PROTECTION DE LA VIE PRIVÉE EN LIGNE

Les consommateurs comme acteurs

union des consommateurs

Rapport final du projet de recherche présenté par Union des consommateurs au Bureau de la consommation d'Innovation, Sciences et Développement économique Canada

Octobre 2021

L'ÉQUIPE

RÉDACTION DU RAPPORT

Union des consommateurs

RECHERCHE ET RÉDACTION

Anaïs Beaulieu-Laporte

DIRECTION DE RÉDACTION

Marcel Boucher

COLLABORATION

Merci aux professeurs Ignacio Cofone et Céline Castets-Renard ainsi qu'aux Mes Cynthia Chassigneux et Julien Lamalice.

7000, avenue du Parc, bureau 201
Montréal (Québec) H3N 1X1
Téléphone : 514 521-6820
Télécopieur : 514 521-0736
info@uniondesconsommateurs.ca
www.uniondesconsommateurs.ca

Organismes membres d'Union des consommateurs :

ACEF Appalaches Beauce Etchemins	ACEF de l'Est de Montréal
ACEF de l'Île Jésus	ACEF du Grand-Portage
ACEF du Nord de Montréal	ACEF du Sud-Ouest de Montréal
ACEF Estrie	ACEF Lanaudière
ACEF Montérégie-Est	ACEF Rive-Sud de Québec
ACQC	Centre d'éducation financière
CIBES de la Mauricie	EBO
	SAC de la Mauricie

LE RAPPORT

Union des consommateurs a reçu du financement en vertu du Programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Innovation, Sciences et Développement économique Canada. Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Innovation, Sciences et Développement économique Canada ou du gouvernement du Canada.

L'usage du masculin, dans ce rapport, a valeur d'épicène.

UNION DES CONSOMMATEURS,

La force d'un réseau

Union des consommateurs est un organisme à but non lucratif qui regroupe 14 groupes de défense des droits des consommateurs.

La mission d'UC est de représenter et défendre les droits des consommateurs, en prenant en compte de façon particulière les intérêts des ménages à revenu modeste. Les interventions d'UC s'articulent autour des valeurs chères à ses membres : la solidarité, l'équité et la justice sociale, ainsi que l'amélioration des conditions de vie des consommateurs aux plans économique, social, politique et environnemental.

La structure d'UC lui permet de maintenir une vision large des enjeux de consommation tout en développant une expertise pointue dans certains secteurs d'intervention, notamment par ses travaux de recherche sur les nouvelles problématiques auxquelles les consommateurs doivent faire face ; ses actions, de portée nationale, sont alimentées et légitimées par le travail terrain et l'enracinement des associations membres dans leur communauté.

Union des consommateurs agit principalement sur la scène nationale, en représentant les intérêts des consommateurs auprès de diverses instances politiques ou réglementaires, sur la place publique ou encore par des recours collectifs. Parmi ses dossiers privilégiés de recherche, d'action et de représentation, mentionnons le budget familial et l'endettement, l'énergie, les questions liées aux télécommunications, à la radiodiffusion, à la télédistribution et à l'Internet, santé, les produits et services financiers ainsi que les politiques sociales et fiscales.

TABLE DES MATIÈRES

LEXIQUE

Quelques termes de base du numérique [1]

Termes français	Termes anglais (lorsque plus connus)	
Internet		Réseau informatique mondial constitué d'une multitude de réseaux (publics et privés), qui permet à partir d'une connexion locale, la communication entre ordinateurs et serveurs au moyen de protocoles standardisés.
World Wide Web (www)		Application d'Internet qui permet la navigation sur le réseau au moyen d'un système d'hypertextes. Par extension, le Web est généralement compris comme l'ensemble des sites Web accessibles par le biais de cette application.
Adresse IP		Numéro unique qui sert à identifier et localiser un appareil connecté à Internet.
Système d'exploitation		Logiciel qui sert à gérer le fonctionnement d'un appareil (ordinateur, téléphone intelligent, tablette, « objet connecté ») et l'exécution de ses programmes.
Application		Logiciel ou programme dont se sert un internaute afin de réaliser une tâche ou activité précise au moyen d'un appareil.
Navigateur		Logiciel qui permet de consulter les sites Web et d'accéder aux moteurs de recherche.
Moteur de recherche		Programme qui indexe le contenu des sites Web et qui permet de faire des recherches et d'accéder au contenu à partir de mots-clés.
Module d'extension / Extension de navigation	*Plug-in*	Logiciel qui se greffe à un autre logiciel afin d'offrir de nouvelles fonctionnalités.

[1] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. Le grand dictionnaire terminologique, en ligne : http://gdt.oqlf.gouv.qc.ca/index.aspx ; LAROUSSE. Dictionnaire de français, en ligne : https://www.larousse.fr/ BUREAU DE TRADUCTION DU CANADA. Termium plus, en ligne : https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&index=alt ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. Technologie, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/

Objet-fenêtre	*Widget*	Petite application qui s'intègre directement à une page Web ou à un système d'exploitation et qui offre du contenu additionnel (ex : calendrier, météo).
Mégadonnées	*Big data*	Grand ensemble de données provenant de sources multiples et dans des formats variés dont le traitement croisé permet de nouvelles possibilités d'exploration, de recoupement et de déduction.
Algorithme		Suite d'instructions ou d'opérations appliquée à des données qui permet de résoudre un problème, de tirer des inférences, etc.
Intelligence artificielle (IA)	*AI*	Système conçu pour permettre à une machine de reproduire des facultés cognitives humaines (ex. : reconnaissance, analyse, calcul).
Chiffrement / Cryptage		Transformation d'un texte clair en un texte inintelligible et inexploitable par quiconque ne possède pas la clé de déchiffrement
Témoin	*Cookie*	Petit fichier transmis par un serveur au navigateur lors de la consultation d'un site Web qui stocke des données relatives à l'utilisation du site Web par l'internaute. Parfois décrit comme la mémoire du navigateur.
Fenêtre publicitaire ou contextuelle	*Pop-up*	Fenêtre publicitaire non sollicitée qui s'ouvre automatiquement sur certains sites Web.

Quelques acronymes juridiques

Francophones	Anglophones	
-	*APIPA*	*Personal Information Protection Act* (loi de l'Alberta)
-	*BCPIPA*	Personal Information Protection Act (loi de la Colombie-Britannique)
CAI	-	Commission d'accès à l'information (du Québec)
-	*CCPA*	*California Consumer Privacy Act of 2018* (loi de la Californie)
CPVP	OPC	Commissariat à la protection de la vie privée du Canada / Office of the Privacy Commissioner of Canada
	FTC	Federal Trade Commission (des États-Unis)
GT Art 29	Art 29 WP	Groupe de travail « Article 29 » (remplacé par le Comité Européen de la Protection des Données (CEPD/EDPB))

LCAP	*CASL*	*Loi canadienne anti-pourriel / Canada's anti-spam legislation*
LPRPDE	*PIPEDA*	*Loi sur la protection des renseignements personnels et les documents électroniques (loi du Canada) / Personal Information Protection and Electronic Documents Act*
LPRPSP	-	*Loi sur la protection des renseignements personnels dans le secteur privé* (loi du Québec)
LPVPC	*CPPA*	*Loi sur la protection de la vie privée des consommateurs / Canada's Consumer Privacy Protection Act* (loi élaborée dans le projet de loi C-11 du Canada)
-	*PIPITPA*	*Personal Information Protection and Identity Theft Prevention Act* (loi du Manitoba)
RGPD	*GDPR*	*Règlement général sur la protection des données / General Data Protection Regulation* (règlement de l'Union européenne)

INTRODUCTION

Pandémie oblige, les Canadiens utilisent Internet plus que jamais. Ils y travaillent ou y étudient. Ils s'y informent, s'y divertissent ou encore y magasinent. Ils y interagissent avec d'autres. Ils accèdent à du contenu en ligne et en créent à leur tour.

Avec ses quelque 1,88 milliard de sites Web[2], le réseau Internet permet ainsi l'accès et la diffusion d'information d'une tout autre ampleur qu'auparavant. 1,2 milliard de recherches sont effectuées sur *Google* chaque année[3]. 70 millions de publications sont diffusées chaque mois sur la plateforme de sites Web et de blogues *WordPress*[4]. Plus de 306 milliards de courriels sont échangés quotidiennement[5]. Près de 350 000 publications éphémères sont diffusées sur *Instagram* chaque minute[6].

Ces chiffres ont de quoi étourdir. Ils peuvent aussi être source d'inquiétude.

Parce que l'avènement du réseau Internet et son utilisation à large échelle ne sont pas sans conséquence pour l'exercice des droits de la personne, particulièrement du droit à la protection de la vie privée. Des experts estiment qu'en 2025, ce sera près de 463 trillions d'octets (soit l'équivalent de 212, 765, 957 DVDs) de données qui seront générés chaque jour sur le réseau[7]. Parmi ces données, on retrouve bon nombre de renseignements personnels, des renseignements collectés, exploités ou vendus par des entreprises, alors que les personnes concernées n'ont que très peu de contrôle sur ces activités.

Cette situation préoccupe de plus en plus les consommateurs d'après de nombreux sondages réalisés dans les dernières années. Or, ces sondages sont généralement américains et européens. Reflètent-ils le point de vue des consommateurs d'ici ? Notre recherche vise ainsi à apporter une perspective canadienne sur la question. Qu'est-ce qui préoccupe les consommateurs canadiens en ligne ? Leur vie privée et leurs renseignements personnels sont-ils adéquatement protégés en ligne, que ce soit par les mesures de protection qu'ils adoptent ou en raison des lois en place au pays qui sont censées y veiller ?

---

[2] Les évaluations varient entre 1,7 milliard et 1,88 milliard de sites Web : ARMSTRONG, M. « How Many Websites Are There? », Statista, 6 août 2021, en ligne : https://www.statista.com/chart/19058/number-of-websites-online/ ; WEBSITESETUP. « How Many Websites Are There en 2021 ? », en ligne : https://websitesetup.org/news/how-many-websites-are-there/ (consulté le 6 octobre 2021).
[3] INTERNET LIVE STATS. « Google Search Statistics », en ligne : https://www.internetlivestats.com/google-search-statistics/ (consulté le 6 octobre 2021).
[4] WORDPRESS. « A live look at activity across WordPress.com », en ligne : https://wordpress.com/activity/ (consulté le 6 octobre 2021).
[5] STATISTA. « Number of sent and received e-mails per day worldwide from 2017 to 2025 », 7 avril 2021, en ligne : https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/
[6] Publications de type *stories* : STATISTA. « Media usage in an internet minute as of August 2020 », en ligne : https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/ (consulté le 6 octobre 2021).
[7] DESJARDINS, J. « How much data is generated each day? », World Economic Forum, 17 avril 2019, en ligne : https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

Le présent rapport s'articulera en six temps. Nous tenterons d'abord de définir ce qu'est la vie privée, et ce, à partir des définitions proposées par certains auteurs et des conceptions de la vie privée retenues par les systèmes juridiques européen, américain et canadien.

Les deuxième et troisième parties du rapport seront consacrées à la documentation des préoccupations des consommateurs pour la protection de leur vie privée et de leurs renseignements personnels en ligne, ainsi que des mesures et comportements de protection qu'ils adoptent en vue de les protéger. Nous rapporterons notamment les résultats d'un sondage et d'entrevues réalisés à l'hiver 2020 auprès de consommateurs canadiens. Nous y traiterons également brièvement du paradoxe de la vie privée en ligne, tel que débattu dans la littérature.

Dans un quatrième temps, nous nous attarderons aux technologies d'amélioration de la confidentialité en ligne, dont l'utilisation est fortement recommandée par les experts, mais qui demeurent apparemment méconnues des internautes canadiens. Nous analyserons la présentation des différents outils offerts en ligne afin de voir dans quelle mesure elle permet aux consommateurs canadiens de comprendre l'utilité de ces outils et de dissiper la méfiance à leur égard.

