsi une forme d'amélioration de la qualité de vie au travail. Des firmes qui étudient les questions d'utilisation des technologies de l'information suggèrent préférable pour les organisations d'autoriser l'utilisation des SRS, tout en imposant des règles de conduite plutôt que de les interdire. Elles pourront ainsi exercer un meilleur contrôle de l'utilisation et de l'apport de ce média.

3. RISQUES PERÇUS EN MATIÈRE DE SÉCURITÉ ET DE VIE PRIVÉE

Plusieurs organisations et chercheurs ont mis en évidence les risques associés à l'utilisation des sites de réseau social (SRS), notamment en ce qui a trait à la vie privée et à la sécurité.

Facebook et ses contemporains

Facebook - Créé en février 2004. Le plus connu et le plus utilisé des réseaux sociaux en ligne. À l'origine destiné aux étudiants de Harvard, il est offert, depuis septembre 2006, à toutes les personnes âgées de 13 ans et plus. Il permet de retrouver et de contacter des amis, parents et collègues de travail gratuitement. Les utilisateurs créent leur profil, le mettent à jour et voient celui de leurs amis. Plusieurs outils, tels que le clavardage, sont disponibles. Les utilisateurs peuvent décider si leurs informations seront accessibles à tous les utilisateurs du réseau ou seulement à leur réseau immédiat. Compte 500 millions de membres.

Hyves - Créé en octobre 2004. Réseau social des Pays Bas. Destiné principalement aux personnes qui parlent le néerlandais. Comme sur les autres réseaux, l'internaute crée son profil en ligne. Il peut rechercher et inviter des amis à faire partie de son réseau. Ce site permet entre autres de partager des messages, des photos et vidéos et d'écrire des blogs. Une multitude d'outils sont disponibles, tel le calendrier d'anniversaires des amis. Les informations sont visibles à tous les utilisateurs du réseau ou uniquement au réseau de l'utilisateur, selon son choix. Il compte 10 409 296 membres.

Viadeo - Créé en 2004. Premier réseau social professionnel en ligne français. Il permet de retrouver des collègues, des clients et des partenaires et de faire des recommandations entre les membres. Il se distingue par ses «hubs» sorte de forums de discussion thématiques. Le service de base est gratuit, mais la plupart des fonctionnalités requièrent l'adhésion à un service payant (quelques euros par mois). Ce site permet la recherche d'emploi. Des entreprises québécoises affichent notamment l'ouverture de postes. Sa politique de protection des renseignements personnels et de la vie privée est régie par les lois européennes. Compte 30 millions de professionnels.

MySpace – Crée en janvier 2004. Ce réseau cible principalement les jeunes. Il permet à ses utilisateurs de consulter le profil d'autres utilisateurs, de bloguer et d'échanger des courriels, de mettre du contenu musical et vidéo. Il se définit comme un lieu permettant l'expression personnelle, l'échange de contenu et de culture. Les données versées sur ce site sont hébergées aux États-Unis. Il compte plus de 122 millions d'utilisateurs actifs par mois.

La Commission européenne préoccupée par le sujet a d'ailleurs identifié les réseaux sociaux en ligne comme potentiellement dangereux pour la vie privée des utilisateurs inexpérimentés. Elle perçoit des risques contre lesquels elle met en garde les utilisateurs, particulièrement les enfants et les adolescents.

Plus spécifiquement, les risques soulignés par la Commission européenne et dans de nombreux documents[7] sont la cyberintimidation, la violation de la vie privée, le vol d'identité, la création d'un profil d'une personne sur un autre SRS à partir d'un profil qu'elle aurait elle-même créé sur un site, la vente illégale de données à des tiers, l'hameçonnage, l'exposition à des contenus dommageables, tels que la pornographie ou les contenus à caractère sexuel, la violence ou les contenus incitant à la mutilation personnelle (suicide, désordre alimentaire, etc.), et la cyberprédation. S'ajoutent à cela les possibilités d'atteinte à la réputation d'une personne et l'utilisation des informations diffusées à des fins commerciales sans que l'utilisateur en ait pleinement conscience, notamment par le profilage des internautes à des fins publicitaires. Certains risques d'être victime d'un de ces crimes ou méfaits semblent plus faibles, mais compte tenu de leur gravité, ils sont source d'inquiétude.

