La sécurité des données personnelles

Une question de perception et d'interactions

Anne-Marie Pratte

Note de recherche no. 6

Chaire de recherche du Canada en sécurité identité technologie

Université de Montréal

Ce travail a été réalisé dans la cadre du cours CRI-6234, « Nouvelles technologies et crimes » (session d'automne 2009), offert aux étudiants de la Maîtrise en Criminologie sous la direction du Professeur Benoît Dupont.

La Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers.

Anne-Marie Pratte
anne-marie.pratte@umontreal.ca

Prof. Benoît Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada
benoit.dupont@umontreal.ca
www.benoitdupont.net
Fax : +1-514-343-2269

Table des matières

INTRODUCTION **4**
BILAN DES CONNAISSANCES **5**
INTERNET ET LA MODIFICATION DES HABITUDES DE VIE 5
INTERNET ET LA SÉCURITÉ DES DONNÉES PERSONNELLES 6
LA CONFIANCE ET LA NOTION DU RISQUE 7
MÉTHODOLOGIE **7**
SONDAGE SUR LE VOL D'IDENTITÉ 8
ANALYSE DOCUMENTAIRE 10
RÉSULTATS **11**
LE DEGRÉ DE CONFIANCE DES QUÉBÉCOIS RELATIVEMENT À DIVERSES ORGANISATIONS 11
LE DEGRÉ DE CONFIANCE EN LIEN AVEC LES VARIABLES PERSONNELLES ET SOCIODÉMOGRAPHIQUES 13
LA REPRÉSENTATION DES RISQUES DANS LES MÉDIAS QUÉBÉCOIS 15
CONCLUSION **17**
RÉFÉRENCES **18**

INTRODUCTION

Nos activités quotidiennes nous imposent à transmettre nos informations personnelles à une diversité d'institutions. Nos employeurs, les différents services gouvernementaux, les institutions financières, les services de la santé, le commerce de détail, les compagnies de communication, pour ne nommer que ceux-là, ont tous un point en commun : ils détiennent un nombre considérable d'information à notre sujet. Dans ce sens, Los (2006) aborde la notion de *data double*, c'est-à-dire qu'il y a tant d'information disponible sur nous que c'est comme si nous avions un double. De plus, les implications de son existence nous échappent le plus souvent puisque la divulgation de nos données personnelles est une activité ancrée dans notre quotidien que nous effectuons sans vraiment y porter attention. Chaque année, il y a une quantité impressionnante de données personnelles qui est compromise créant des brèches de sécurité et en augmentant les probabilités que ces informations se retrouvent entre de mauvaises mains.

Par ailleurs, beaucoup de nos activités routinières s'effectuent par l'intermédiaire d'Internet où nous effectuons diverses transactions qui nous obligent à divulguer nos informations personnelles. À la Hansel et Gretel[1], nous laissons derrière nous plusieurs morceaux de notre identité lorsque nous naviguons sur le World Wide Web. L'utilisation massive d'Internet pour gérer nos activités quotidiennes amène aussi son lot de préoccupations quant à la sécurité des données personnelles. Certains individus jugent le risque de subir un préjudice faible tandis que d'autres montrent une inquiétude manifeste. Bref, la confiance envers les institutions n'est pas uniformément distribuée au sein de la population.

Dans cette optique, il est intéressant de s'attarder sur la perception des individus relativement à la sécurité de leurs données personnelles sur Internet. À l'heure actuelle, ce sujet nous semble peu, pour ne pas dire pas étudié. Il y a Dupont qui s'est intéressé furtivement à la question. Il affirme que la confiance envers les institutions ne se répartit pas de manière identique parmi tous les groupes de la population (2008 : 24). Nous proposons donc de poursuivre sa recherche, mais en amenant de nouvelles hypothèses explicatives sur le sujet. De façon plus spécifique, nous nous intéressons à la perception qu'ont les Québécois quant à la sécurité de leurs données personnelles sur Internet et ce, d'un point de vue constructiviste. Par ailleurs, partant de la prémisse que la confiance relève d'une construction que les sujets se font de la réalité, il est intéressant de s'attarder à une diversité de variables afin de vérifier cette hypothèse.

La première section de cet article permet d'effectuer un bref aperçu des connaissances sur les conséquences qu'Internet a eu sur les habitude de vie, sur la protection des données personnelles sur Internet et sur la notion de la confiance. La seconde section fournit une description de notre méthodologie qui aborde à la fois un devis quantitatif et qualitatif. Pour le devis quantitatif, nous allons effectuer un examen des associations entre les degrés de confiance vis-à-vis une diversité d'institutions et des variables sociodémographiques et personnelles. En ce qui concerne le devis qualitatif, nous allons effectuer un examen plus général de la représentation des risques dans les médias québécois. Finalement, notre troisième section présente les résultats de notre recherche qui se scinde en trois principaux points. Premièrement, nous décrivons le degré de confiance des Québécois envers huit institutions.

[1] Compte des frère Grimm datant du XIXe siècle qui raconte l'histoire d'un frère et d'une sœur qui pour retrouver leur chemin laisse plusieurs bouts de pain sur leur passage.

Deuxièmement, afin d'expliquer cette confiance, nous présentons les résultats des associations statistiques entre les degrés de confiance et des variables sociodémographiques et personnelles. Troisièmement, à titre complémentaire, nous terminons avec un examen général de la représentation des risques dans les médias québécois.

BILAN DES CONNAISSANCES

Internet et la modification des habitudes de vie

Comme l'ont souligné Cohen et Felson (1979) les modifications des habitudes de vie ont eu un impact quant à la hausse de la criminalité dans les années 1970. Il y a eu une dispersion des activités à l'extérieur de la résidence occasionnant une augmentation des opportunités criminelles. Durant cette période, l'introduction par effraction a connu une hausse considérable qui peut être en partie attribuable à la modification des habitudes de vie. Les délinquants profitent de ces opportunités pour commettre des délits. En d'autres termes, « l'occasion fait le larron ».