Le tout sera suivi d'une analyse de la législation en vigueur au Canada en matière de protection des renseignements personnels. Quatre lois sont présentement applicables au secteur privé ; une loi fédérale et trois lois provinciales. Nous nous attarderons à la manière dont ces lois s'attaquent aux enjeux qui préoccupent les consommateurs, le cas échéant. Nous étudierons aussi leur compatibilité avec le comportement réel des consommateurs canadiens en ligne, tel que révélé par nos enquêtes.

Dans la sixième et ultime partie de notre rapport, nous rapporterons les points de vue d'experts issus du milieu académique canadien que nous avons consultés dans le cadre de la présente recherche. Que pensent-ils de l'approche législative canadienne ? De son traitement de la responsabilité des consommateurs et du consentement requis de ces derniers ? Nous aborderons avec eux une variété d'éléments dont les législateurs devront tenir compte dans le cadre de la révision prochaine des lois canadiennes que beaucoup jugent aujourd'hui désuètes.

Les conclusions de notre recherche seront suivies de nos recommandations.

Soulignons enfin que la présente étude se concentre sur la protection de la vie privée des internautes en regard du secteur privé et de la consommation et n'aborde pas les considérations relatives aux atteintes potentielles par l'État (surveillance policière, profilage à des fins politiques, etc.) ou par d'autres acteurs en position d'autorité (employeur, propriétaire, etc.).

LA VIE PRIVÉE : QUELQUES ÉLÉMENTS DE CONTEXTE

Définir la vie privée est complexe. À preuve, les auteurs et les disciplines ont produit une panoplie de définitions au fil du temps. Certaines des conceptions contemporaines de la vie privée seront abordées dans le présent chapitre, mais avant tout, il parait utile d'exposer brièvement la progression historique de la quête de vie privée chez les individus.

1.1 La petite histoire de la vie privée

La notion de vie privée serait apparue vers la fin du Moyen-Âge, alors qu'on commence peu à peu à distinguer l'espace privé de l'espace public. Avant cela, l'individu fait partie d'une collectivité avec qui il partage tous ses biens et prend toutes ses décisions[8].

Avec la montée de l'individualisme au 18e siècle en Angleterre, la notion de vie privée prend davantage de place[9]. On reconnait plusieurs espaces d'intimité, comme la famille, le journal intime, le bureau (le *study*) ou encore la garde-robe[10]. La popularisation et la démocratisation de la lecture contribuent également au développement d'un plus grand sentiment d'autonomie personnelle[11]. Mais la recherche de la solitude et le désir d'être à l'abri des regards demeurent très mal vus[12].

L'apparition subséquente des journaux de type tabloïd qui publicisent des potins sur des personnalités publiques donne lieu aux premières tensions entre vie privée et technologies des communications[13] - une tension encore bien présente aujourd'hui.

Le 19e siècle mènera à la consécration de la vie privée par le processus d'individualisation qui se poursuit (en raison des progrès médicaux et hygiéniques par exemple), la valorisation de la vie domestique et l'urbanisation (par cette nouvelle proximité du voisinage)[14].

---

[8] « Vie privée ? », L'Influx, décembre 2013, en ligne : http://www.linflux.com/societe/droit-justice/vie-privee/#
À noter que certains auteurs réfèrent aux écrits d'Aristote et d'autres penseurs grecs pour établir que la notion de vie privée était déjà présente durant l'Antiquité, en ce qu'on y distinguait les notions d'*oikos* (famille) et de *polis* (sphère publique et politique). Notons toutefois que l'*oikos* diffère considérablement du foyer familial tel qu'on le comprend aujourd'hui : KEULEN, S. et KROEZE, R. « Privacy from a Historical Perspective » dans VAN DER SLOOT, B. et DE GROOT, A., dir, *The Handbook of Privacy Studies: An Interdisciplinary Introduction*, Amsterdam University Press, 2018, p.24.
[9] KEULEN et KROEZE. « Privacy from a Historical Perspective », *supra* note 8, pp.24-25.
[10] *Ibid.*, pp.25-26.
[11] *Ibid.*, p.26.
[12] *Ibid.*, pp.25-26.
[13] *Ibid.*, pp.27 et 31-32.
[14] LUKÁCS, A. « What is privacy? The history and definition of privacy », 2016, p.257, en ligne : https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf ; LEPORE, J. « The Prism: Privacy in an Age of

La montée du libéralisme suivant la Première Guerre mondiale confirmera de nouveau toute l'importance de la vie privée pour les individus, en l'opposant à l'État cette fois. Ce dernier se modernise et offre davantage de soutien et de services à ses citoyens (dont un filet de sécurité sociale), mais impose en échange surveillance et divulgation de renseignements personnels[15].

Enfin, le développement du réseau Internet et du World Wide Web dans les années 1980 et 1990 et les plus récentes innovations technologiques qui en découlent changent une nouvelle fois l'environnement et le quotidien des individus et influencent leur perception de la vie privée et des menaces potentielles auxquelles elle est soumise.

> Changes in modern communication techniques, from the printing press and telephone to the computer and Internet, have had a great impact on the way privacy was understood as well. All these changes have made privacy a slippery concept that is difficult to grasp in general terms[16].

1.2 Comment définir la vie privée ?

Il n'existe aucune définition universelle de la vie privée[17]. Sans être exhaustive, la présente section vise à présenter les perspectives d'une sélection d'auteurs sur le sujet. Nous y aborderons également les approches adoptées par les systèmes de justice européen, américain et canadien en ce qui concerne la notion de vie privée.

1.2.1 De nombreuses définitions proposées au fil du temps

Il existe deux grandes conceptions de la vie privée dans la littérature. L'une se rattache davantage à la notion d'isolement de l'espace public et l'autre à la notion de contrôle. À partir de celles-ci, la vie privée peut prendre diverses formes plus spécifiques selon les auteurs qui se prêtent à ce difficile exercice de définition du concept.

1.2.1.1 Une question d'isolement de l'espace public

Warren et Brandeis ont fourni en 1890 la définition la plus connue de la vie privée ; leur article paru dans le *Harvard Law Review* est considéré comme l'un des articles de droit les plus influents de tous les temps[18].

Publicity », The New Yorker, 24 juin 2013, en ligne : https://www.newyorker.com/magazine/2013/06/24/the-prism

[15] KEULEN et KROEZE. « Privacy from a Historical Perspective », *supra* note 8, p.34.

[16] *Ibid.,* p.40.

[17] LUKÁCS, A. « What is privacy? », *supra* note 14, pp.256-258.

[18] *Ibid.,* pp.257-258 ; BRATMAN, B. E. « Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy », Tennessee Law Review vol. 69, 2002, p.624 ; HOLVAST, J. « History of Privacy » dans MATYÁŠ, V. *et al.*, dir, The Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology,

Selon ces deux avocats américains, la vie privée se définirait comme le droit d'être laissé à soi-même (« the right to be left alone »)[19]. L'individu doit pouvoir disposer d'un espace privé pour y développer ses croyances et opinions, sans craindre le jugement des autres et les pressions de sa communauté[20].

Les auteurs se montrent particulièrement critiques des journalistes et des photographies instantanées qui accompagnent régulièrement les articles dans les tabloïds de l'époque[21]. C'est à eux qu'ils attribuent l'exposition non souhaitable des individus à l'attention de la masse qui nuit ultimement à leur capacité à se développer et qui serait responsable de la dégradation de la moralité en société[22].

Depuis la parution de l'article de Warren et Brandeis, nombre d'auteurs s'en sont inspirés pour proposer une définition revisitée de la vie privée centrée autour de l'accès limité des autres à soi[23].

Gavison affirme par exemple ceci :

> I suggest that an individual enjoys perfect privacy when he is completely inaccessible to others. This may be broken into three independent components: in perfect privacy no one has any information about X, no one pays any attention to X, and no one has physical access to X. Perfect privacy is, of course, impossible in any society. The possession or enjoyment of privacy is not an all or nothing concept, however, and the total loss of privacy is as impossible as perfect privacy[24].

L'auteure identifie donc trois éléments connexes à l'accès limité des autres à soi : la solitude, l'anonymat et le secret[25]. Ce dernier élément a d'ailleurs été spécifiquement retenu par certains, comme le juge Posner et l'auteur Parent, qui conçoivent la vie privée comme le fait de garder secrets les renseignements personnels d'un individu[26]. Pour ces derniers, l'accès physique aux individus devient secondaire puisque le désir de paix et de tranquillité de Warren et Brandeis serait dorénavant comblé par le mode de vie occidental contemporain[27]. Et Posner réfère à son tour à une autre notion pertinente à sa définition de la vie privée : la protection de la réputation des individus. Si les renseignements

---

vol. 298, 2009, p.18 ; WALDMAN, A. Privacy as Trust: Information Privacy for an Information Age, Cambridge University Press, 2018, p.11.

[19] WARREN, S. D. et BRANDEIS, L. D. « The Right to Privacy », Harvard Law Review, vol. 4, no. 5, 15 décembre 1890, p.195. À noter que cette expression a d'abord été utilisée par le juge Thomas Cooley dans le cadre d'un ouvrage sur les *torts* de common law dix ans avant l'article de Brandeis et Warren : SOLOVE, D. J. « Conceptualizing privacy », California Law Review vol. 90, no. 4, 2002, p.1100.

[20] BEZANSON, R. P. « The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990 », California Law Review, vol. 80, no. 5, octobre 1992, p.1134.

[21] WARREN et BRANDEIS. « The Right to Privacy », *supra* note 19, p.213 ; BRATMAN. « Brandeis and Warren's The Right To Privacy », *supra* note 18, pp.624 et 630 ; LUKÁCS. « What is privacy? », *supra* note 14, pp.257-258.

[22] BEZANSON. « The Right to Privacy Revisited », *supra* note 20, pp.1138-1139.

[23] SOLOVE. « Conceptualizing privacy », *supra* note 19, p.1102.

[24] GAVISON, R. « Privacy and the Limits of Law », The Yale Law Journal, vol. 89, no. 3, 1980, p.428.

[25] *Ibid.*

[26] Selon Posner, la vie privée serait le droit pour un individu de garder secrets des renseignements déshonorants à son sujet : POSNER, R. A., The Economics of Justice, Harvard University Press, 1983.
Selon Parent, la vie privée est « the condition of not having undocumented personal information about oneself known by others » : PARENT, W. A. « A New Definition of Privacy for the Law », Law and Philosophy, vol. 2, no. 3, 1983, p.306.

[27] POSNER, R. A. « Privacy, Secrecy, and Reputation », Buffalo Law Review, vol. 28, 1979, pp.4-5

personnels doivent être gardés secrets, c'est pour assurer la réputation de tous et chacun[28].

Il est à noter que les conceptions de la vie privée qui s'appuient sur le secret ont été critiquées par plusieurs pour leur distinction simpliste entre les renseignements privés et publics[29]. Un renseignement personnel perd-il son caractère privé dès qu'il est divulgué directement ou indirectement à quelqu'un ? Les caractéristiques et les capacités physiques générales d'un individu qui se trouve dans l'espace public sont divulguées au public. Et un individu laisse vraisemblablement des traces biologiques sur son passage (ADN, cheveux, etc.). Ces renseignements deviendraient-ils publics pour autant ? Cette conclusion est certainement difficile à soutenir et parait assez peu adaptée à l'époque actuelle.

> When understood as a right to separate and exclude, privacy vanishes the moment we let others in. That erases privacy in today's technology-driven world, where some amount of disclosure of data is inevitable and often mandatory[30]

1.2.1.2 Une question de contrôle

Il existe un second courant de pensée davantage centré sur la notion de contrôle. La vie privée ne serait pas liée à la capacité de chacun de s'isoler du reste de la société, mais bien à sa capacité à déterminer à qui et quoi il donne accès[31]. Gerety parle par exemple de l'autonomie exercée par chacun sur l'intimité de son identité personnelle[32].