Au nombre des risques contre lesquels on met en garde les utilisateurs des SRS s'ajoutent ceux qui sont liés à leur propre comportement. Plusieurs utilisateurs s'attendent à ce que l'information soit diffusée dans un groupe restreint et durant un certain temps. Diffuser des informations sans se méfier de quoi que ce soit constitue un autre risque qui augmente les possibilités d'être victime d'un des crimes ou méfaits ci-haut mentionnés. La divulgation excessive d'informations personnelles expose les utilisateurs à plus de risques. En croisant des bases de données, des habitudes de vie peuvent être mises à jour, tels que des déplacements, des formes de consommation, des intérêts, des liens sociaux, des activités particulières, etc. C'est une possibilité ouverte aux firmes de marketing, d'assurance, aux services de police ou aux malfaiteurs (cambrioleurs), par exemple. Les informations sont divulguées sans aucune obligation et souvent avec une grande naïveté. Les exemples de propos publiés sur un réseau social qui ont nui à leur auteur ne sont pas rares. Récemment, le quotidien *Le Monde* faisait état d'un dossier en justice concernant le congédiement de trois employées ayant échangé sur Facebook, des propos injurieux et diffamatoires quant à la gestion des services de leur organisation *SOS-femmes*; messages qui auraient été interceptés par l'employeur. L'annonce sur Facebook du décès de la chanteuse Lhasa de Sela par de proches parents qui croyaient communiquer entre eux a suscité plusieurs discussions sur les réseaux, notamment Twitter, et dans la presse écrite. La nouvelle s'est répandue comme une traînée de poudre avant qu'une annonce officielle n'ait été faite. Il devint difficile de savoir s'il s'agissait d'une rumeur ou de la réalité, compte tenu de la multiplication des propos, entre autres, la maison de disque qui affirmait qu'elle se portait bien. Autre exemple bien connu, celui d'une personne en congé de maladie diffusant des photos où elle festoie et qui affirme avoir été pénalisée par son assureur, ce que dément toujours ce dernier.

Sur un SRS, toutes les interactions, les informations laissent une trace, contrairement aux relations hors ligne. Ainsi, l'utilisateur devrait davantage se soucier de protéger sa vie personnelle. Les SRS, pour leur part, devraient offrir des niveaux de confidentialité comparables à ce qu'on retrouve dans les relations hors ligne, soutient Barrigar (2010) dans un document qui compare les politiques de vie privée de six SRS.

Les renseignements personnels diffusés sur les SRS peuvent aussi satisfaire les intérêts des responsables des ressources humaines lors de la sélection de candidats. L'étude « Online Reputation Study »[8], de la firme Cross Tab Marketing Service réalisée pour le compte de Microsoft, révèle que les recruteurs professionnels ont tendance à explorer la réputation en ligne des candidats. L'étude mentionne que « 70 % des responsables RH interrogés aux États-Unis ont déclaré avoir déjà écarté un candidat à cause de sa réputation en ligne ». Cette tendance est beaucoup plus marquée aux États-Unis où il s'agit d'un critère dans le processus d'évaluation. Elle ne tardera probablement pas à se répandre dans le monde.

Malgré toutes ces inquiétudes, peu d'études montrent l'ampleur de ces dérives. Quelques chercheurs ont mené des travaux dans lesquels ils concluent que davantage d'études sont nécessaires afin d'obtenir un tableau réel de l'incidence des problèmes ayant causé des préjudices à des utilisateurs de SRS. Les cas qui ont été révélés au public l'ont souvent été par les médias, avec relent de sensationnalisme, soulignent les chercheurs qui ont étudié le sujet.

Une étude récente[9] a recensé les « incidents criminels associés à des sites de socialisation en ligne » survenus aux États-Unis et au Canada au cours d'un peu plus d'un an. Les résultats préliminaires font état de crimes sexuels, d'attaques informatiques, d'actes de violence et de menaces. S'ajoutent à cela les fraudes et atteintes aux biens. Les chercheurs soulignent que chaque site fait face à des risques spécifiques et certains utilisateurs semblent davantage à risque, notamment les jeunes adultes. Les auteurs remarquent aussi que des contenus problématiques peuvent faire peser des risques sur les individus et les organisations. Les retombées des informations privées révélées sur les SRS « ne sont pas encore pleinement maîtrisées » par les utilisateurs. Cela peut entraîner des abus dommageables pour les individus ou les organisations. Celui qui n'a pas correctement précisé l'accès à son profil pourrait rendre accessible des informations embarrassantes pour lui-même ou quelqu'un de son entourage.