Par ailleurs, les années 1990 se caractérisent par l'explosion du World Wide Web, soit une application qui opère par l'entremise d'Internet (Castells, 2001). L'arrivée de cette technologie a eu des répercussions importantes dans les habitudes de vie des citoyens créant une fragmentation des communications sociales. Le courriel remplace l'appel téléphonique ou une visite à domicile. Le commerce en ligne réduit la fréquentation des centres d'achats. Les transactions financières en ligne réduisent la fréquentation des institutions financières. Le jeu en ligne vient graduellement remplacer les différents clubs. Internet est devenu, par l'entremise de l'ordinateur, un outil privilégié pour réaliser différentes activités. Bref, Internet est utilisé de façon croissante pour effectuer une diversité de transaction (Lynch et Lundquist, 1996).

À titre indicatif, l'Institut de la statistique du Québec a effectué un sondage sur l'utilisation d'Internet par les ménages québécois. Il en ressort qu'en 2001, 69 % des ménages utilisent régulièrement Internet (Poussart, 2001). Près d'une décennie plus tard, nous pouvons estimer que ce pourcentage est encore plus élevé. Selon Dryburgh (2001), c'est par intérêt personnel que les individus se branchent à Internet. Ils cherchent des renseignements sur des produits et des services et pour accéder à des sites de nouvelles en ligne. Il apparaît que 24 % des Canadiens interrogés effectuent du cybercommerce et que 23 % utilisent des services bancaires électroniques. Une autre étude mentionne que l'envoie ou la lecture de courriel est l'activité dominante (80 %), suivi de la lecture de bulletin de nouvelles (51 %), de la navigation pour le plaisir (49 %), du clavardage en direct (47 %), de la recherche d'informations (36 %), du jeu en ligne (23 %), du téléchargement et de l'écoute de musique (14 %) et finalement la dernière activité effectuée quotidiennement consiste à gérer ses finances (14 %) (Institut de la sécurité de l'information du Québec, 2007).

Internet fait maintenant partie de notre quotidien, et ce changement dans les habitudes de vie peut inciter certains délinquants à développer des outils modernes pour commettre leurs délits. Les auteurs de certains crimes conventionnels comme la fraude et le vol d'identité en sont venus à intégrer les technologies pour arriver à leurs fins (Leman-Langlois, 2006). Internet est à la fois responsable de la modernisation de certains crimes et de l'émergence d'autres. Par

exemple, l'hameçonnage et le pharming sont deux techniques de fraude développées par les pirates informatiques grâce à Internet. L'hameçonnage consiste à tenter d'obtenir des informations personnelles d'un grand nombre d'individus en les dirigeant, à leur insu, vers une copie frauduleuse d'un site Web légitime. Le pharming est une technique, communément appelée empoisonnement du système du nom de domaine, qui ressemble beaucoup à l'hameçonnage. La différence c'est que le courriel n'est pas utilisé comme appât. Sans s'étendre sur le sujet, nous pouvons affirmer que la cybercriminalité est un phénomène en pleine émergence.

Internet et la sécurité des données personnelles

Dupont et Gagnon (2008) affirment que depuis les dernières années, il y a un déficit manifeste relativement à la gestion informatique des données personnelles. Qu'il s'agisse de vol, de négligence, de piratage ou de perte, certaines organisations sécurisent mal les informations de leurs clients créant des brèches au niveau de la sécurité. Par ailleurs, comme il vient d'être mentionné, Internet est maintenant un outil de prédilection pour effectuer une diversité de transactions ce qui semblerait augmenter les risques de compromission des données personnelles.

Dans son rapport, l'Institut de la sécurité de l'information du Québec (2007) a mentionné dans quelle proportion 1070 Québécois fournissaient leur nom et leur adresse en ligne. Il appert que 67 % des Québécois donnent ces infos pour transiger avec des organismes gouvernementaux, dans 55 % du temps pour faire des achats en ligne, dans 53 % pour participer à des concours en ligne, dans 49 % pour participer à des sondages, dans 44 % pour s'abonner à une publication, dans 32 % pour avoir un compte courriel gratuit et dans 21 % pour créer un compte de messagerie instantanée. En résumé, plusieurs occasions semblent être bonnes pour divulguer des données personnelles. Nous pourrions même affirmer qu'il est quasiment impossible de faire des transactions sur Internet sans divulguer nos renseignements.

Dans une perspective de choix rationnel, Haggerty (2003) suggère que les individus effectuent un calcul coût/bénéfice à l'égard des risques qu'ils peuvent rencontrer et la probabilité d'être victime. Leurs actions seront donc fonction de la conjoncture entre les probabilités de rencontrer un risque et l'incidence qu'il produirait s'il advenait à se produire. Lorsqu'appliquer a la divulgation des renseignements personnels sur Internet, il semblerait que les individus jugent que les risques de subir un préjudice sont inférieurs aux bénéfices attendus. En agissant de la sorte, certains se mettent dans une position de victime potentielle. D'autres individus sont inquiets quant à la sécurité et de la protection de leurs renseignements personnels sur Internet (Dryburgh, 2001). À cet effet, 37 % des canadiens affirment être très inquiets relativement à la protection de leurs renseignements personnels, 29 % sont légèrement inquiets, 9 % sont à peine inquiets, 23 % ne sont nullement inquiets et 2 % sont sans opinion. Dryburg (2001) affirme que les utilisateurs d'Internet qui sont le plus inquiets relativement à la protection de leurs renseignements personnels sont ceux qui sont le moins susceptibles d'effectuer dans transactions par Internet. Pour certains, les risques de subir un préjudice sont trop élevés ce qui les amènent à renoncer à faire des transactions sur Internet.