Moore, pour sa part, restreint sa définition de la vie privée au contrôle exercé par chacun sur l'accès qu'ont les autres à soi et à ses renseignements à caractère personnel[33]. Si cette définition peut sembler similaire à celle de Gavison sur l'accès limité des autres à soi, elle diffère en ce que l'accent est mis sur le contrôle qui est exercé et non sur le résultat obtenu. Ainsi, un individu qui permettrait un large accès du public à différentes facettes de sa personne maintiendrait théoriquement sa vie privée, selon Moore, pour autant que la portée de cet accès résulte de ses propres choix[34].

Plus restrictives, les définitions de Westin et Fried se limitent au contrôle sur les renseignements personnels communiqués aux autres[35].

---

[28] *Ibid.*, pp.5-6.
[29] MOORE, A. D. « Privacy: Its Meaning and Value », American Philosophical Quarterly, vol. 40, juillet 2003, p.218 ; SOLOVE. « Conceptualizing privacy », *supra* note 19, p.1107.
[30] WALDMAN. Privacy as Trust, *supra* note 18, p.26.
[31] FRIED, C. « Privacy », The Yale Law Journal, vol. 77, 1968, p.482.
[32] GERETY, T. « Redefining Privacy », Harvard Civil Rights-Civil Liberties Law Review, vol. 12, no. 2, 1977, p.236.
[33] MOORE. « Privacy », *supra* note 29, p.218 ; MOORE, A. « Defining Privacy », Journal of Social Philosophy, vol. 39, no 3, 2008, pp.420
[34] AUSTIN, L. M. « Rereading Westin », Theoretical Inquiries in Law, vol. 20, no. 1, 2019.
[35] *Ibid.* et SOFFER, T. et COHEN, A. « Privacy Perception of Adolescents in a Digital World », Bulletin of Science, Technology & Society, vol. 34, no. 56, 1er octobre 2014, p.147 ; FRIED, C. « Privacy », *supra* note 31 p.483.

> Privacy, thus, is control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well.[36]

En plus du contrôle sur l'accès à la personne physique et à ses renseignements personnels, certains auteurs ont ajouté un troisième volet à la définition de la vie privée : la capacité à prendre des décisions importantes sur son mode de vie et sa famille[37]. Mentionnons à cet égard que le droit à l'avortement a historiquement été associé au droit à la vie privée chez nos voisins du sud[38].

Tout comme la définition relative à l'accès, la définition de la vie privée qui s'attarde au contrôle a fait l'objet de certaines critiques du fait de son caractère circulaire :

> Gavison and other critics of the assumption that privacy functions through control contend that this assumption makes it impossible to escape from within privacy because every choice is an exercise of control[39]

1.2.1.3 Des perspectives qui ont beaucoup en commun

Il ressort de ce survol des grandes définitions de la vie privée qu'elles présentent certaines similarités claires, notamment en ce qui concerne leur lien étroit avec la notion de liberté.

Ainsi, les définitions de la vie privée découlent généralement d'une reconnaissance de la liberté de chaque individu, une liberté qui est abordée de différentes manières :

> Today, the function of privacy relating to freedom of the individual as an individual is the dominant one; the function of privacy relating to social control is greatly diminished. The freedoms protected by today's more individualistic idea of privacy are of two sorts: freedom from intrusiveness and freedom to achieve identity[40].

Les définitions de la vie privée ont également en commun leur approche basée sur la reconnaissance d'un droit fondamental aux individus[41]. Il existe néanmoins quelques auteurs, comme Lessig par exemple, qui désapprouvent cette analyse et qui sont d'avis que la vie privée relève plutôt de la notion de propriété[42]. D'autres, comme Jarvis Thomson, ne conçoivent pas la vie privée comme un droit en soi, mais bien comme le produit ou l'amalgame d'une multitude de droits.

> For if I am right, the right to privacy is "derivative" in this sense: it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning the right to

---

[36] FRIED. « Privacy », *supra* note 35, p.483.
[37] STANFORD ENCYCLOPEDIA OF PHILOSOPHY. « Privacy », en ligne : https://plato.stanford.edu/entries/privacy/#VieMeaValPri
[38] *Roe* v *Wade*, 410 U.S. 113.
[39] INNESS, J. C. Privacy, Intimacy, and Isolation, Oxford University Press, 1996, p.52.
[40] BEZANSON. « The Right to Privacy Revisited », *supra* note 20, p.1144.
[41] WALDMAN. Privacy as Trust, *supra* note 18, p.11.
[42] Voir par exemple : LESSIG, L. « Privacy as Property », Social Research, vol. 69, no. 1, printemps 2002, pp.257-262.

privacy. Indeed, the wrongness of every violation of the right to privacy can be explained without ever once mentioning it[43].

1.2.1.4 Les différentes dimensions de la vie privée

Face à la complexité qui interfère avec toute tentative de définir la vie privée en une seule base conceptuelle, certains auteurs ont plutôt tenté de la définir en identifiant ses différentes dimensions ou les éléments qui la composent[44].

En pratique, on remarquera que les auteurs qui ont fait cet exercice reprennent sensiblement les perspectives des auteurs mentionnés précédemment, mais sous des classifications différentes, ce qui appuie la thèse d'une complémentarité des définitions possibles de la vie privée.

Voici quelques exemples des dimensions identifiées :

Tableau 1
Les dimensions de la vie privée selon une sélection d'auteurs

<table>
<tr><th>J. K. Burgoon (1982)[45]</th><th>R. Clarke (1992, 2013)[46]</th><th>S. Gutwirth et al. (2011)[47],</th></tr>
<tr><td>La vie privée sociale (relative aux relations interpersonnelles)</td><td rowspan="2">La vie privée communicationnelle (relative aux échanges entre personnes)</td><td>La vie privée communicationnelle</td></tr>
<tr><td>La vie privée psychologique (relative aux échanges intimes entre personnes)</td><td>La vie privée associative (relative aux associations entre personnes)</td></tr>
</table>

[43] JARVIS THOMSON, J. « The Right to Privacy », Philosophy & Public Affairs, vol. 4, no. 4, 1975, p.313.
[44] KOOPS, B-J. *et al*. A « Typology of Privacy », University of Pennsylvania Journal of International Law, vol. 38, no. 2, 2017, pp.483, en ligne : https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1938&context=jil
[45] « *Social privacy,* », « *physical privacy* » et « *psychological privacy* » : BURGOON, J. K. « Privacy and communication » dans BURGOON, M., dir, Communication Yearbook 6, SAGE, 1982, pp. 206–249 ; VON PAPE, T., TREPTE, S. et MOTHES, C. « Privacy by Disaster? Press Coverage of Privacy and Digital Technology », European Journal of Communication, vol. 32, no. 3, juin 2017, p.191.
[46] « Privacy of the physical person », « privacy of personal communications », « privacy of personal data », « privacy of personal behaviour » et « privacy of personal experience » : CLARKE, R. A Framework for Analysing Technology's Negative and Positive Impacts on Freedom and Privacy, 16 aout 2015, en ligne : http://www.rogerclarke.com/DV/Biel15-DuDA.html#App3 (consulté le 2décembre 2019) ; KOOPS. « A Typology of Privacy », *supra* note 44, pp.497-500.
[47] « Privacy of communication », « privacy of the person », « privacy of location and space », « privacy of association », « privacy of behaviour and action », « privacy of thoughts and feelings » et « privacy of data and image » : GUTWIRTH, S. *et al.* « Legal, social, economic and ethical conceptualisations of privacy and data protection », Prescient project, 23 mars 2011, pp.63 et ss, en ligne : http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

<table>
<tr><td rowspan="2">La vie privée physique
(relative au domicile, au corps, etc.)</td><td rowspan="2">La vie privée physique</td><td>La vie privée personnelle
(relative au corps)</td></tr>
<tr><td rowspan="2">La vie privée spatiale
(relative aux déplacements dans l'espace public, semi-public et privé)</td></tr>
<tr><td rowspan="3"></td><td rowspan="2">La vie privée comportementale
(relative aux actions)</td></tr>
<tr><td>La vie privée comportementale</td></tr>
<tr><td>La vie privée informationnelle
(relative aux renseignements à caractère personnel)</td><td>La vie privée informationnelle et visuelle</td></tr>
<tr><td>La vie privée expérientielle
(relative aux idées, concepts et contenus expérimentés et consultés)</td><td>La vie privée émotionnelle et idéationnelle
(relative aux pensées et sentiments)</td></tr>
</table>

1.2.2 Différentes perspectives juridiques sur le sujet

Parallèlement au développement de la littérature en matière de vie privée, certains acteurs étatiques ont dû eux aussi prendre parti dans les débats entourant la définition de la vie privée. C'est le cas entre autres des législateurs et des juges. À l'image de la littérature, les différents systèmes juridiques présentent des conceptions variées de la vie privée, qui rejoignent bien entendu certains éléments des théories issues des sciences humaines sur le sujet, mais qui méritent d'être analysées distinctement, puisque certains fondements sous-jacents s'articulent différemment.

Nous traiterons donc brièvement des perspectives juridiques européenne, américaine et canadienne sur le sujet dans la présente section. Si notre voisin du Sud influence couramment l'état du droit au Canada[48], le vieux continent mérite aussi notre attention vu son statut de précurseur en matière de protection de la vie privée des consommateurs ; le Wall Street Journal l'ayant déjà qualifié de « privacy Cop to the World »[49].

[48] Voir par exemple : MANFREDI, C. « The Use of United States Decisions by the Supreme Court of Canada Under the Charter of Rights and Freedoms », Canadian Journal of Political Science, vol. 23, no. 3, 1990.
[49] SCHEER, D. « Europe's New High-Tech Role: Playing Privacy Cop to World « , Wall Street Journal, 10 octobre 2003, en ligne : https://www.wsj.com/articles/SB106574949477122300

Notons d'entrée de jeu que, malgré d'importantes nuances, les législations canadienne, américaine et européenne ont toutes les trois deux fondements communs :

1. Elles centrent leur intervention autour de la vie privée informationnelle, en ce que les encadrements en vigueur se concentrent surtout sur la collecte, le traitement et la gestion des renseignements personnels des individus ;

2. Elles accordent une place fondamentale aux notions de choix et de consentement des individus, rejoignant ainsi davantage la notion de contrôle mise de l'avant par des auteurs comme Moore, Westin ou Fried[50]. Précisons à ce sujet que, de manière générale, les modalités et la capacité réelle des individus à exercer ce contrôle sont bien supérieures en Europe qu'au Canada et aux États-Unis.

1.2.2.1 La vie privée des consommateurs en droit européen : une question de dignité humaine

Au sein de l'Union européenne, la protection de la vie privée des individus est d'abord abordée dans des instruments juridiques de reconnaissance des droits humains. « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. » : voilà ce que prévoient la Convention européenne des droits de l'homme[51] et la Charte européenne des droits fondamentaux[52].

Le régime européen distingue par ailleurs le droit à la vie privée du droit à la protection des renseignements personnels, contrairement aux auteurs mentionnés précédemment, pour qui les renseignements personnels ou l'information relative aux individus sont généralement perçus comme une composante de la vie privée. Ces deux droits sont explicitement liés dans les instruments européens, mais sont traités par des articles distincts[53], puisque le droit à la protection des renseignements personnels ne découlerait que partiellement du droit à la vie privée[54]. La protection des renseignements personnels fait d'ailleurs l'objet d'un large encadrement qui lui est spécifique, soit le *Règlement général sur la protection des données* (*RGPD*, mieux connu sous son acronyme anglophone *GDPR*) adopté en avril 2016 puis mis en œuvre en mai 2018.