> 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 (Dupont, Lavoie et Fortin, 2010 :9)

Les chercheurs n'ont pas trouvé de corrélation entre le nombre d'utilisateurs des sites et le nombre d'incidents recensés. Ils constatent plutôt des différences selon les particularités des sites et la technologie utilisée.

Retenons aussi de cette étude empirique que « rien n'indique que la fréquentation des ces sites génère pour [les millions d'utilisateurs] (y compris les plus jeunes d'entre eux) des risques excessifs qui seraient individuellement et collectivement intolérables » (Dupont, Lavoie et Fortin, 2010 :13). Il faudrait donc éviter de réglementer à outrance.

Les risques perçus d'atteinte à la vie privée ou à la sécurité ne semblent pas constituer un frein pour les internautes. Pour preuve, les utilisateurs de SRS continuent de se multiplier. C'est pourquoi plusieurs études[10] ont analysé les motivations des utilisateurs à diffuser des informations personnelles en ligne. Selon celles-ci, les avantages de la participation semblent faire un contre poids aux risques. Néanmoins, des mesures de prévention apparaissent nécessaires afin de mieux outiller les internautes et la population en général en vue d'une utilisation sécuritaire pour réduire les risques éventuels. Il faudrait notamment insister sur l'importance de configurer son compte comme cela est possible sur Facebook.

Face à ces risques, les préoccupations des responsables de la protection de la vie privée des citoyens et consommateurs ont donné lieu à diverses démarches en vue de les contrer.

4. CONTRER LES RISQUES D'ATTEINTE À LA VIE PRIVÉE

En plus des chercheurs, différentes organisations publiques se sont intéressées au phénomène des réseaux sociaux en ligne et ont signalé les défis qu'ils posent en matière de protection de la vie privée des participants et de leur sécurité. Elles ont, dès lors, déployé des mesures visant à lutter contre les risques potentiels. Des études ont été réalisées, des recommandations formulées et du matériel d'information sur le sujet a été préparé. L'OCDE soulignait, dans un rapport en 2007, que les forces de l'ordre, les responsables gouvernementaux et les sites de réseau social (SRS) devaient accorder une attention prioritaire à mettre en place des mesures de sécurité, éduquer les parents et les enfants et tenter de réduire les risques de comportements déviants sur les SRS.

Des différentes analyses et enquêtes, le principal moyen de contrer les risques d'atteinte à la vie privée par les SRS parait être l'incitation à la prudence. Un rapport de l'European Network and Information Security Agency (ENISA), publié en 2007, mettait déjà en garde les utilisateurs de SRS contre les risques d'atteinte à la vie privée provoqués par une mauvaise utilisation de ceux-ci. On y recommandait, notamment, des campagnes de sensibilisation et d'éducation à l'utilisation sécuritaire des SRS et la révision et la réinterprétation du cadre réglementaire et, si nécessaire, la modification des lois actuelles afin de tenir compte des nouveaux médias, tels que les réseaux en ligne.

La Commission européenne a constitué, en 2008, un groupe de travail chargé d'élaborer des lignes directrices de protection des jeunes internautes utilisant des SRS. Ce groupe était composé de chercheurs et de responsables de « sites de socialisation » et d'organisations non gouvernementales de protection des jeunes. Il a donc été demandé aux responsables des principaux SRS d'adopter un code de conduite visant à protéger les jeunes utilisateurs. Une vingtaine d'entreprises du monde numérique ont signé, en février 2009, une charte de bonne conduite – *Safer social Networking Principles for the EU*. Celle-ci vise à accroître la sécurité des mineurs lorsqu'ils utilisent les SRS, en Europe. La plupart des signataires, dont Facebook, Hyves et MySpace, ont expliqué de quelle manière ils mettent en œuvre cet engagement.