La confiance et la notion du risque

Ce calcul coût/bénéfice repose sur un élément essentiel : la confiance qui se traduit par un sentiment de sécurité face à quelqu'un ou quelque chose. C'est sur ce concept que repose toute relation d'échange (Choux et Perrien, 2004). La confiance est une mesure complexe ayant plusieurs dimensions. Dépendant de l'angle d'approche, la confiance peut être vue de diverses façons. Les psychologues voient la confiance comme un trait de personnalité, les sociologues la voient comme une structure sociale, les économiques la voient comme un mécanisme de choix (Bartikowski, Chandon et Müller, 2002). Pour le dire autrement, il serait réducteur de définir uniquement la confiance par une ou l'autre de ces dimensions. Dans le cadre de recherche portant sur le degré de confiance des Internautes relativement au site Web, Bartikowski, Chandon et Müller (2002) arrivent à la conclusion qu'il y a deux principales dimensions qui déterminent la confiance. La première porte sur les croyances constitutives de la confiance, c'est-à-dire la perception de l'individu face aux sites Web. La seconde porte sur l'intention d'engagement dans une relation de confiance. Il s'agit de déterminer jusqu'à point l'individu est prêt à s'investir dans une relation avec le site Web.

Par ailleurs, McKnight, Kacmar, Choudhury (2004) mentionnent que la confiance et la méfiance ne sont pas seulement les extrémités d'un même construit. Il s'agirait, selon ces chercheurs, de deux construits distincts qui provoque des comportements différents. La méfiance serait basée sur la peur et l'inquiétude tandis que la confiance est basée sur un sentiment de calme et de sécurité. Ces chercheurs rajoutent qu'un individu développe un sentiment de méfiance lorsqu'il est dans une situation où il perçoit un risque élevé. La méfiance est donc intrinsèquement liée à un risque perçu. Cette constatation rejoint celle émise par Frewer (2003) qui affirme que la confiance du public est un élément important du concept de l'amplification sociale du risque puisqu'il y a un lien entre la confiance et la gestion des risques. Par ailleurs, Frewer (2003) mentionne que la confiance est un élément variable qui dépend de plusieurs facteurs : la source de l'information, les variables personnelles, les variables démographiques et les variables sociales.

MÉTHODOLOGIE

Comme le souligne Rosa (2003) le risque se présente de moins en moins comme une donnée objective, mais de plus en plus comme une construction sociale. En d'autres mots, un fait social résulte de la signification que lui accorde chaque individu (Leman Langlois, 2007) et les connaissances de chacun ne sont pas la copie de la réalité, mais plutôt une construction que les sujets font de cette réalité. Dans cette optique, l'objectif de notre recherche est de décrire de quoi dépend la confiance des Québécois par rapport à la sécurité de leurs données personnelles sur Internet, mais d'un point de vue constructiviste. C'est-à-dire, en terme simple, que les connaissances et les perceptions de chacun ne sont pas représentatives de la réalité, mais sont plutôt une reconstruction de celle-ci. Il s'agit en fait d'un paradigme qui aborde un fait social d'après la construction sociale de leur signification (Leman-Langlois, 2006).

Selon cette approche constructiviste, l'explication d'un tel phénomène ne peut pas être circonscrite en un seul élément de réponse. Vu le manque de recherche sur le sujet, nous n'avons pas de balises pour nous guider dans notre démarche méthodologique puisque nous n'avons pas trouvé d'hypothèses ou des théories sur le sujet qui accorderaient une importance

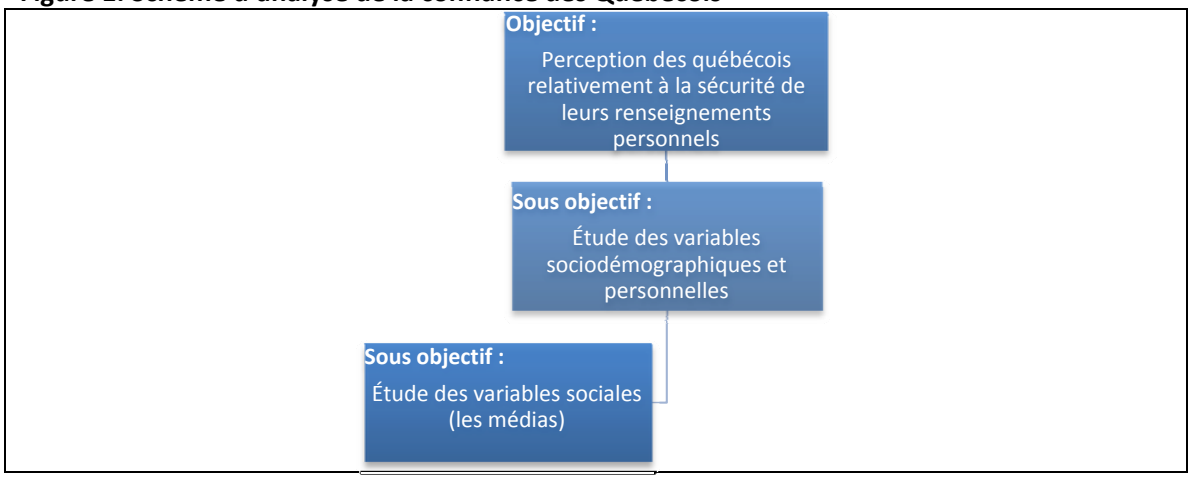
particulière à des facteurs spécifiques. Nous nous proposons alors de mener une recherche exploratoire et descriptive où nous nous intéressons à différents types de variables (personnelles, sociodémographiques et sociales).