---

[50] WALDMAN. Privacy as Trust, *supra* note 18, p.30.
[51] CONSEIL DE L'EUROPE. Convention européenne des droits de l'homme, STCE no : 005, art 8.
[52] UNION EUROPÉENNE. Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, art II-7 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».
[53] *Ibid.,* arts II-7 et II-8.
[54] UNION EUROPÉENNE. « Explications relatives à la Charte des droits fondamentaux », Journal officiel de l'Union européenne, C 303, 14.12.2007, p. 17–35, en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32007X1214(01)&from=EN ; MOSTERT, M. *et al*. « From Privacy to Data Protection in the EU: Implications for Big Data Health Research », European Journal of Health Law, vol. 25, no. 1, décembre 2017, p.5, en ligne : https://bartvandersloot.com/onewebmedia/From%20privacy%20to%20Data%20Protection.pdf

En plus d'une mention spécifique au préambule du *RGPD*[55], le type d'encadrement retenu par le Parlement européen est particulièrement indicateur du statut (légal et philosophique) de la protection des renseignements personnels à titre de droit fondamental. Il s'agit d'une réglementation de type omnibus qui concerne autant les acteurs privés que publics[56] et qui s'applique à tous renseignements d'une personne identifiée ou identifiable[57], couvrant ainsi un très large éventail de situations. Et on y prévoit une série de protections minimales applicables automatiquement et auxquelles un consommateur ne peut renoncer dans le cadre d'une entente privée[58].

La vision européenne de la vie privée et de la protection des renseignements personnels est intimement liée à la sauvegarde de la dignité humaine, de l'honneur et de la réputation des individus.

> Despite its almost invisible presence in the GDPR, human dignity is the fundamental concept that provides the framework within which one needs to interpret what the GDPR—and more generally European culture and jurisdiction — understand by informational privacy (henceforth only privacy) [59]. [citations omises]

De manière générale, la réglementation en place au sein de l'Union européenne vise ainsi à octroyer aux individus le contrôle sur la divulgation de leurs renseignements personnels dans le but ultime d'éviter une exposition publique non désirée et l'embarras ou l'humiliation qui pourrait l'accompagner[60]. Cette perspective européenne de la vie privée n'est pas sans rappeler les préoccupations de Warren et Brandeis sur le sujet.

Le « droit à l'oubli » conçu et implanté d'abord en droit européen est un exemple clair de l'importance accordée à la protection de la réputation dans l'exercice du droit à la vie privée. Ce droit, parfois qualifié de « rédemption numérique » (« digital redemption »)[61], permet aux Européens, dans certaines circonstances, de demander aux moteurs de recherche de déréférencer des hyperliens les concernant[62]. Parmi les exemples fournis par Google, notons le déréférencement d'hyperliens d'articles de presse relatifs à des condamnations datant de plusieurs années et pour lesquelles les peines ont été purgées, des accusations n'ayant pas mené à des déclarations de culpabilité, des faillites

---

[55] « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental » : UNION EUROPÉENNE. Règlement général sur la protection des données, 2016/679, préambule, para (1) [RGPD].
[56] SCHWARTZ, P. M. et SOLOVE, D. J. « Reconciling Personal Information in the United States and European Union », California Law Review, vol. 102, no. 4, 2013, pp.880-881.
[57] RGPD, *supra* note 55, art 4(1). Pour des explications sur le caractère identifiable d'un renseignement, voir le préambule, para (26).
[58] LYNSKEY, O. The foundations of EU data protection law, Oxford University Press, 2015, p.40.
[59] FLORIDI, L. « On Human Dignity as a Foundation for the Right to Privacy », Philosophy & Technology, vol. 29, no. 4, décembre 2016, p.307.
[60] WHITMANT, J. Q. « The Two Western Cultures of Privacy: Dignity versus Liberty », The Yale Law Journal, vol. 113, no. 6, janvier 2004, p.1161.
[61] JONES, M. Ctrl + Z : The Right to Be Forgotten. New York University Press, 2016, p.81.
[62] COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS. « Droit au Déréférencement. Les critères communs utilisés pour l'examen des plaintes », en ligne : https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf (consulté le 6 août 2021).

personnelles ou encore les propos tenus par des personnes qui étaient mineures à l'époque[63].

Dans cette perspective européenne de la vie privée, qui se distingue considérablement de celle des Américains, les craintes d'intrusion sont plus grandes lorsque ces intrusions sont le fait d'acteurs privés que d'acteurs publics, puisqu'elles sont plus susceptibles de nuire à la réputation publique des individus.

> Dignity is protected first and foremost in society, so one's dignity does not necessarily suffer from government actions as much as it potentially suffers from the thoughts and perceptions of other members of society. If the goal of privacy protection is ultimately the protection of dignity, then it is clear that privacy must be protected first and foremost in society, and that government intrusions are less worrisome. [64]

1.2.2.2 La vie privée des consommateurs en droit américain : le libre marché avant tout

Alors que le cadre européen reconnait explicitement un droit général à la protection de la vie privée, ce droit, lorsqu'il vise le secteur privé, est moins explicite en sol américain. Une allusion indirecte à la vie privée se trouve au quatrième amendement de la Constitution américaine, qui interdit les perquisitions et les saisies déraisonnables par l'État[65]. Au fil du temps, l'interprétation de ce droit a été élargie afin de couvrir une protection plus large contre les intrusions de l'État dans la vie des Américains et particulièrement dans les décisions personnelles qu'ils prennent (propriété, santé, etc.)[66].

Et contrairement à la conception européenne de la vie privée, qui a pour pilier la dignité humaine, la conception américaine se concentre davantage autour du droit à la liberté ; une liberté qui s'exerce avant tout face à l'État.

> America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home. The prime danger, from the American point of view, is that "the sanctity of [our] home[s]," in the words of a leading nineteenth-century Supreme Court opinion on privacy, will be breached by government actors[67].

Qu'en est-il du secteur privé ? Lorsqu'il est question de la protection de la vie privée des consommateurs, non pas par rapport à l'État, mais plutôt par rapport aux commerçants et aux tiers, la perspective américaine se fonde avant tout sur le bon fonctionnement du libre

---

[63] GOOGLE. « Demandes de suppression de contenu dans le cadre de la législation européenne sur le respect de la vie privée », en ligne : https://transparencyreport.google.com/eu-privacy/overview (consulté le 5 avril 2021).
[64] LEVIN, A. et NICHOLSON, M. J. « Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground », University of Ottawa Law & Technology Journal, vol. 2, no. 2, 2005, p.388-389.
[65] ÉTATS-UNIS. Constitution, amendement IV.
[66] WHITMANT, J. Q. « The Two Western Cultures of Privacy », *supra* note 60, pp.1212 et 1214
[67] *Ibid.,* pp.1161-1162.

marché[68]. L'État fédéral américain limite ses interventions à la protection des renseignements les plus sensibles, tels que les renseignements relatifs à la santé[69] ou aux mineurs[70], pour lesquels les marchés n'offriraient pas de protections adéquates. Ce faisant, le régime américain actuel est une courtepointe de règlements sectoriels et d'autoréglementation de l'industrie[71]. Il revient à la Federal Trade Commission (FTC) de veiller à la protection des renseignements personnels des consommateurs dans le cadre de son pouvoir d'exercice en matière de pratiques commerciales déloyales et/ou trompeuses[72].

Et puisqu'on n'accorde pas autant d'importance à la protection de la vie privée des consommateurs au sein du régime américain qu'au sein du régime européen, elle l'emporte rarement lorsqu'elle est confrontée à d'autres droits, tels que la liberté de commerce et la liberté d'expression[73].

Soulignons tout de même que quelques États - la Californie, le Colorado et la Virginie - ont mis en place un régime plus complet de protection des renseignements personnels des consommateurs[74]. Plusieurs autres États étudient également cette possibilité face à l'échec des tentatives en ce sens sur la scène fédérale[75].

1.2.2.3 La vie privée des consommateurs en droit canadien : à mi-chemin entre l'Europe et les États-Unis

La conception juridique canadienne en matière de vie privée des individus se situe à mi-chemin entre celles de l'Europe et des États-Unis. Elle intègre des notions de protection

---

[68] ASHWORTH, L., et FREE, C. « Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns », Journal of Business Ethics, vol. 67, no. 2, 2006, p.109 ; LEVIN. « Privacy Law in the United States », *supra* note 64, p.362.
[69] ÉTATS-UNIS. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 201.
[70] ÉTATS-UNIS. Children's Online Privacy Protection Act, 15 U.S.C. 91.
[71] GADY, F-S. « EU/U.S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis », Georgetown Journal of International Affairs, 2014, p.15 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Consentement et protection de la vie privée - Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques », mai 2016, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/consent_201605/
[72] FEDERAL TRADE COMMISSION. « What We Do », en ligne : https://www.ftc.gov/about-ftc/what-we-do
EIJK, N. V., HOOFNAGLE, C. J. et KANNEKENS, E. « Unfair Commercial Practices: A Complementary Approach to Privacy Protection », European Data Protection Law Review, vol. 3, 2017, p. 325 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. Consentement et protection de la vie privée », *supra* note 71.
[73] HOOFNAGLE, C. J., VAN DER SLOOT, B et ZUIDERVEEN BORGESIUS, F. « The European Union general data protection regulation: what it is and what it means », Information & Communications Technology Law, vol. 28, no. 1, 2019, p.75 ; SCHWARTZ. « Reconciling Personal Information », *supra* note 56, pp.880-881.
[74] ÉTAT DE LA CALIFORNIE. California Consumer Privacy Act of 2018 et ÉTAT DE LA CALIFORNIE. California Privacy Rights Act of 2020 ; ÉTAT DU COLORADO. Colorado Privacy Act ; ÉTAT DE LA VIRGINIE. Consumer Data Protection Act.
[75] IAPP. « US State Privacy Legislation Tracker », en ligne: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (consulté le 10 juin 2021).

des droits humains (et ainsi, de dignité humaine), mais son encadrement vise avant tout la réglementation des marchés. En ce sens, la réflexion canadienne en matière de protection de la vie privée des consommateurs peut paraitre quelque peu inachevée, comme si elle ne savait trop sur quel pied danser…

Le droit à la protection de la vie privée est reconnu (indirectement) dans la *Charte canadienne des droits et libertés,* sous les droits *à la liberté et à la protection contre les fouilles, perquisitions ou saisies abusives*[76]. Cette protection vise uniquement les intrusions de l'État. Lorsqu'il est plutôt question des intrusions potentielles par le secteur privé, la loi fédérale pertinente est la *Loi sur la protection des renseignements personnels et les documents électroniques*[77] (*LPRPDE,* souvent identifiée par son acronyme anglais *PIPEDA*). Trois provinces ont adopté des lois réputées « essentiellement similaires » qui s'appliquent en lieu de la *LPRPDE*[78]. Le fonctionnement spécifique de ces lois et les règles qu'elles y prévoient seront étudiés au chapitre 5.

Notons par ailleurs que la province de Québec reconnait formellement dans sa *Charte des droits et libertés de la personne*, le droit à la protection de la vie privée, tant par rapport à l'État qu'au secteur privé[79]. Ultimement, les différentes lois applicables au Canada étant toutes « essentiellement similaires », cette particularité québécoise affecte peu notre analyse de la conception de la vie privée par le système juridique canadien.

Comme l'encadrement réglementaire européen et américain, l'encadrement canadien ne concerne que la protection des renseignements personnels. Puisqu'aucune règle ne distingue au pays le droit à la vie privée du droit à la protection des renseignements personnels, nous sommes portés à croire que le premier serait davantage perçu comme une composante du second que comme un élément réellement distinct.