Les autorités de protection de la vie privée en Europe se sont aussi penchées sur les enjeux que soulèvent les SRS en matière de vie privée. Principalement sur le fait qu'en contrepartie de leur gratuité, ils fournissent des renseignements personnels à des fins d'utilisation commerciale. Ainsi, le G29[11], a émis un avis, en juin 2009, à propos de l'applicabilité du droit européen de protection des renseignements personnels et de la vie privée sur les SRS. Cet avis précise de quelle manière les réseaux sociaux peuvent « répondre aux exigences de la législation de l'UE en matière de protection des données ». Il vise à indiquer aux fournisseurs de SRS les mesures à mettre en place afin de respecter la vie privée des utilisateurs. Les recommandations sont basées sur la Directive européenne de 1995[12]. Ces recommandations rappellent, entre autres, l'importance d'informer les participants aux SRS du traitement qui sera fait de leurs renseignements personnels, et plus particulièrement de ceux des mineurs. Elles signalent la nécessité d'obtenir le consentement préalable lorsqu'on exploite les informations d'une autre personne. De plus, les recommandations devraient s'appliquer aussi aux SRS quand leur siège social se trouve à l'extérieur de l'Europe.

Le G29 a ainsi adopté des standards destinés aux réseaux sociaux. Ceux-ci demandent principalement au SRS de :

- définir des paramètres par défaut limitant la diffusion des données des internautes.
- mettre en place des mesures pour protéger les mineurs.
- supprimer les comptes qui sont restés inactifs pendant une longue période.
- permettre aux personnes, même si elles ne sont pas membres des réseaux sociaux, de bénéficier d'un droit de suppression des données qui les concernent. proposer aux internautes d'utiliser un pseudonyme, plutôt que leur identité réelle.
- mettre en place un outil accessible aux membres et aux non membres, sur la page d'accueil des réseaux sociaux permettant de déposer des plaintes relatives à la vie privée. (Rapport du groupe de travail « Éthique du Numérique », 2010 :15)

Au Canada, le Commissariat à la protection de la vie privée (CPVP) a émis des recommandations à l'égard du SRS Facebook à la suite d'une plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC). Cette plainte portait sur plusieurs aspects. Le CIPPIC prétendait que Facebook ne respectait pas la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Elle dénonçait, entre autres, des failles concernant les paramètres de confidentialité par défaut, la collecte et l'utilisation des renseignements personnels des utilisateurs à des fins publicitaires et la communication des renseignements personnels des utilisateurs aux tiers développeurs d'applications[13], et la désactivation d'un profil. Pour les allégations jugées fondées, le CPVP a émis vingt recommandations. Depuis, Facebook a procédé à des modifications, dans certains cas. De ce nombre, notons :

- à propos des applications de tiers, que Facebook informe les utilisateurs des renseignements que chacune requiert et à quelles fins ;
- en matière de conservation des renseignements, que Facebook élimine les renseignements dans ses serveurs après une période raisonnable et en informe les utilisateurs. Demande qui a été acceptée.

Le CPVP a aussi demandé à Facebook d'expliquer plus clairement dans sa politique de confidentialité le rôle de la publicité ainsi que l'utilisation des renseignements du profil à des fins de publicité ciblée, puisqu'elle reconnait son importance sûr un site gratuit. Facebook a notamment accepté de décrire plus clairement la publicité envisagée et a apporté des modifications sur son site afin que les utilisateurs dénichent plus facilement cette information.

Cet exemple illustre de quelle manière les autorités responsables de la vie privée peuvent jouer un rôle vis-à-vis de nouveaux phénomènes de communication, tels que les SRS et comment les lois actuelles peuvent servir face à de nouvelles situations. Ce cas d'enquête de Facebook a bien sur été suivi à l'échelle de la planète puisqu'il visait tous les utilisateurs de ce réseau, au Canada et ailleurs.

Une analyse comparative de la vie privée sur six SRS pour le compte du CPVP a également permis de soumettre quelques recommandations aux responsables des SRS afin qu'ils améliorent différents éléments de leur site et assurent une plus grande protection de la vie privée.

Les différents organismes de protection de la vie privée, le G29 et le CPVP insistent sur l'importance d'informer clairement les utilisateurs et de rappeler le besoin d'obtenir leur consentement quant au traitement de leurs renseignements personnels et de la protection de leur vie privée, ce à quoi semblent se prêter les SRS. Cependant, les politiques de confidentialité demeurent généralement illisibles. Elles sont rarement lues, entre autres, à cause de leur longueur et de leur teneur juridique. Tout en tenant compte de la nécessité de mettre à la disposition des internautes plus d'informations, il faudrait éviter que de telles recommandations ne se traduisent par des politiques de confidentialité encore plus longues et complexes que personne ne lira (Gautrais, 2010). Souvent en raison de sa formulation, le consentement protège davantage l'organisation qui offre le service que l'individu. Des politiques de confidentialités plus courtes, seraient probablement plus claires pour les utilisateurs qui donneraient alors un consentement réellement éclairé.