Par ailleurs, afin d'arriver à notre objectif de recherche, nous avons besoin des informations suivantes qui sont présentées à la figure 1 :

1. D'effectuer un examen des associations entre les degrés de confiance vis-à-vis une diversité d'institutions et des variables sociodémographiques et personnelles.
2. D'effectuer un examen plus général de la représentation des risques dans les médias québécois.

La combinaison d'un devis de recherche quantitatif et qualitatif s'est avérée nécessaire pour rendre compte de notre objectif. L'emploi d'une base de données nous a permis de répondre à notre premier sous objectif et l'analyse documentaire nous a permis de répondre à notre second sous objectif.

Figure 1. Schème d'analyse de la confiance des Québécois



Sondage sur le vol d'identité

En 2007, Benoît Dupont, titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie, en collaboration avec la Direction de la prévention et de la lutte contre la criminalité (ministère de la Sécurité publique), ont élaboré un questionnaire sur le vol d'identité et la cybercriminalité. Ce questionnaire, comprenant 36 questions, a été administré à un échantillon de 1100 québécois, du 17 au 30 septembre 2007.

Dans le cadre de notre recherche, nous nous sommes intéressés à une question spécifique : « Faites-vous confiance aux organisations suivantes pour prévenir et contrôler la criminalité sur Internet? » :

- la police;
- les tribunaux;
- les organismes de protection des consommateurs et de la vie privée;
- les services gouvernementaux;
- les institutions financières;

- les fournisseurs d'accès à Internet;
- les entreprises qui offrent des services sur Internet;
- les fabricants d'équipements informatiques et de logiciels.

Nous avons opté d'analyser ces réponses en fonction de six variables sociodémographiques ou personnelles qui étaient comprises dans ce questionnaire. Pour chacune des catégories de réponse nous avons mis entre parenthèses le nombre d'individus y appartenant. Ces variables sont : la victimisation, le niveau de revenu, l'âge, le niveau de scolarité, le sexe et la consommation d'Internet à des fins personnelles.

1) la victimisation;
   Cette variable se compose de six sous variables dichotomiques. fraude sur un site d'encan en ligne (8);
   a) fraude financière par l'entremise d'un courriel afin d'obtenir plus d'argent (4);
   b) fraude par l'entremise d'un courriel afin d'obtenir un prix (5);
   c) intrusion informatique (50);
   d) menace ou intimidation sur Internet (5).
   e) Fraude par l'entremise d'un courriel qui recommande d'acheter des actions de la bourse (0).

2) le niveau de revenu :
   Il s'agit d'une variable catégorielle concernant le revenu familial avant impôt qui est divisée de la façon suivante :
   a) moins de 20 000 $ (207);
   b) 20 000 $ à 39 999 $ (263);
   c) 40 000 $ à 59 999 $ (187);
   d) 60 000 $ à 79 999 $ (117);
   e) 80 000 $ et plus (137);
   f) Refus (192).

3) l'âge;
   Il s'agit d'une variable catégorielle qui est divisée de la façon suivante :
   a) 19 ans à 24 ans (48);
   b) 25 ans à 34 ans (145);
   c) 35 ans à 44 ans (212);
   d) 45 ans à 54 ans (258);
   e) 55 ans à 64 ans (193);
   f) 65 ans et plus (232);
   g) Refus (12).

4) niveau de scolarité;
   Il s'agit d'une variable catégorielle qui est divisée de la façon suivante :
   a) primaire (88);
   b) secondaire (461);
   c) collégiale (257);
   d) universitaire (277);
   e) refus (17).

5) le sexe;
   Il s'agit d'une variable dichotomique.
   a) Homme (410);
   b) femme (690).

6) la consommation d'Internet à des fins personnelles;
   Les catégories sont réparties de la façon suivante :
   a) moins de 5 heures (823);
   b) entre 5 heures et 10 heures (168);
   c) entre 11 heures et 20 heures (69);
   d) plus de 20 heures (40).

À l'aide du logiciel SPSS (*Statistical Package for the Social Sciences)*, nous avons effectué des analyses bivariées, et plus spécifiquement des tableaux croisés. Ce type d'analyse nous a permis de tester l'hypothèse selon laquelle il existe une association entre deux variables catégorielles. Nous avons pris les huit institutions comme variables dépendantes et les six variables sociodémographiques et personnelles comme variables indépendantes. Afin de déterminer l'existence d'une association entre nos variables, nous avons regardé la signification de nos résultats, c'est-à-dire si la relation observée entre nos données est le fruit du hasard ou non. Dans le cadre de notre recherche, nous avons établi notre seuil de significativité en deçà de 0,05 ce qui signifie que nous avons moins de 5 chances sur 100 de nous trompé en affirmant une association entre les variables. Par ailleurs, nous avons dû retirer la variable victimisation de nos analyses, car la faible proportion d'individus victimisés ne permettant pas d'effectuer des analyses statistiques.

Analyse documentaire

À des fins complémentaires, nous nous sommes proposé d'effectuer une analyse documentaire sur les informations véhiculées par les médias concernant la sécurité des données personnelles. Afin d'analyser la somme des informations colligées lors de notre analyse documentaire, nous avons décidé de procéder à de l'analyse thématique. Le repérage constitue une fonction de cette méthode d'analyse, la tâche étant de relever tous les thèmes pertinents en lien avec nos objectifs (Paillé et Mucchielli, 2003).