Sans dire officiellement qu'on vise à y assurer la protection de la vie privée, la *LPRPDE* mentionne tout de même qu'elle fixe des règles relatives à la collecte, l'utilisation et la communication de renseignements personnels « d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent[80] ». Aussi, à l'instar de *RGPD*, elle adopte une définition large et inclusive de ce qu'est un renseignement personnel[81] et ne limite pas son application à certains renseignements personnels sensibles. De même, la *LPRPDE* et les lois provinciales équivalentes couvrent l'ensemble du secteur privé à quelques exceptions près[82]. Nous

---

[76] CANADA. Loi constitutionnelle de 1982, Annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11, arts 7 et 8.
[77] CANADA. Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c 5 [LPRPDE].
[78] QUÉBEC. Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1 [LPRPSP], ALBERTA. Personal Information Protection Act, statutes of Alberta, 2003, c P-6.5 [APIPA], COLOMBIE-BRITANNIQUE. Personal Information Protection Act, SBC 2003, c 63 [BCPIPA]. À noter qu'il existe aussi des lois provinciales qui visent uniquement les renseignements personnels sur la santé (Nouveau-Brunswick, Nouvelle-Écosse, Ontario, Terre-Neuve-et-Labrador).
[79] QUÉBEC. Charte des droits et libertés de la personne, RLRQ c C-12, art 5.
[80] LPRPDE, *supra* note 77, art 3.
[81] « Tout renseignement concernant un individu identifiable » : *Ibid.*, art 2.
[82] *Ibid.*, art 4 ; LPRPSP, *supra* note 78, art 3 *a contrario* ; APIPA, *supra* note 78, art 4 ; BCPIPA, *supra* note 78, art 3.

sommes donc bien loin des faibles protections américaines offertes uniquement aux renseignements relatifs à la santé ou à ceux qui concernent des personnes mineures.

Mais si la *LPRPDE* présente ainsi des signes d'une perspective canadienne de la vie privée centrée sur la reconnaissance et la protection d'un droit fondamental, les origines du document en sont bien loin !

Le législateur canadien avait deux objectifs avec l'adoption de la loi, tous deux centrés principalement sur le développement de l'économie numérique qui, en 2000, en était encore à ses débuts. D'abord, on souhaitait favoriser la confiance du public dans le commerce électronique et ainsi « mo[ve] Canada to the forefront of the global digital economy », comme le présentait le ministre de l'Industrie de l'époque[83]. Cet objectif se reflète très clairement dans le titre complet de la loi, dans lequel la protection des renseignements personnels est réduite à une manière de faciliter le commerce :

> Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions et en modifiant la Loi sur la preuve au Canada, la Loi sur les textes réglementaires et la Loi sur la révision des lois[84]

Le second objectif de l'adoption de la *LPRPDE* était d'assurer le maintien des échanges commerciaux avec l'Union européenne, considérant l'élaboration quelques années auparavant de la Directive 95/46/EC par le Parlement européen[85]. L'article 25 de cette directive interdisait le transfert de données à caractère personnel de résidents des États membres de l'Union européenne vers des États tiers à moins que ces derniers assurent eux aussi un niveau de protection adéquat des données en question[86]. Le Canada a obtenu cette « certification » grâce à la *LPRPDE* en 2002[87].

Le résumé qu'offre la professeure et spécialiste en droit de la vie privée au Canada, Teresa Scalla, illustre bien l'absence étonnante de considérations pour la protection d'un droit aussi fondamental dans la mise en place de la loi qui le concerne :

> To understand why PIPEDA is such a mess requires some history. PIPEDA was passed by Parliament in 2000. Its enactment followed closely on the heels of the EU's Data Protection Directive, which, like the GDPR, threatened to disrupt data flows to countries that did not meet minimum standards of private sector data protection. Canada needed private sector data protection legislation and it needed it fast. […] The private sector did not want such legislation. As a compromise, the government decided to use the CSA Model Code – a voluntary privacy code developed with multi-stakeholder input – as the normative heart of the statute. There had been enough buy-in with the Model Code that the government felt that it avoid excessive pushback from the private sector. The Code, therefore, originally drafted to provide voluntary

---

[83] LEVIN. « Privacy Law in the United States », *supra* note 64, p.379.
[84] LPRPDE, *supra* note 77.
[85] UNION EUROPÉENNE. Directive 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, 95/46/CE.
[86] Le critère d'adéquation de la législation du pays tiers est aujourd'hui prévu à RGPD, *supra* note 55, art 45.
[87] COMMISSION DES COMMUNAUTÉS EUROPÉENNES. Décision 2002/2/CE, Journal officiel n° L 002 du 04/01/2002, p. 13–16, en ligne : https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002

> guidance, was turned into law. The prime minister at the time, the Hon. Jean Chretien, did not want Parliament's agenda overburdened with new bills, so the data protection bill was grafted onto another bill addressing the completely different issue of electronic documents[88].

La faiblesse des pouvoirs d'intervention conférés au Commissariat à la protection de la vie privée du Canada chargé de veiller au respect de la *LPRPDE* laisse aussi croire que la vie privée des consommateurs n'est pas perçue (du moins pleinement) comme une question de droits humains.

La conception canadienne de la vie privée parait donc plus difficile à cerner que celle de ses pendants européen et américain. Désireuse de présenter et d'encadrer la protection des renseignements personnels dans une perspective de droit fondamental, elle adopte tout de même rapidement la voie d'un encadrement axé sur les pratiques commerciales répréhensibles relatives aux renseignements personnels.

Des réformes canadiennes qui pourraient éventuellement changer la donne

Notons que nous assistons à une tendance vers l'uniformisation des lois en matière de vie privée dans le monde, basée sur l'encadrement européen[89]. Le Canada ne fait pas exception à cette tendance : l'année 2020 a vu le dépôt de deux projets de loi inspirés du *RGPD*, l'un au Parlement fédéral et l'autre à l'Assemblée nationale du Québec. Le projet québécois a depuis été adopté et est devenu la Loi 25 dont l'entrée en vigueur est prévue pour septembre 2023 (à l'exception de quelques dispositions). Le projet fédéral, lui, est mort au feuilleton à l'été 2021. La conception juridique canadienne en matière de vie privée est-elle en train de changer ?

Pas forcément. Les deux projets de loi proposaient l'ajout de nouveaux droits reconnus aux consommateurs dans le cadre de l'utilisation de leurs renseignements personnels (le droit à la mobilité des renseignements par exemple), mais ne remettaient pas réellement en question l'équilibre en place entre les besoins des consommateurs et les besoins et désirs des entreprises. Le titre du projet de loi fédéral était modifié pour refléter certains changements, mais les objectifs explicites de facilitation et promotion du commerce électronique y demeuraient centraux et la protection des renseignements personnels demeurait un moyen d'arriver à ces fins.

---

[88] SCASSA, T. « PIPEDA reform should include a comprehensive rewrite », 9 juillet 2018, en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=279:pipeda-reform-should-include-a-comprehensive-rewrite&Itemid=80&tmpl=component&print=1

[89] BERNIER, C. « L'évolution des distinctions entre le droit à la vie privée canadien et étranger », Association du Barreau canadien, 19 novembre 2020, en ligne : https://www.cba.org/Sections/Privacy-and-Access/Articles/2020/The-evolving-distinctions-between-Canadian-and-for

LPRPDE	Projet de loi C-11
Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions et en modifiant la Loi sur la preuve au Canada, la Loi sur les textes réglementaires et la Loi sur la révision des lois	Loi visant à faciliter et à promouvoir le commerce électronique au moyen de la protection des renseignements personnels recueillis, utilisés ou communiqués dans le cadre d'activités commerciales

Ironiquement, le titre abrégé de la nouvelle loi fédérale prévue au projet de loi C-11 aurait été la « Loi sur la protection de la vie privée des consommateurs ». Peut-être s'agit-il d'un indice additionnel de l'ambivalence canadienne en matière de protection de la vie privée ou tout simplement d'un exercice de marketing par le gouvernement fédéral…

1.3 Et la vie privée en ligne ?

Le présent rapport se concentrera spécifiquement dans les chapitres qui suivent sur la protection de la vie privée en ligne. Internet change-t-il la donne en matière de vie privée des consommateurs ?

Internet présente certaines caractéristiques techniques qui simplifient le partage de renseignements à caractère personnel et l'accès à l'information par tous, et ce, gratuitement ou à très faible coût. Les instruments de connexion, tels que les ordinateurs ou les objets connectés, permettent la collecte et le traitement de ces renseignements partagés et même de renseignements sur l'utilisation même du réseau par les individus sans que ces derniers n'en soient nécessairement conscients[90]. Certains affirment que le réseau n'oublie jamais. Si cette expression n'est pas tout à fait exacte[91], il demeure qu'Internet permet et facilite une plus grande préservation de l'information. Le réseau est plus largement à l'origine d'importants changements au sein de la société.

> Together these technological advancements have contributed to incredible social shifts in the way information is created, shared, and understood, leaving overwhelming information vulnerabilities[92].

[90] JONES. Ctrl Z, *supra* note 61, p.83.
[91] Des études démontrent que la grande majorité des contenus disponibles en ligne disparaitront dans l'année suivant leur publication. Voir par exemple : AMBROSE, M. « It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten ». Stanford Technology Law Review, vol. 16, no. 2, 2013, p.369.
[92] JONES. Ctrl Z, *supra* note 61, p.83.

La place que prend aujourd'hui Internet dans la vie des consommateurs et son impact sur leur vie privée sont bien entendu le résultat d'un long processus (toujours en cours) d'adaptation des consommateurs et de développement des technologies. Les auteurs Yun, Lee et Kim ont développé une chronologie générale de cette évolution d'Internet et de la perception qu'en ont les internautes[93] :

- 1991-2000 : débuts d'Internet - période d'« Introduction » (World Wide Web, Google, les blogs, etc.)
- 2001-2007 : avènement des médias sociaux - période de « prise de conscience » (Youtube, Facebook, Netflix, les podcasts, etc.)
- 2008-2013 : mise en place de l'économie du partage - période de « développement » (téléphones intelligents, big data, informatique en nuage, etc.)
- 2014-aujourd'hui : transition vers l'automatisation technologique - période d'« extension » (Internet des objets, Airbnb, etc.)

Comme c'était le cas pour la vie privée en général, nous constatons qu'il n'existe aucune définition commune de la vie privée numérique. L'approche des législateurs n'aborde pas de manière différente la protection des renseignements personnels et de la vie privée par des entités privées dans le monde physique ou numérique, mais, de l'avis de plusieurs, la législation affiche généralement un retard particulièrement frappant par rapport aux développements technologiques[94].

Malgré l'absence de définition spécifique et universelle de la vie privée dans un contexte numérique, nous observons tout de même l'apparition ou la transformation de certains éléments qui sont susceptibles d'aider à cerner le concept de vie privée dans ce contexte :

- La protection de la vie privée en ligne est dorénavant perçue davantage comme un enjeu de protection des consommateurs que comme un enjeu sociopolitique[95]
- La protection des renseignements personnels est actuellement perçue comme l'élément dominant de la protection de la vie privée des consommateurs en ligne[96]
- La distinction entre les renseignements personnels dits privés et publics est de plus en plus difficile à faire dans le contexte numérique :

[93] YUN, H., LEE, G. et KIM, D. J. « A Chronological Review of Empirical Research on Personal Information Privacy Concerns: An Analysis of Situational Contexts and Research Constructs », Information & Management, vol. 56, no. 4, 1er juin 2019, p.574.
[94] Voir par exemple : TENE, O. « Privacy: The New Generations », International Data Privacy Law, vol. 1, no. 1, 2011, pp.11-13, en ligne : https://www.researchgate.net/publication/228226941_Privacy_The_New_Generations
[95] CAMPBELL, J. E. et CARLSON, M. « Panopticon.com: Online Surveillance and the Commodification of Privacy », Journal of Broadcasting & Electronic Media, vol. 46, no. 4, 2002.
[96] SHAPIRO, S. « Places and Spaces: The Historical Interaction of Technology, Home, and Privacy », Information Society, vol. 14, no. 4, octobre 1998.

> Electronic media have facilitated the development of a 'middle region' between the frontstage and backstage; they integrate 'formerly private situations into formerly public ones'. Thus, the line between the 'public' frontstage and the 'private' backstage has been substantially blurred. These impacts of the media and ICTs on the public/private distinction are apparent in a number of areas, most notably in surveillance, webcam broadcasting, the work/home division, and the social web. (…) the public/private distinction is best thought of as a continuum. This continuum is anchored on one end by the 'private' and on the other by the 'public'[97].