Des organisations gouvernementales en différents endroits du monde mettent au point des documents visant la meilleure utilisation possible des réseaux sociaux. C'est notamment le cas en Caroline du Nord. Cet État américain a émis des lignes directrices à l'intention des organisations publiques qui veulent exploiter les réseaux sociaux. Les responsables souhaitent que ces informations protègent les employés de l'État et assurent une cohérence dans l'intégration des médias sociaux à la mission des organisations. Après avoir établi si un SRS est nécessaire à la stratégie de communication de l'organisation, cette dernière doit définir les limites de l'utilisation par les employés afin de prévenir les éventuels problèmes. Les organisations doivent aussi former les employés quant aux informations pouvant être partagées et les risques de divulguer certains renseignements. Elles doivent prévenir entre autres la fraude, telle que l'affichage d'une information bidon pouvant nuire à la notoriété de l'organisation, ou l'accès illégal à des informations personnelles sur les employés ou les citoyens et qui pourrait mettre en jeu la sécurité de l'organisation et la protection des citoyens.

Même chose au Royaume-Uni où le Central Office of Information (COI) a publié un guide destiné aux employés de l'État à propos de l'utilisation des médias sociaux, incluant les SRS.

Des documents de sensibilisation et d'éducation du public ont aussi été préparés par le CPVP. Sur leur site on trouve notamment une vidéo, des fiches d'informations et un document sur l'identité en ligne et la vie privée. Concernant le gouvernement du Québec, les outils de sensibilisation semblent inexistants pour le moment. On retrouve sur le Portail gouvernemental un bref avertissement à propos de problèmes pouvant survenir lors de l'utilisation des réseaux sociaux en ligne. Différents ministères et organismes pourraient intervenir en matière d'éducation du public afin de lutter contre la tendance à rendre publics des aspects de la vie privée sur Internet, particulièrement dans les réseaux sociaux. Le ministère de l'Éducation pourrait notamment instaurer des mesures de sensibilisation et d'éducation destinées aux jeunes et au personnel enseignant, dans les écoles primaires et secondaires.

Que ce soit au Canada, en Union européenne, aux États-Unis ou ailleurs dans le monde, les instances qui veillent à la protection des citoyens contribuent à une meilleure gestion de la protection de la vie privée sur les SRS. Leur rôle semble d'autant plus important, compte tenu de la relative nouveauté du phénomène.

Outre les organisations, les utilisateurs des SRS ont aussi un rôle à jouer dans la protection de la vie privée. Tout comme ils participent à la création du contenu, ils devront aussi collaborer à la protection des renseignements personnels et de la vie privée. En tant qu'acteurs des réseaux sociaux ils devront connaître leurs droits et devoirs afin d'agir de manière éclairée. Ils devront apprendre à gérer leur identité numérique. C'est un des constats que font la majorité des auteurs consultés sur le sujet. L'État et les organisations responsables pourront ainsi poursuivre leur travail de soutien. Ils devront veiller à ce que les outils permettant de prendre des décisions éclairées soient disponibles et que les politiques et mesures de protection de la vie privée soient à jour.

Selon Alex Türk[14], président du G29, en l'état actuel du droit et en l'absence de standards juridiques internationaux concernant les SRS, c'est à chacun de maîtriser l'information qu'il met sur les SRS.

Soulignons enfin que les enjeux de protection des renseignements personnels et de vie privée traités dans ce texte s'évaluent en fonction de législations dans un contexte de démocratie libérale. Il faut être conscient que des problèmes très graves surgissent dans des États qui exercent une surveillance étroite de tous types de communication, y compris les réseaux sociaux, avec l'objectif de faire taire les utilisateurs qui portent ombrage à l'autorité politique en place.