Les médias sont une importante source d'information et ils sont des plus accessibles. Nous nous sommes donc intéressés au contenu qu'ils livrent relativement à la sécurité des informations personnelles sur Internet. Nous avons utilisé la base de donnée Eureka.cc (biblio branchée) afin de compiler les articles des médias québécois portant sur la sécurité des données personnelles sur Internet. Nos mots clés pour effectuer nos recherchent étaient les suivants :

- sécurité;
- données personnelles;
- renseignements personnels;
- vol d'identité;
- Internet

Notre période de référence étant de septembre 2006 à septembre 2007, soit l'année précédent le sondage sur le vol d'identité. Au total, 195 documents sont ressortis de la recherche. Après un examen minutieux de tous ces articles nous en avons retenu uniquement 25 qui traitaient spécifiquement de notre sujet.

RÉSULTATS

Partant de la prémisse que la confiance relève d'une construction que les sujets se font de la réalité, il est intéressant de s'attarder à une diversité de variables afin de vérifier cette hypothèse. Notre analyse de scinde en trois principaux points. Premièrement, nous décrivons le degré de confiance des Québécois envers les huit institutions énumérées précédemment. Deuxièmement, afin d'expliquer cette confiance, nous présentons les résultats des associations statistiques entre les degrés de confiance et des variables sociodémographiques et personnelles. Troisièmement, à titre complémentaire, nous terminons avec un examen général de la représentation des risques dans les médias québécois.

Le degré de confiance des Québécois relativement à diverses organisations

La confiance est un concept relatif et variable qui n'est pas distribué également entre les institutions. Certaines institutions évoquent un plus grand sentiment de sécurité que d'autres au sein de la population. À cet effet, Roberts (2004), a publié un rapport à l'intention de la Sécurité publique et Protection civile Canada, qui nous renseigne sur le degré de confiance exprimé par les Canadiens à l'égard de plusieurs institutions publiques. Les résultats ont été obtenus lors de l'enquête sociale générale (ESG) de 2003. Lors de cette enquête, les répondants avaient le choix entre quatre degrés d'appréciation soit : très grande confiance, grande confiance, peu confiance et pas du tout confiance. Il est à noter que dans le cadre de notre étude, nous avons regroupé ces quatre catégories pour en faire que deux : confiance accordée et confiance refusée. Le tableau 1 fournit les résultats en ordre décroissant de confiance.

Tableau 1. Degré de confiance des Canadiens relativement à diverses organisations. Résultats de l'ESG de 2003 (Roberts, 2004).

Organisations	Confiance accordée (%)	Confiance refusée (%)
police	83	17
Entreprises locales	80	20
Banques	68	32
Régimes de soins de santé	67	33
Système scolaire	65	35
Système de justice	57	43
entreprises	46	54
Parlement	43	57
Système d'aide sociale	41	59

La police constitue l'organisation ayant le plus la confiance du public (83 %) tandis que le système d'aide social est celle ayant le plus faible degré de confiance accordé (41 %). Il s'agit ici d'un degré de confiance global envers ces organismes. Il est donc intéressant de comparer ces résultats avec l'étude de Dupont (2008) qui porte sur des points spécifiques.

Comme il a été mentionné antérieurement, le sondage sur le vol d'identité (Dupont, 2008) comprend des questions relatives à la confiance du public envers huit types d'organisation, dans la capacité de prévenir et contrôler la criminalité sur Internet. Nous retrouvons au tableau 2 les résultats en ordre décroissant de confiance.

Il est intéressant de noter que les trois organisations ayant le plus faible degré de confiance sont toutes directement reliées au domaine de l'informatique. Au dernier rang, nous retrouvons les entreprises qui offrent des services Internet (22,2 %), suivi des fournisseurs d'accès Internet (37,6 %), et des fabricants d'équipements informatiques et de logiciels (40,5 %). Aux rangs médians, nous retrouvons les services gouvernementaux (55,7 %), et les tribunaux (56,3 %) suivi au troisième rang des organismes de protections des consommateurs et de la vie privée (66 %). Au second rang, nous retrouvons la police (66,5 %) et finalement les institutions financières (68,5 %) sont les organisations ayant le plus haut degré de confiance du public.

Tableau 2. Degré de confiance des Québécois relativement à diverses organisations. Résultats du sondage sur le vol d'identité (Dupont, 2008).

organisations	Oui		non	
	n	%	n	%
Institutions financières	753	68,5	347	31,5
La police	731	66,5	369	33,5
Les organismes de protections des consommateurs et de la vie privée	726	66,0	374	34,0
Les tribunaux	619	56,3	481	47,7
Services gouvernementaux	613	55,7	487	44,3
Fabricants d'équipements informatiques et de logiciels	446	40,5	654	59,5
Fournisseurs d'accès à Internet	414	37,6	686	62,4
Entreprises qui offrent des biens et des services sur Internet	244	22,2	856	77,8

Comme le souligne Dupont (2008), le fait que les institutions financières occupent le premier rang des organisations ayant la confiance du public est assez inattendu. Cependant ce résultat démontre une correspondance avec l'étude de Roberts (2004). De plus, nous pouvons aussi expliquer ce haut degré de confiance par le fait que ce type d'institution a tout intérêt à protéger les renseignements de ses clients ainsi que d'offrir des moyens adaptés pour lutter contre la cybercriminalité. En date du 23 novembre 2009, nous avons consulté la page Web de la banque RBC Banque royale et nous avons regardé la rubrique Protection des renseignements et sécurité. Nous pouvons lire sur cette page : « la protection de vos renseignements personnels et financiers constitue la pierre angulaire de notre entreprise et demeura toujours l'une de nos priorités »[2]. En naviguant sur le site, nous retrouvons une diversité de renseignements concernant les mesures que l'institution prend pour protéger les renseignements de ses clients et nous retrouvons aussi une liste de conseils pour préserver notre sécurité informatique. Bref, cette institution démontre un intérêt marqué pour la sécurité des données personnelles de ses usagers. Toutefois, une question reste en suspend à savoir si cette présentation flatteuse

[2] http://www.rbc.com/rensperssecurite/ca/

s'accompagne d'une efficacité avérée dans ce domaine. Il serait donc intéressant dans des recherches subséquentes de s'attarder à cette question.