Nous verrons d'ailleurs au chapitre 3 que des renseignements historiquement considérés privés par les consommateurs ne font plus l'objet d'une détermination aussi tranchée aujourd'hui, en raison notamment de leur présence accrue sur les médias sociaux.

Mais avant, il importe de dresser un portrait général des préoccupations des internautes, des préoccupations qui sont influencées par leur conception respective de la vie privée et vice versa.

[97] FORD, S. M. « Reconceptualizing the public/private distinction in the age of information technology », Information, Communication & Society, vol. 14, no. 4, 2011, pp.555 et 560.

VIE PRIVÉE EN LIGNE ET CONSOMMATEURS : SURVOL DE LA LITTÉRATURE

2.1 Portrait des préoccupations des consommateurs relativement à leur vie privée en ligne

La présente section a pour but d'exposer les grands constats de la littérature en ce qui a trait aux préoccupations des consommateurs pour leur vie privée en ligne. Quelles préoccupations ont été identifiées ? Quels risques potentiels inquiètent particulièrement les internautes ? Afin de faciliter la compréhension, les éléments retenus sont accompagnés d'exemples concrets de ces risques ou de pratiques des entreprises qui justifient ou appuient les préoccupations des consommateurs en la matière. Nous aborderons également les facteurs personnels ou collectifs susceptibles d'influencer le niveau général de préoccupation des internautes ou leurs inquiétudes plus spécifiques.

Il est à noter que les préoccupations et risques soulevés dans la présente section tirent principalement leur source de sondages et d'enquêtes réalisés auprès d'internautes des États-Unis ou d'Europe[98]. Nous verrons tout de même, dans le cadre de notre exposé des résultats du sondage pancanadien de 2020 à la section suivante, qu'ils correspondent relativement bien aux préoccupations des internautes canadiens.

2.1.1. Des internautes de plus en plus inquiets pour leur vie privée

Une étude de Westin[99] sur les différents sondages d'opinion publique réalisés aux États-Unis relativement à la vie privée de la fin des années 1970 au début des années 2000 révèle certaines tendances historiques. L'auteur note un changement dans l'opinion publique vers le milieu des années 1990 en ce qui concerne le traitement de renseignements personnels par des entreprises privées[100]. Si à l'époque, l'État demeure la première source d'inquiétude, les entreprises privées arrivent dorénavant bon deuxième et le niveau de préoccupation à leur égard ne cesse d'augmenter. Les banques, les assureurs et toutes entreprises œuvrant sur Internet préoccupent tout particulièrement. Cette progression s'est poursuivie dans les vingt dernières années.

Aujourd'hui, la référence en matière d'évaluation des préoccupations relatives à la vie privée est le sondage annuel mené par Ipsos pour le compte du Centre for International Governance Innovation, d'Internet Society et de la Conférence des Nations Unies sur le

[98] HONG, W., CHAN, F. et THONG, J. « Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective », Journal of Business Ethics, vol. 168, no. 3, 2019.
[99] WESTIN, A. F. « Social and Political Dimensions of Privacy », Journal of Social Issues, vol. 59, no. 2, 2003.
[100] Voir aussi sur le sujet : O'NEIL, D. « Analysis of Internet Users' Level of Online Privacy Concerns », Social Science Computer Review, vol. 19, no. 1, février 2001, p.18.

commerce et le développement. On y sonde quelque 25 000 internautes qui couvrent les cinq continents. En 2019, c'était près de 8 répondants sur 10 qui se disaient préoccupés par leur vie privée en ligne ; 3 sur 10 se disaient très préoccupés[101]. Ces pourcentages sont constamment en hausse, puisqu'une majorité de répondants se disent chaque année plus inquiets qu'ils ne l'étaient l'année précédente :

Tableau 2

Le niveau général de préoccupation des internautes en matière de vie privée en ligne par rapport à l'année précédente

	2014	2016	2017	2018	2019
% des répondants qui se disent plus préoccupés par leur vie privée en ligne qu'il y a douze mois	64 %[102]	57 %[103]	55 %[104]	52 %[105]	53 %[106]
Beaucoup plus préoccupés (*much more concerned*)	31 %	31 %	28 %	22 %	22 %
Un peu plus préoccupés (*somewhat more concerned*)	33 %	26 %	27 %	30 %	31 %

* À noter que les données ne sont pas disponibles pour 2015 et 2020 (en date de l'été 2021).

Qu'est-ce qui peut expliquer cette progression continue du niveau de préoccupation des internautes pour leur vie privée ? Plusieurs facteurs sont généralement soulevés par les auteurs. Le plus important est indéniablement le transfert des préoccupations des individus en matière de vie privée vers le Web et ses technologies connexes, dont le développement rapide affecte considérablement le traitement des renseignements personnels.

> While consumers have had privacy concerns long before the advent of the Internet, their PIP [personal information privacy] concerns have evolved significantly with time in part due to the emergence of disruptive technologies including ecommerce, mobile computing, social media, location-based service (LBS), radio-frequency identification (RFID), IoT (Internet of Things), and big data analytics[107].

---

[101] CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION et IPSOS. « 2019 CIGI-Ipsos Global Survey on Internet Security and Trust », parties I & II, p.8, en ligne : https://www.cigionline.org/internet-survey-2019 (consulté le 20 novembre 2020).
[102] *Ibid.,* Présentation, p.17.
[103] *Ibid.,* Table de données, question 1.
[104] *Ibid.,* présentation, p.4.
[105] *Ibid.*
[106] *Ibid.,* parties I & II, p.10.
[107] YUN. « A chronological review », *supra* note 93, p.572.

Les enjeux relatifs à la protection de la vie privée en ligne prennent davantage de place dans les médias et dans l'actualité ces dernières années, ce qui peut aussi expliquer une sensibilisation accrue du public aux risques pour leur vie privée en ligne. On note par exemple la couverture importante faite suite à des fuites de données à grande échelle (Facebook en 2018, Sony en 2014, etc.)[108]. De même, les campagnes d'information et de lobbying de certains groupes influents, tel qu'Electronic Privacy Information Center (EPIC), peuvent aussi avoir contribué à l'inquiétude ambiante actuelle[109].

Enfin, si les préoccupations relatives aux gouvernements ont repris du galon suite aux scandales de Wikileaks et de Cambridge Analytica, les commerçants en ligne et les entreprises du Web demeurent fortement mal-aimés. Questionnés sur les sources de leur méfiance envers Internet, les répondants au sondage Ipsos cité plus haut pointaient notamment[110] :

- Les plateformes de médias sociaux (75 %)
- Les moteurs de recherche (65 %)
- Les fournisseurs de services d'accès Internet (63 %)
- Les plateformes de commerce en ligne (61 %)
- Les plateformes bancaires en ligne et sur mobile (56 %)

2.1.2. Les grandes préoccupations des consommateurs

Lorsqu'il est question des préoccupations plus spécifiques des internautes pour leur vie privée en ligne, plusieurs réfèrent aux travaux de Malhotra, Kim et Aagarwal[111]. Insatisfaits par les écrits passés sur le sujet – parce que peu adaptés au contexte numérique ou trop abstraits[112] - ces auteurs ont cherché à définir plus spécifiquement les grandes préoccupations des consommateurs en ligne en ce qui a trait à leur vie privée. Ils en ont retenu trois qui se rapportent aux éléments de collecte, de contrôle et de connaissance.

---

[108] HONG. « Drivers and Inhibitors », *supra* note 98; WIRTZ, J., LWIN, M. et WILLIAMS, J. « Causes and consequences of consumer online privacy concern », International Journal of Service Industry Management, vol. 18, no. 4, 2017, p.327 ; METZGER, M. J. « Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce », Journal of Computer-Mediated Communication, vol. 9, no. 4, juin 2006.
[109] WIRTZ. « Causes and consequences », *supra* note 108, p.327.
[110] CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION. « Global Survey », *supra* note 101, parties I & II, p.116.
[111] MALHOTRA, N. K., KIM, S. S. et AGARWAL, J. « Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model », Information Systems Research, vol. 15, no. 4, décembre 2004, pp. 336-35 ; PREIBUSCH, S. « Guide to measuring privacy concern: Review of survey and observational instruments », International Journal of Human-Computer Studies, vol. 71, 2013, p.1136.
[112] MALHOTRA. « IUIPC », *supra* note 111, pp.337-338 et 340.

2.1.2.1 Préoccupations quant à l'ampleur de la collecte de renseignements personnels en ligne

La première préoccupation des internautes identifiée par Malhotra, Kim et Agarwal concerne l'ampleur de la collecte de renseignements personnels en ligne[113]. Cette préoccupation n'est guère surprenante puisqu'au quotidien, un internaute fournira, volontairement ou à son insu, une quantité impressionnante de renseignements personnels à son sujet lors de son utilisation d'Internet.

- En naviguant sur le Web : En moyenne 77 % des pages Web consultées par un internaute comprennent des dispositifs de suivi (ex. : cookies)[114] ;
- En utilisant un réseau social : Près de 30 % des abonnés de Facebook partagent du contenu sur la plateforme tous les jours[115] ;
- En utilisant une application mobile : 93 % des applications de jeux disponibles sur le Google Play Store présenteraient au moins un dispositif de suivi d'un tiers (« third party trackers »)[116] ;
- En utilisant leur téléphone intelligent : un téléphone Android sur lequel Chrome est activé, communique des données de géolocalisation à Google en moyenne 14 fois par heure, et ce, même si l'utilisateur n'interagit pas avec l'appareil[117].

L'empreinte numérique

L'ensemble des données numériques semées par un internaute pendant son utilisation d'Internet forme sa trace ou son empreinte numérique[118]. Celle-ci comprend deux volets : les données personnelles partagées ou fournies activement par la personne en ligne d'une part et les données personnelles collectées passivement, c'est-à-dire à son insu (données issues d'un suivi, données relatives à l'utilisation d'appareils, données de géolocalisation, etc.) d'autre part.

L'empreinte numérique (volets actif et passif) et le traitement ultérieur des données issues des deux volets permettent généralement de dresser un portrait très détaillé de la

---

[113] *Ibid.*, pp.338-339.
[114] KARAJ, A. et al. « WhoTracks. Me: Shedding light on the opaque world of online tracking », 2018, p.1, en ligne : https://arxiv.org/abs/1804.08959
[115] FRACTL. « Average Facebook User Sharing Habits Study », 2016, en ligne : https://www.frac.tl/work/marketing-research/facebook-user-sharing-habits-study/
[116] BINNS, R. et al. « Third Party Tracking in the Mobile Ecosystem », avril 2018, p.6, en ligne : https://arxiv.org/pdf/1804.03603.pdf
[117] SCHMIDT, D. C. « Google Data collection », Digital Content Next, août 2018, en ligne : https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf
[118] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAIS. « Trace numérique », en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26508672

personne concernée[119]. À titre d'exemple, un groupe de chercheurs des universités Stanford et Cambridge qui s'est ainsi attardé à la capacité de l'intelligence artificielle d'évaluer la personnalité d'un individu à la lumière de son empreinte numérique sur les médias sociaux a obtenu des résultats pour le moins impressionnants :

> The results show that by mining Facebook Likes, the computer model was able to predict a person's personality more accurately than most of their friends and family. Given enough Likes to analyse, only a person's spouse rivalled the computer for accuracy of broad psychological traits[120].

L'empreinte numérique dépasse largement le seul contexte des médias sociaux comme Facebook. Par contre, elle semble dorénavant y prendre naissance, et ce, avant même que la personne concernée ne soit à même d'utiliser Internet ! Une étude de 2010 relative au phénomène du *sharenting* évaluait par exemple que 84 % des enfants de moins de 2 ans avaient une présence numérique au Canada (notamment par la présence de photos ou d'autres renseignements à leur sujet sur les médias sociaux de leur entourage)[121]. Une étude récente de la Commissaire aux enfants d'Angleterre évaluait qu'un enfant ferait en moyenne l'objet de 1300 publications en ligne par ses parents avant d'atteindre l'âge de 13 ans[122]. Et l'enfant fera lui-même en moyenne 70 000 publications sur les médias sociaux avant d'atteindre l'âge de la majorité[123].