CONCLUSION

Phénomène nouveau qui soulève l'engouement dans tous les groupes d'âge et fait partie du quotidien de millions de personnes partout sur la planète, les sites de réseau social (SRS) entraînent avec eux des inquiétudes associées à la sécurité et la protection de la vie privée. Caractérisés par la possibilité d'interaction simultanée avec plusieurs personnes dans le monde, les réseaux sociaux en ligne comportent beaucoup d'avantages pour les personnes qui en font partie. Ils permettent notamment de maintenir le contact avec des personnes éloignées physiquement. Depuis la création des sites de réseau social en 1997, des risques qui peuvent causer préjudice à la vie privée et mettre la sécurité des personnes en péril ont été perçus. Des cas de crimes et méfaits envers des utilisateurs des SRS ont été relevés, mais peu d'études ont jusqu'à présent permis d'en révéler « l'ampleur réelle ». Pour le moment, rien d'alarmant aux États-Unis et au Canada, annoncent les premiers résultats de chercheurs du Québec. En général, on perçoit des risques, certains semblent exagérés ou obtenir une plus grande attention des médias. Les réseaux sociaux en ligne sont un nouveau phénomène en mouvance; ils évoluent et s'adaptent au marché, aux utilisateurs et aux pressions de la société. C'est pourquoi il faut rester attentif afin de prévenir les dérives.

Compte tenu de la nouveauté du phénomène et des craintes soulevées par l'adhésion aux SRS, beaucoup d'actions ont été menées par les responsables du respect de la vie privée en divers endroits du monde. Les nombreuses recommandations visant à protéger la vie privée sur les SRS en témoignent. Les recommandations émises par ceux qui ont étudié la question concernent surtout la nécessité de la prévention, de la sensibilisation et de l'éducation plutôt que l'interdiction, les mises en garde sévères et le besoin de nouvelles lois. Davantage d'études sur l'impact véritable des SRS sur la vie privée et la sécurité s'avèrent nécessaires. Des données plus précises concernant les cas de crimes et de méfaits perpétrés à partir de SRS permettront d'améliorer la protection des renseignements, de la vie privée et de la sécurité des citoyens.

Notes

1 « Renseignements personnels » fait référence à toutes les données qui permettent d'identifier une personne. La protection des renseignements personnels assurée par la législation vise le traitement des données de manière générale, ce qui inclut tant leur divulgation que leur utilisation, leur communication et leur conservation.

2 La vie privée englobe les informations personnelles qu'un individu juge importantes et qu'il ne souhaite pas porter à la connaissance de la population entière.

3 À la suite d'une plainte contre Facebook aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), la commissaire adjointe à la vie privée du Canada, s'est penchée sur les annonces publicitaires sur le site Facebook. Elle reconnait, dans son rapport d'enquête, l'utilité de la publicité qui permet la gratuité du service, mais signale aussi la nécessité de mieux informer les utilisateurs à ce sujet. Elle insiste sur le besoin d'obtenir un consentement éclairé des utilisateurs, particulièrement quand des concepteurs de programmes informatiques accèdent aux renseignements personnels de ceux-ci.

4 Pour plus d'information sur le site, voir l'article « Aux Pays-Bas, la politique au crible des internautes », par Jean-Pierre Stroobants, *Le Monde.fr*, 10 juin 2010, ou le site en néerlandais *SchaduwKamer.nl* http://panel.noties.nl/schaduwkamer/?home&PHPSESSID=b9ljpm3a0iphfkkuj1ns1q9455(*consulté août 2010)*.

5 *Twitter* est à cheval entre deux types de médias sociaux. Il fonctionne à la fois comme un SRS et comme un service de mise à jour ou de microblogage, c'est-à-dire qu'il permet aux utilisateurs d'écrire de courts messages et de lire ceux des autres qui font partie de leur réseau.

6 Ruette-Guyot et Leclerc (2009) illustrent, à l'aide de divers exemples, les avantages de l'utilisation de réseaux sociaux à l'intérieur d'une organisation. Ils expliquent, notamment, comment le Groupe Canam, entreprise qui œuvre dans le domaine de la construction et de l'ingéniérie, a fait adhérer ses gestionnaires à Facebook afin de préparer efficacement un événement d'importance pour l'organisation.

7 Voir notamment le site de la Clinique d'intérêt public et de politique d'Internet du Canada – CIPPIC à propos des risques associés aux réseaux sociaux en ligne et l'article de Dupont, Benoît et Vincent Gautrais. 2010. « Crime2.0 : le web dans tous ses états! », *Champ pénal/ Penal field, nouvelle revue internationale de criminologie*, vol. VII.