Par ailleurs, un résultat qui est des plus surprenants concerne le degré de confiance accordé à la police dans la prévention et le contrôle de la cybercriminalité et le vol d'identité. La police arrive au second rang des institutions ayant la confiance du public quand, dans les faits, il y a approximativement 245 policiers au Canada qui sont affectés à la cybercriminalité (Presse canadienne, 14 septembre 2006). Ce degré de confiance nous apparaît irréaliste compte tenu du nombre très limité d'effectifs attitré à cette tâche, mais il concorde avec les résultats obtenus par Roberts (2004). Ce dernier affirme que la police arrive au premier rang des institutions ayant la confiance générale de la population canadienne avec un pourcentage de 83 %. Ce constat reflète le fait que la confiance résulte d'une construction que les individus se font de la réalité et que cette construction ne sont fonde pas nécessairement sur des faits objectifs.

En ce qui concerne, les trois organisations qui fournissent les infrastructures nécessaires au bon fonctionnement d'Internet, elles se retrouvent au bas de la hiérarchie de la confiance accordée. Comment l'explique Dupont « ce manque de confiance reflète certainement la perception du manque d'intérêt des entreprises concernées pour la question de sécurité… » (2008 : 23). Pour le dire autrement, la confiance des gens correspond à un miroir de leur perception de cette réalité et que ce construit résulte d'une diversité de facteurs.

Le degré de confiance en lien avec les variables personnelles et sociodémographiques

Tout d'abord, les femmes font davantage confiance ont diverses institutions que les hommes. En effet, elles font davantage confiance à la police (+ 11 %), aux tribunaux (+ 8,7 %), aux organismes de protection des consommateurs et de la vie privée (+10,7 %) et aux services gouvernementaux (+12,6 %) que les hommes. Il est à noter que les femmes font aussi davantage confiance aux quatre autres institutions que les hommes, mais les associations ne sont statistiquement significatives. Le manque de recherche sur le sujet ne nous a pas permis de constater si cette différence entre les hommes et les femmes a déjà été observée. Sans comparer ce résultat au nôtre, nous savons selon Statistique Canada (2003) que les femmes feraient moins confiance aux gens en général que les hommes (- 3 %).

Ensuite, concernant le revenu familial, nous avons constaté que les répondants ayant un revenu annuel supérieur à 80 000 $ font moins confiance aux tribunaux (-9 %), mais font davantage confiance aux fournisseurs d'accès à Internet (+12 %) que le reste de l'échantillon. Ici, il est intéressant de noter une différence avec les données de Statistiques Canada (2004) portant sur la confiance générale envers les institutions, puisque ce même groupe de répondants fait plus confiance à la police (+10,8 %), au système de la santé (+5,2 %) et aux tribunaux (+10,7 %). Donc, d'un côté les gens ayant un revenu supérieur ont davantage confiance envers les tribunaux, mais lorsqu'il est question de la protection des renseignements personnels et de la lutte contre la cybercriminalité, le degré de confiance décroît.

Par ailleurs, nous avons observé une association statistiquement significative entre le revenu familial et la scolarité des répondants. Les répondants ayant un revenu plus faible étaient ceux le moins scolarisés Cette association positive vient donc créer un effet de triangulation entre le revenu familial, le degré de confiance et la scolarité des répondants. Il devient donc impossible

d'affirmer si c'est le revenu ou le niveau de scolarité qui est associé au degré de confiance des répondants. Cependant, nous avons observé des associations statistiquement significatives entre le niveau de scolarité et le degré de confiance envers certaines institutions qui ne l'étaient pas avec le revenu familial. En effet, les répondants ayant un niveau de scolarité primaire font moins confiance aux organismes de protection des consommateurs et de la vie privée (-12,8 %), aux services gouvernementaux (-10,7 %), aux institutions financières (-21,4 %), aux fabricants d'équipements informatiques (-23 %) que le reste de l'échantillon. Bref, ces résultats nous indiquent que les répondants étant moins scolarisés sont moins enclins à faire confiance aux institutions. De plus, selon des résultats émis par Statistique Canada (2004) ce groupe de la population fait moins confiance aux gens que ceux ayant atteint de niveau de scolarité plus élevée (-26 %).

Il a aussi été observé que les personnes âgées (plus de 65 ans) font moins confiance aux fournisseurs d'accès à Internet (-21,2 %), aux entreprises qui offrent des services sur Internet (-16,6 %) et aux fabricants d'équipements informatiques (-34,2 %) que le reste de l'échantillon. Ce manque de confiance envers ces institutions peut s'expliquer par le fait que les aînées sont ceux qui utilisent le moins Internet et l'ordinateur en général (Statistique Canada, 2009). Les générations X, Y et même les baby-boomers ont évolué avec les technologies informatiques tandis que pour les aînés il s'agit d'une toute nouvelle réalité à laquelle ils doivent s'adapter. Il est donc normal que ce groupe de la population soit plus méfiant à l'égard des technologies.

La dernière variable étudiée concerne la consommation d'Internet à des fins personnelles. Nous avons observé que les personnes consommant plus de 20 heures par semaine font davantage confiance aux fournisseurs d'accès à Internet (+11,2 %), aux entreprises qui offrent des services sur Internet (+13,2 %) et aux fabricants d'équipements informatiques (+26,3 %) que le reste de l'échantillon. Nous pouvons tirer deux conclusions à ce constat. D'une part, nous pouvons croire que les plus grands consommateurs d'Internet font confiance aux institutions qui en assurent le bon fonctionnement sinon pourquoi passeraient-ils autant d'heures sur Internet? D'une autre part, nous pouvons tout simplement croire à un certain utilitarisme de la part des usagers face à ces institutions puisqu'ils en tirent des bénéfices.