La multiplicité des intervenants

Si l'on pointe (et critique) rapidement les grandes entreprises du Web telles que Facebook, Amazon ou Google pour leur collecte massive de renseignements personnels, elles sont loin d'être les seules à y participer. À la lumière des travaux de Yun, Lee et Kim[124], nous notons trois grands types d'intervenants impliqués dans la collecte ou la transmission de renseignements personnels en ligne, dont plusieurs sont généralement inconnus du consommateur :

---

[119] Pour plus de détails sur la capacité d'analyse des données par l'intelligence artificielle, voir section sur le profilage (section 2.1.2.2)
[120] CAMBRIDGE UNIVERSITY. « Computers using digital footprints are better judge of personality than friends and family », 12 janvier 2015, en ligne : https://www.cam.ac.uk/research/news/computers-using-digital-footprints-are-better-judges-of-personality-than-friends-and-family
[121] MANOTIPYA, P. et GHAZINOUR, K. « Children's Online Privacy from Parents' Perspective », Procedia Computer Science, vol. 177, 2020, p.178.
[122] CHILDREN'S COMMISSIONER. « Children's Commissioner's report calls on internet giants and toy manufacturers to be transparent about collection of children's data », 8 novembre 2018, en ligne : https://www.childrenscommissioner.gov.uk/2018/11/08/childrens-commissioners-report-calls-on-internet-giants-and-toy-manufacturers-to-be-transparent-about-collection-of-childrens-data/
[123] *Ibid.*
[124] YUN. « A Chronological Review », *supra* note 93, p.585.

Type 1 - L'internaute lui-même, qui diffuse ou transmet volontairement ou activement des renseignements personnels à son sujet en ligne, par exemple sur les médias sociaux ou lors de transactions en ligne.

Type 2 - Les entreprises avec lesquelles l'internaute fait directement affaire lorsqu'il se procure un bien ou qu'il utilise un service en ligne. L'entreprise peut collecter des renseignements :

- Fournis activement par l'internaute (ex. : ses renseignements financiers en vue de conclure une transaction) ;
- Fournis passivement par l'internaute dans le cadre de la transaction et de son utilisation du produit ou du service (ex. : témoins de connexion de l'entreprise sur son site Web, données d'utilisation d'un objet connecté, etc.).

Type 3 - Les tiers qui n'ont pas de lien direct avec la personne concernée par les renseignements personnels, par exemple :

- Les entreprises qui collectent des données à partir de dispositifs de suivi (tels que des témoins et des balises Web) ;
- Les entreprises d'exploration de données qui utilisent notamment des procédés de *data harvesting, data crawling* et *data mining* afin de collecter à grande échelle des données disponibles sur Internet ;
- Les entreprises de courtage de données qui achètent et vendent les renseignements personnels d'internautes, notamment auprès d'entreprises ayant fait affaire directement avec eux et auprès d'entreprises de suivi et d'exploration de données ;
- Les pirates informatiques qui accèdent de manière non autorisée aux renseignements personnels (par *hacking,* par *phishing,* au moyen de *spywares,* etc.).

Le phénomène des mégadonnées

Il importe aussi d'aborder brièvement l'existence des mégadonnées, mieux connues sous leur nom anglais de *Big data*, qui contribue assurément à la préoccupation des consommateurs quant à la quantité de leurs renseignements personnels qui circulent en ligne.

Les mégadonnées sont en fait des ensembles de données, structurés ou non, qu'on peut décrire par trois « v » : volume, variété et vitesse[125]. Elles représentent en réalité une très

[125] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. « Mégadonnées », en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26507313 (consulté le 10 avril 2021).

large quantité de données qui proviennent d'une grande variété de sources. Et elles sont entreposées et traitées particulièrement rapidement au moyen d'outils technologiques de pointe (les outils classiques de traitement des données n'étant pas assez puissants). La variété de sources de ces données et les formats dans lesquelles elles sont enregistrées sont les éléments distinctifs des mégadonnées par rapport à celles qui se retrouvent dans les bases de données traditionnelles[126].

Selon le Forum économique mondial, c'est quelques 463 exaoctets[127] de données qui seront créés chaque jour à partir de 2025[128].

2.1.2.2 Préoccupations quant à la perte de contrôle sur les renseignements personnels en ligne

La seconde préoccupation des internautes identifiée par Malhotra, Kim et Agarwal concerne la perte de contrôle sur leurs renseignements personnels en ligne[129], que ce soit au moment de la collecte, de la divulgation ou de l'utilisation. Face à l'ampleur de la collecte de données décrite plus haut, il n'est guère surprenant que plusieurs sondages américains et européens confirment le sentiment généralisé des internautes quant à cette perte de contrôle[130].

Bien que le consentement du consommateur soit couramment demandé par une entreprise en vue de collecter ses renseignements personnels en ligne, ce dernier n'a bien souvent pas d'autre choix réel que d'accepter s'il souhaite accéder au site Web de l'entreprise ou utiliser son service. Le « contrôle » qu'il pourrait dès lors exercer, par exemple en refusant la collecte, se trouve assorti de conséquences négatives, comme la perte d'accès ou la perte de choix dans les services et produits disponibles. Plus encore, dans certains cas, cette perte d'accès ne garantit pas pour autant l'absence d'intrusion dans sa vie privée. Facebook a été sévèrement critiqué par le passé en raison de sa collecte de renseignements personnels relatifs à des internautes n'utilisant même pas le service[131] !

---

[126] IPPOLITO, P. P. « Big Data Analysis: Spark and Hadoop », Towards data science, 11 juillet 2019, en ligne : https://towardsdatascience.com/big-data-analysis-spark-and-hadoop-a11ba591c057

[127] 1,000,000,000,000,000,000 bytes

[128] Soit l'équivalent de 212,765,957 DVDs par jour. DESJARDINS, J. « How much data is generated each day? », World Economic Forum, 17 avril 2019, en ligne : https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

[129] MALHOTRA. « IUIPC », *supra* note 111, p.339.

[130] KEDMEY, D. « 9 in 10 Americans Feel They've Lost Control of Their Personal Data », Time, 12 novembre 2014, en ligne : https://time.com/3581166/privacy-personal-data-report/ ; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION. « Most Americans Continue to Have Privacy and Security Concerns », 20 août 2018, en ligne : https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds ; AXCIOM et DMA. « Data privacy: What the consumer really thinks », février 2018, p.15, en ligne : https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy---what-the-consumer-really-thinks-final_5a857c4fdf799.pdf

[131] INGRAM, D. « Facebook fuels broad privacy debate by tracking non-users », Reuters, 15 avril 2018, en ligne : https://www.reuters.com/article/us-facebook-privacy-tracking-id ; BRANDOM, R. « Shadow profiles are the biggest flaw in Facebook's privacy defense », The Verge, 11 avril 2018, en ligne : https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy

Pour expliquer le fondement de cette préoccupation des internautes à l'égard du contrôle qu'ils exercent sur leurs renseignements personnels, les auteurs réfèrent au désir de justice intrinsèque aux individus. Une situation sera perçue comme plus acceptable - plus juste - si elle fait suite à une procédure sur laquelle le consommateur a pu exercer un certain contrôle[132]. En ce sens, l'absence ou le degré très faible de contrôle qu'exercent aujourd'hui les internautes sur la collecte de leurs renseignements personnels en ligne et les usages subséquents les rend naturellement plus inquiets pour leur vie privée en ligne[133].

2.1.2.3 Préoccupations quant au manque de connaissances relatives à la protection de la vie privée en ligne

L'ultime préoccupation générale identifiée par Malhotra, Kim et Agarwal se rapporte au manque de renseignements disponibles et à la méconnaissance des internautes relativement aux pratiques des entités privées en ligne qui sont impliquées dans le traitement de leurs renseignements personnels[134]. Cette préoccupation qui réfère plus largement aux questions de transparence est particulièrement importante étant donné que les choix faits par les internautes lorsqu'ils utilisent Internet sont tributaires de leur compréhension des pratiques et politiques des entreprises à ce sujet.

Les auteurs Correia et Compeau se sont penchés sur la sensibilisation des internautes relativement à la protection de leur vie privée en ligne. Ils identifient différents volets de la tâche colossale à laquelle devrait s'astreindre quiconque désire être informé et comprendre l'environnement numérique dans lequel ses renseignements personnels circulent[135] :

- Connaissance et compréhension des pratiques courantes de traitement des renseignements personnels par les entreprises en ligne ;
- Connaissance et compréhension des technologies utilisées ;
- Connaissance et compréhension de l'encadrement législatif et réglementaire pertinent ;
- Évaluation de l'impact de ces différents éléments sur le traitement des renseignements personnels dans une situation donnée ;
- Évaluation de l'impact des actions posées et des choix offerts sur le traitement des renseignements personnels dans une situation donnée.

---

[132] MALHOTRA. « IUIPC », *supra* note 111, p.339.
[133] Voir également KUO, K-M et TALLEY, P. C. « An empirical investigation of the privacy concerns of social network site users in Taiwan », 2014, p.6, en ligne : https://pdfs.semanticscholar.org/e2c0/e03165b91bdcab6e9e2d9858b5d3be015489.pdf
[134] MALHOTRA. « IUIPC », *supra* note 111, p.339.
[135] CORREIA, J. et COMPEAU, D. « Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA », 50 th Hawaii International Conference on System Sciences, 2017, pp.4023-4024, en ligne : https://pdfs.semanticscholar.org/b9e7/0317060e75bdaf52174391fb1f93e77b5268.pdf

D'autres auteurs ont également inclus la connaissance qu'ont les internautes des atteintes passées à leurs renseignements personnels en ligne et de celles qui sont susceptibles de se produire dans le futur[136].

Les politiques de protection de la vie privée

Lorsqu'il est question de la faible compréhension qu'ont les internautes du traitement de leurs renseignements personnels en ligne et des préoccupations que cette situation engendre, les problèmes relatifs aux politiques de protection de la vie privée (parfois appelées politiques de vie privée ou politiques de confidentialité) ne peuvent être passés sous silence.

Ces documents, auxquels renvoient régulièrement des liens dans des fenêtres et bannières au bas des pages Web, décrivent les pratiques d'une organisation ou d'un site Web en matière de collecte, d'utilisation et de communication des renseignements personnels. Si ces documents sont en théorie « the single most important source of information for users[137] », on leur reproche régulièrement de ne pas réellement faciliter comme ils le devraient la compréhension de l'information par les internautes. Pourquoi ?

Les documents sont trop longs, ce qui en décourage plus d'un et rend irréaliste une lecture attentive et répétée. Une étude du New York Times sur la politique de protection de la vie privée de Google exposait l'évolution drastique du document sur une période de 20 ans ; quelque trente versions différentes, qui l'ont fait passer de 600 mots en 1999 à 4000 mots en 2019[138]! À elle seule, la lecture d'un tel document prendra en moyenne près de 20 minutes à l'internaute, ce qui la rend d'autant moins plausible[139]. La lecture des politiques de Facebook, de Wikipedia ou encore de Netflix dépasse elle aussi la barre des 20 minutes chacune[140].