8 Étude « Online Reputation Study » commanditée par Microsoft et réalisée par le cabinet d'études « Cross Tab Marketing Service » auprès d'individus, professionnels des RH et recruteurs, des États-Unis, du Royaume-Uni, d'Allemagne et de France. L'échantillon était constitué de 343 personnes en France, 9334 en Allemagne, 335 aux États-Unis et 333 au Royaume-Uni. Quant aux professionnels des RH et recruteurs, environ 275 par pays ont été rencontrés.

9 Voir les résultats préliminaires de l'étude de Dupont, Benoit, Pierre- Eric Lavoie & Francis Fortin. 2010. *Les crimes sur le web 2.0,* Une recherche exploratoire, Note de recherche no. 8, Chaire de recherche du Canada en sécurité, identité et technologie.http://www.benoitdupont.net/sites/default/files/Dupont%20Lavoie%20Fortin%20crimes%20web%202%200.pdf

10 Voir notamment les études récentes de Newk-Fon Hey Tow, Dell et Venable, 2010, à propos de la diffusion d'information sur Facebook par des internautes australiens, celle de Krasnova *et al*, 2010, sur les motivations à la divulgation d'information et celle De Souza et Dick, 2008, sur la diffusion d'information sur MySpace.

11 Organe consultatif européen indépendant qui regroupe les représentant de contrôle et de protection des personnes à l'égard du traitement des renseignements personnels de chacun des États membres de l'Union européenne.

12 *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.*

13 Programmes informatiques qui permettent à un utilisateur de faire des tâches spécifiques. Sur les sites de réseaux sociaux, en l'occurrence Facebook, on pense aux jeux, horoscopes, et autres extensions qui y sont intégrés.

14 Propos rapportés dans un article de Catherine Vincent « Vie privée sur Internet: la polémique Facebook », *Le Monde*, 19 février 2009.

Bibliographie

Balagué, Christine, and David Fayon. 2010. *Facebook, twitter et les autres : intégrer les réseaux sociaux dans une stratégie d'entreprise*. Paris: Pearson.

Barrigar, Jennifer. 2009. *La vie privée sur les sites de réseau social analyse comparative de six sites*. Ottawa, Ont.: Commissariat a la protection de la vie privée du Canada. http://site.ebrary.com/lib/librarytitles/Doc?id=10330317.

Christensen, Miyase. 2010. Facebook is watching you. *Manière de voir - Internet, révolution culturelle* 109 (Février - mars):53-55.

CIPPIC - Clinique d'intérêt public et de politique d'Internet du Canada. *What are some of the risks associated with social networking websites?* Mis à jour juin 2008, (consulté le 26 juillet 2010). www.cippic.ca/social-networking/.

COI Central Office of Information. *Engaging through social media. A guide for civil servants*. http://coi.gov.uk/documents/Engaging_through_social_media.pdf.

Commission européenne. *Social Networking Sites. Opportunities and Risks.* Europa 2010. http://ec.europa.eu/information_society/activities/social_networking/opps_risks/index_en.htm

Commission européenne. 2009. *Safer Social Networking Principles for the EU.* http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

Cousin, Capucine. 2008. *Tout sur le Web 2.0*. Paris: Dunod.

Cross Tab. 2010. *Online Reputation in a Connected World.* http://www.microsoft.com/privacy/dpd/research.aspx.

Davies, Alysia. 2010. *Les médias sociaux. 3. La protection des renseignements personnels : l'exemple de Facebook.* Bibliothèque du Parlement (8 février), http://dsp-psd.tpsgc.gc.ca/collections/collection_2010/bdp-lop/bp/2010-06-fra.pdf.

De Souza, Zaineb, and Geoffrey N. Dick. 2008. Information Disclosure on MySpace--the What, the Why and the Implications. *Pastoral Care in Education* 26 (3):143-157.

Denham, Elizabeth. 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: Commissariat à la protection de la vie privée du Canada. http://epe.lac-bac.gc.ca/100/200/301/opc-cpvp/rep_findings_complaint_filed-f/IP54-31-2009-fra.pdf.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=1995&nu_doc=46.

Dupont, Benoit, Pierre-Eric Lavoie et Francis Fortin. 2010. Les crimes sur le web 2.0: une recherche exploratoire. *Note de recherche no. 8,* http://www.benoitdupont.net/sites/default/files/Dupont%20Lavoie%20Fortin%20crimes%20web%202%200.pdf.