En bref, nous avons pu observer que la confiance envers les institutions ne se répartit pas de façon identique parmi tous les groupes de l'échantillon. Nous retrouvons des éléments de réponse ici et là sans toutefois cerner de façon précise de quoi dépend la confiance des Québécois par rapport à la sécurité de leurs données personnelles sur Internet. Certaines caractéristiques sociales et démographiques influencent pour des raisons diverses la manière dont les personnes se représentent le phénomène de la protection de leurs données personnelles. Il s'agit en fait d'une perception d'une réalité plutôt que la représentation de faits objectifs. Ici, il importe de préciser que les résultats présentés ne sont pas généralisables à une échelle microscopique. Par exemple, nous ne pouvons pas affirmer qu'une personne âgée ne fait pas confiance aux institutions qui assurent le bon fonctionnement d'Internet, mais nous pouvons affirmer que règle générale les personnes âgées accordent moins de crédit à ce type d'institution. La nuance entre les deux s'avère être primordiale afin de bien comprendre la perception des Québécois relativement à la sécurité de leurs données personnelles.

La représentation des risques dans les médias québécois

Comme il vient d'être mentionné, la confiance est une variable qui n'est pas distribuée également au sein de la population. Il y a des groupes qui font plus confiance à certaines institutions et les variables démographiques et personnelles ne semblent pas rendre compte du phénomène à elles seules. Dans cette optique, nous nous sommes intéressés à une autre forme de variable, soit les médias. Nous trouvions intéressant d'effectuer un examen plus général de la représentation des risques dans les médias québécois puisque ces derniers sont souvent identifiés comme étant la source d'amplification du risque et de la peur du crime (Heath et Gilbert, 1996; Altheide, 1997). De plus, comme le souligne Altheide (1997) les médias de masse sur représentent certains risques ce qui fait que la population se fait une perception erronée d'une problématique. Toutefois, comme le mentionnent Heath et Gilbert « Media messages do net affect all of the people all of the time, but some of the messages affect some of the people some of the time » (1996 : 385).

Les médias de masse sont de plus en plus accessibles et populaires et par leurs diverses formes, ils sont devenus de puissants véhicules d'information. Suivant cette logique nous avons décidé d'explorer la représentation des risques relativement à la sécurité des données personnelles sur Internet qu'ils diffusent. Contre toute attente, nous avons observé que les articles de journaux analysés ont un discours favorable à l'égard de la sécurité des données personnelles sur Internet quoique leur nombre nous a apparu très limité. En effet, sur une période d'un an, uniquement 25 articles, paru dans six journaux différents[3], ont traité de ce sujet et certains d'entre eux abordaient très furtivement la question d'Internet. Ce nombre très limité d'articles a donc rendu notre analyse thématique plus complexe. Étant incapables d'extraire des thèmes, nous avons décidé de présenter une vue d'ensemble des articles recensés.

Il s'en dégage que la majorité des articles recensés ont mentionné qu'il n'y avait aucune inquiétude à avoir concernant la sécurité des données personnelles sur Internet. À cet effet, nous avons sélectionné ces informations :

- « Paradoxalement, quand vous mettez des données sur Internet, c'est souvent les segments plus sécuritaires » (Le Soleil, 20 janvier 2007).
- Les factures électroniques réduisent les risques de vol d'identité (La Presse, 18 février 2007).
- Dans un article faisant le point sur la panne de service de Revenu Canada, nous pouvons lire les propos suivants : « la sécurité et la confidentialité des renseignements ont été protégées constamment et n'ont en aucun temps été compromises pendant la suspension préventive des services en ligne » (La Presse, 18 mars 2007).

En aucun cas, nous n'avons identifié un discours alarmiste relativement à la sécurité des données personnelles sur Internet. Certains articles mentionnaient que la perte des données est un sujet plus préoccupant que la sécurité des données sur Internet (Le Devoir, 14 décembre 2006; Le Soleil, 20 janvier 2007). Un autre article paru dans La Presse Canadienne (20 avril 2007) nous informe que l'agence de publicité DoubleClik ne suit pas les normes du gouvernement et de l'industrie publicitaire protégeant la vie privée. Bref, les médias analysés n'ont en aucun cas amplifié les risques, nous pourrions même dire qu'ils les ont atténués.

[3] Les six journaux sont : La Presse, Le devoir, Le droit, Le soleil, Le temps, L'express.

Nous ne pouvons pas nier que la divulgation de renseignements personnels sur Internet comporte certains risques puisque ce médium est un réseau ouvert à quiconque le désire. Il est donc possible pour un individu ayant les connaissances nécessaires d'intercepter des données personnelles pendant leur transfert d'un site à un autre ou en apposant un logiciel malveillant dans notre ordinateur.

La question ici n'est pas d'énumérer les techniques qui viennent compromettre la sécurité des données personnelles, mais bien d'illustrer qu'Internet n'est pas un château fort pour nos données. Toutefois, les médias ne semblent pas prêter attention à cette réalité ce qui nous porte à la réflexion. En effet, le sujet semble sous représenté ce qui porte à réflexion.