Dupont, Benoît, and Vincent Gautrais. 2010. Crime 2.0 : le web dans tous ses états ! *Champ pénal / Penal field, nouvelle revue internationale de criminologie [En ligne]* (mis en ligne le 23 février), http://champpenal.revues.org/7782.

ENISA - European Network and Information Security Agency. 2007. *Security Issues and Recommandations for Online Social Networks*, Position Paper No. 1. http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks.

Gautrais, Vincent, and Pierre Trudel. 2010. *Circulation des renseignements personnels et Web 2.0*. Montréal: Éditions Thémis.

Gautrais, Vincent. 2010. Entretien, 17 septembre.

Groupe de travail « article 29 » sur la protection des données. *Avis 5/2009 sur les réseaux sociaux en ligne*, adopté le 12 juin 2009. http://www.cnpd.public.lu/fr/publications/groupe-art29/wp163_fr.pdf

Ipsos Reid. 2010. *The Canadian Inter@ctive Reid Report 2009 Fact Guide*.

Krasnova, Hanna, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. Online social networks: why we disclose. *Journal of Information Technology* 25 (2):109-125.

Lobe, Bojana. *Implementation of the Safer Social Networking Principles for the EU: Testing of 20 social Networks in Europe - Facebook*, February 2010. http://ec.europa.eu/information_society/activities/social_networking/docs/individ_reports/facebook.pdf.

Microsoft. *69% des Français concernés par l'impact de leur réputation en ligne sur leur vie privée et professionnelle*. Microsoft 2010. http://www.microsoft.com/France/InformationsPresse/Fiche-Communique.aspx?EID=a4cc249e-2930-48ce-8c03-c87f9c97a09b.

Ruette-Guyot, Emmanuelle, and Serge Leclerc. 2009. *Web 2.0 : la communication iter-@ctive*. Paris: Economica.

Saint-Laurent, Jacques 2010. *La protection des droits dans un contexte de mondialisation: Défis afférents à la protection des données personnelles pour la garantie des droits fondamentaux et la consolidation de la démocratie*, Allocution. Journées des réseaux institutionnels de la francophonie, Association francophone des autorités de protection des données personnelles (AFAPDP), 18 et 19 mai.

Stroobants, Jean-Pierre. 2010. Aux Pays-Bas, la politique au crible des internautes. *Le Monde.fr*, http://panel.noties.nl/schaduwkamer/?home&PHPSESSID=b9ljpm3a0iphfkkuj1ns1q9455.

Timm, Dianne, and Carolyn Duven. 2008. Privacy and social networking sites. *New Directions for Student Services* 2008 (124):89-101.

Torloting, Philippe. 2006. *Enjeux et perspectives des réseaux sociaux.* Institut Supérieur du Commerce de Paris. Marketing, Management et Technologies de l'information. http://www.phive-online.com/divers/reseau_social/Memoire_Reseaux_Sociaux_Philippe_Torloting.pdf.

Tow, William Newk-Fon Hey, Peter Dell, and John Venable. 2010. Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology* 25 (2):126-136.

Le Laboratoire d'étude sur les politiques publiques et la mondialisation a été créé en 2004 par une entente de partenariat entre le ministère des Relations internationales et l'ENAP. Le Laboratoire est un lieu de veille et d'analyse consacré à l'étude des effets de la mondialisation sur le rôle de l'État et sur les politiques publiques au Québec, et ce sur les enjeux d'ordre culturel, économique, environnemental, de santé, d'éducation et de sécurité.

Relations internationales
Québec

Directeur : Paul-André Comeau

Pour renseignements :
Karine Plamondon
Téléphone : (418) 641-3000 poste 6864
leppm@enap.ca

Les publications du Laboratoire peuvent être consultées sur le site :
www.leppm.enap.ca

Pour citer ce document :

TREMBLAY, Monica. Réseaux sociaux sur Internet et sécurité de la vie privée. Québec, Laboratoire d'étude sur les politiques publiques et la mondialisation, ENAP, 2010, 19 p. (Rapport évolutif. Analyse des impacts de la mondialisation sur la sécurité au Québec; Rapport 9).

ENAP
L'Université de l'administration publique

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2010
Dépôt légal - Bibliothèque et Archives Canada, 2010

ISBN978-2-923856-06-3 (version imprimée)
ISBN 978-2-923856-07-0 (PDF)