CONCLUSION

Il s'en dégage que la confiance des Québécois par rapport à la sécurité de leurs données personnelles sur Internet repose sur une diversité de facteurs. Certaines variables personnelles et démographiques sont ressorties comme étant associées à la confiance envers certaines institutions, mais nous croyons que cette association résulte plutôt d'une série d'interactions positives et négatives que vivent certains groupes de la population. Par exemple, les personnes qui consomment plus de 20 heures par semaine d'Internet vivent des expériences positives lors de leur navigation. Il en résulte que leur perception relativement aux institutions assurant le bon fonctionnement du réseau est favorable. La confiance repose donc sur une série d'interactions vécues par des sujets que ça soit au contact d'autres personnes, d'expériences personnelles ou de messages véhiculés par différents médias. Pour le dire autrement, les interactions vécues par les sujets sont un facteur important de leur perception de la confiance envers les institutions.

Rétrospectivement, nous croyons qu'il serait intéressant de poursuivre cette recherche en adoptant un cadre théorique plus interactionniste ce qui viendrait nous aider à comprendre jusqu'à quel point les interactions vécues ont un impact sur la confiance accordée. À cet effet, la théorie de l'interactionnisme symbolique de George Blumer (1969) nous semble tout indiqué. Théorie qui met l'accent sur le fait que nos interprétations de la réalité sont le fruit de ce que nous avons appris des autres qui nous entoure.

De plus, nous sommes conscients que les médias sélectionnés dans cette recherche sont très limités et peu diversifiés. Il serait donc intéressant de prendre un plus grand échantillon de sources médiatiques afin de déterminer si la sécurité des données personnelles est un sujet qui est bel et bien sous représenté.

Références

Altheide, D. L. (1997). The new media, the problem frame, and the production of fear. *The sociological quarterly.* 38 (4) : 647-668.

Bartikowski, B., Chandon, J-L. et Müller, B. (2008). Mesurer la confiance des Internautes par rapport aux Sites Web marchands : Adaptation de McKnight, Kacmar et Choudhury (2002). Consulté le 16 novembre 2009 sur http://www.escp-eap.net/conferences/marketing/2008_cp/Materiali/Paper/Fr/Bartikowski_Chandon_Muller.pdf

Blumer, H. (1969). *Symbolic Interactionnism : Perspective and method,* Berkeley, University of California Press (1986).

Castells, M. (2001). Chapitre 1 : ce que nous apprend l'histoire d'Internet. *La galaxie Internet*. Paris : Fayard, 18-49.

Choux, I. et Perrien, J. (2004). Les facteurs expliquant la confiance du consommateur lors d'un achat sur un site marchand : une étude exploratoire. *Décisions maketing*. 35. 75-86.

Cohen et Felson (1979). Social change and crime rate trends: a routine activity approach. *American sociological review*. 44: 588-605.

Dryburgh, H. (2001). *Le temps changent : pourquoi les canadiens utilisent Internet.* Statistique Canada. Nº56F0006XIF au catalogue.

Dupont, B. (2008). Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec. Ministère de la Sécurité Publique.

Dupont, B. et Gagnon, B. (2008). La sécurité précaire des données personnelles en Amérique du Nord : Une analyse des statistiques disponibles. Note de recherche no. 1 de la Chaire de recherche du Canada en Sécurité, identité et technologie. Montréal.

Frewer, L. (2003). Trust, transparency, and social context: implication for social amplification of risk. Dans N. Pidgeon, R. Kasperson, P. Slovic. *The social amplification risk.* (123-137). Cambridge University Press.

Haggerty. K. (2003). From risk to precaution: the rationalities of personal crime prevention. Dans Richard V. Ericson et Aaron Doyle: *Risk and morality* (193-214). Tontonto: University of Toronto Press.

Heath, L. et Gilbert, K. (1996). Mass Media and fear of crime. *American behavioral scientist*. 39 : 379-386.

Institut de la sécurité de l'information du Québec (2007). *Semaine de la sécurité de l'information au Québec du 11 au 15 juin 2007.* Consulté le 25 octobre 2009 sur https://www.isiq.ca/entreprise/publications/presentations/presentations_pdf/isiq_pres-semaine_si_quebec_citoyens.07.pdf

Leman Langlois, S. (2007). *La sociocriminologie.* Les presses de l'Université de Monréal.

Los, M. (2006). Looking into the future: surveillance, globalization and totalitarian potential. Dans D. Lyon: *Theorizing surveillance. The panopticon and beyond* (p.69- 94). Cullompton : William Publishing.

Lynch, D. et Lundquist, L. (1996). *Digital money : the new Era of Internet commerce.* John Wiley & Sons, New York, NY.

Poussart, B. (2001). L'utilisation d'Internet par les ménages québécois en 2000. Institut de la statistique du Québec. Consulté le 7 novembre 2009, sur http://www.stat.gouv.qc.ca/publications/savoir/pdf/analyse2000.pdf.

McKinght, D.H., Kacmar, C.J. Choudhury, V. (2004). Dispositional trust and distrust dinstinctions in predicting high-and low risk Internet Expert advice site perceptions. *E-service journal*. 35-58.

Roberts, J. V. (2004). *La confiance du public dans la justice pénale : bilan des dernières tendances 2004-05.* Rapport à l'intention de Sécurité publique et Protection civile Canada. Consulté le 18 novembre 2009, sur http://www.publicsafety.gc.ca/res/cor/rep/_fl/2004-05-pub-conf-fra.pdf

Rosa, E. A. (2003). The logical structure of the social amplification of risk framework (SARF): Metatheoretical foundations and policy implications. Dans N. Pidgeon, R.E. Kasperson et P. Slovic, *The Social Amplification of RISK* (p.47-79), Cambridge: university press.

Statistique Canada (2004). *Enquête sociale générale de 2003 sur l'engagement social, cycle 17: un aperçu des résultats.* Nº89-598-XIF au catalogue.

Statistique Canada (2009). *Les activités en ligne des baby-boomers et des aînés canadiens.* Nº11-008-X au catalogue.