Les politiques sont ambiguës, ce qui en rend difficile la compréhension. Une étude de Kaur *et al.* sur les politiques de protection de la vie privée de plusieurs milliers de sites Web, dont les 1000 plus fréquentés, notait la présence très courante de termes ambigus (*may, generally, appropriate,* etc.)[141]. En fait, près de 50 % des phrases des 2000 documents étudiés comportaient au moins un mot qualifié d'ambigu par les auteurs de l'étude publiée

---

[136] Voir par exemple BRECHT, F. *et al*. « Communication Anonymizers: Personality, Internet Privacy Literacy and Their Influence on Technology Acceptance », European Conference on Information Systems 214, 2012, p.3.
[137] REIDENBERG, J. R. *et al*. « Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding », Berkeley Technology Law Journal, vol. 30, 2015, p.39.
[138] WARZEL, C. et NGU, A. « Google's 4,000-Word Privacy Policy Is a Secret History of the Internet », New York Times, 10 juillet 2019, en ligne : https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html
[139] Cette évaluation a été réalisée à l'aide du site http://www.combiendemots.com/ à partir de la version de la politique de Google en date du 22 janvier 2019.
[140] Ces évaluations ont été réalisées à l'aide du site http://www.combiendemots.com/ à partir des documents suivants : version de la politique de Facebook en date du 19 avril 2018, version de politique de Wikipedia en date du 24 mai 2018 et version de la politique de Netflix en date du 24 avril 2019.
[141] KAUR, J. *et al*. « A comprehensive keyword analysis of online privacy policies », Information Security Journal: A Global Perspective, vol. 27, no. 5-6, 2018, p.268.

au printemps 2019[142]. Par conséquent, les interprétations, même entre experts, peuvent varier considérablement au sujet d'une même politique, comme le rapportait une étude de Reidenberg *et al.*[143]

Et elles sont complexes. Selon une seconde étude du New York Times, la complexité des termes employés et la longueur des phrases de nombreuses politiques sont telles que le niveau de lecture requis correspond, pour la plupart, à celui que demandent des études collégiales ou universitaires. Le niveau requis pour les politiques de Airbnb, Twitch et Ebay est, par exemple, similaire à celui qu'exige l'œuvre d'Emmanuel Kant, *Critique de la raison pure*[144].

2.1.3 Les principaux risques identifiés par les consommateurs

La littérature relève également une série de risques plus spécifiques qui préoccupent les consommateurs en ce qui concerne la protection de leur vie privée en ligne. Ils sont résumés et mis en contexte dans les pages qui suivent.

Mentionnons d'emblée qu'il existe un lien entre le niveau général de préoccupation des internautes pour la protection de leur vie privée en ligne et leurs croyances à l'égard des risques qu'ils courent en ligne. Sauf exception, plus un internaute est inquiet, plus il identifiera des risques pour ses renseignements personnels en ligne et plus il jugera risqué de les divulguer en ligne[145].

Mentionnons également que les préoccupations de chaque consommateur ne sont pas fixes et peuvent varier considérablement selon les circonstances et surtout selon les renseignements personnels en jeu. Les sondages repris dans la littérature ne font généralement pas la distinction selon le type de renseignements personnels (ex. : renseignements sensibles) dans les questionnaires, pas plus que dans les résultats.

2.1.3.1. Risques relatifs à la sécurité des renseignements

Parmi les risques les plus couramment cités dans les sondages réalisés auprès d'internautes, on trouve ceux relatifs à la sécurité des renseignements en ligne.

---

[142] *Ibid.*
[143] « The findings show areas of common understanding across all groups for certain data collection and deletion practices, but also demonstrate very important discrepancies in the interpretation of privacy policy language, particularly with respect to data sharing. The discordant interpretations arose both within groups and between the experts and the two other groups. » : REIDENBERG. « Disagreeable Privacy Policies », *supra* note 137, p.40.
[144] LITMAN-NAVARRO, K. « We Read 150 Privacy Policies. They Were an Incomprehensible Disaster », New York Times, 12 juin 2019, en ligne : https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html
[145] KOOHANG, A., PALISZKIEWICZ, J. et GOLUCHOWSKI, J. « Social media privacy concerns: trusting beliefs and risk beliefs », Industrial Management & Data Systems, vol. 118, no. 6, 2018, p.1214.

Pourtant, ce thème ne relève pas a priori de la protection de la vie privée. La question de la sécurité des données réfère aux protections mises en place par les entreprises afin d'éviter l'accès non autorisé ou la perte de données collectées, conservées et traitées par elles. Les données dont il est question ne sont pas nécessairement des renseignements personnels. La question de la protection de la vie privée en ligne ne concerne pour sa part que les renseignements à caractère personnel (c'est-à-dire ceux qui se rapportent à une personne identifiée ou identifiable)[146], mais couvre par contre d'autres volets que la seule sécurité desdits renseignements.

Pourquoi donc parler de sécurité des données dans le cadre de l'étude des préoccupations des consommateurs pour la protection de leur vie privée en ligne ? Parce qu'en pratique, les consommateurs ne font pas cette distinction - les législateurs non plus d'ailleurs - et parce qu'une atteinte à la sécurité de renseignements personnels détenus par une entreprise, par exemple, peut rapidement engendrer une atteinte à la vie privée de l'individu concerné. Il est donc légitime, voire essentiel, d'aborder les préoccupations des consommateurs relativement à la sécurité des données dans le cadre de cette étude.

Voyons donc les principales préoccupations à ce sujet recensées dans les sondages passés.

De nombreux internautes s'inquiètent du stockage de leurs renseignements personnels de manière inadéquatement sécurisée[147]. Ce risque couvre aussi bien les systèmes sur lesquels ils ont le contrôle (ex. : ordinateur personnel, téléphone intelligent) que les systèmes d'entreposage proposés par les entreprises (services d'infonuagique par exemple) ou utilisés par ces dernières afin de conserver les données collectées, traitées ou achetées d'une autre entreprise.

On craint bien entendu l'accès non autorisé aux systèmes et aux renseignements qui s'y trouvent, mais également la perte desdits renseignements qui découlerait par exemple d'un problème technique, d'une erreur humaine ou d'un évènement externe imprévisible ex. : des centres de données affectés par la foudre[148], ravagés par des incendies[149] ou détruits lors de l'effondrement d'un immeuble[150]).

---

[146] THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO et DELOITTE & TOUCHE. « The Security-Privacy Paradox: Issues, Misconceptions, and Strategies », août 2003, en ligne : https://www.ipc.on.ca/wp-content/uploads/Resources/sec-priv.pdf ; MINORITY HIV/AIDS FUND. « The Difference between Security and Privacy and Why It Matters to Your Program », U.S. Department of Health & Human Services, en ligne : https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program

[147] OFCOM et ICO. « Internet users' experience of harm online: summary of survey research », 18 septembre 2018, pp.7-9, en ligne : https://www.ofcom.org.uk/__data/assets/pdf_file/0018/120852/Internet-harm-research-2018-report.pd ; KPMG. « Companies that fail to see privacy as a business priority risk crossing the 'creepy line' », 7 novembre 2016, en ligne : https://home.kpmg/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html

[148] « Google loses data as lightning strikes », BBC News, 15 avril 2015, en ligne : https://www.bbc.com/news/technology-33989384

[149] SAWERS, P. « OVH datacenter disaster shows why recovery plans and backups are vital », VentureBeat, 10 mars 2021, en ligne : https://venturebeat.com/2021/03/10/ovh-datacenter-disaster-shows-why-recovery-plans-and-backups-are-vital

[150] GUILBAULT, J-F. « L'infonuagique, nerf du commerce au 21e siècle », Radio-canada, 23 août 2019, en ligne : https://ici.radio-canada.ca/nouvelle/1267691/infonuagique-commerce-securite-donnees-quebec-analyse-experts

En ce qui concerne l'accès non autorisé aux renseignements personnels, les consommateurs réfèrent tout particulièrement aux situations de vols de données, notamment à la suite ou au moyen de cyberattaques (virus, maliciel, logiciel espion, cheval de Troie[151], etc.)[152]. Ce n'est donc pas ultimement la non-sécurisation des bases de données qui les préoccupe, mais plutôt l'accès non autorisé qui pourrait en résulter et l'utilisation subséquente qui pourrait être faite des renseignements personnels qui s'y trouvaient[153].

Des cas de piratage de renseignements personnels sur des sites Web, des plateformes ou des serveurs d'entreprises en ligne font couramment les manchettes. Et les quantités de renseignements en jeu et d'internautes visés peuvent être alarmantes, comme en témoignent les exemples suivants :

- 3 milliards de comptes de messagerie *Yahoo* dont les renseignements ont été piratés en 2013 (coordonnées, dates de naissances, numéros de téléphone, mots de passe cryptés, questions de sécurité, etc.)[154]
- 540 millions de fichiers relatifs aux utilisateurs de Facebook ont été piratés en 2019[155]
- 383 millions de fichiers relatifs aux usagers des hôtels Marriott International ont été piratés en 2018 (coordonnées, adresses courriel, numéro de passeport, modes de paiement, etc.)[156]
- 145 millions de fichiers relatifs aux usagers d'*Ebay* ont été piratés en 2014 (coordonnées, mots de passe cryptés, etc.)[157]

---

[151] Pour des explications sur les différents types de chevaux de Troie (*Backdoor Trojan, Infostealer Trojan, Trojan IM, Ransom Trojan, Fake AV Trojan,* etc.), voir : NORTON. « What is a Trojan ? Is it a virus or is it malware? », en ligne : https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (consulté le 10 août 2021).
[152] OFCOM. « Internet users' experience », *supra* note 147, pp.7-9.
[153] *Ibid.,* p.13 ; PAINE SCHOFIELD, C. *et al.* « Internet users' perceptions of 'privacy concerns' and 'privacy actions' », International Journal of Human-Computer Studies, vol. 65, 2007, p.531, table 1 ; ACEI. « Les Canadiens méritent un meilleur Internet », juin 2019, en ligne : https://www.cira.ca/fr/resources/letat-de-linternet/rapport/les-canadiens-meritent-un-meilleur-internet ; MOZILLA. « Hackers, Trackers and Snoops: Our Privacy Survey Results », 9 mars 2017, en ligne : https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5
[154] PERLROTH, N. « All 3 Billion Yahoo Accounts Were Affected by 2013 Attack », New York Times, 3 octobre 2017, en ligne : https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html
[155] SILVERSTEIN, J. « Hundreds of millions of Facebook user records were exposed on Amazon cloud server », CBS News, 4 avril 2019, en ligne : https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/
[156] O'FLATHERTY, K. « Marriott CEO Reveals New Details About Mega Breach », Forbes, 11 mars 2019, en ligne : https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#d1045cb155c0
[157] KELLY, G. « eBay Suffers Massive Security Breach, All Users Must Change Their Passwords », Forbes, 21 mai 2014, en ligne : https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#4ef529797492

L'utilisation des renseignements personnels à des fins criminelles

Si les consommateurs soulèvent régulièrement le thème distinct de la sécurité des données dans le cadre de sondages relatifs à la protection de leur vie privée, ils tendent aussi à inclure un autre thème connexe, celui de l'utilisation criminelle de leurs renseignements personnels (généralement à la suite d'un accès non autorisé).

Les sondages font ainsi état de plusieurs préoccupations relatives à l'utilisation non autorisée de leurs renseignements (vol d'identité[158], transactions financières non autorisées, fraudes) et aux conséquences de cette utilisation (pertes financières[159], dossier de crédit entaché[160], extorsion[161]). On y note également des craintes relativement à la vente de renseignements volés, un marché particulièrement lucratif. Une recherche menée par l'émission *BBC Watchdog* révélait par exemple que la valeur des données volées avait considérablement augmenté en 2019, allant jusqu'à tripler dans certains cas[162]. Les données relatives aux comptes bancaires, aux cartes de crédit et aux cartes de débit d'un consommateur vaudraient aujourd'hui environ 1500 $ (1025 €), 50 $ (33 €) et 70 $ (46 €) respectivement. Les données relatives au passeport se vendraient près de 3000 $ (2050 €) et celles relatives au permis de conduire, 1400 $ (956 €). Plus modeste, le coût des données concernant les comptes Facebook et Netflix ne s'élèverait qu'à une vingtaine de dollars (une quinzaine d'euros tout au plus)[163].

---

158 NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *supra* note 130 ; PAINE SCHOFIELD. « Internet users' perceptions », *supra* note 153, p. 531, table 1 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019 », 11 mars 2019, figure 8, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/

159 OFCOM. « Internet users' experience », *supra* note 147, pp.7-9 et 13 ; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *supra* note 130 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Recherche qualitative sur l'opinion publique auprès des Canadiennes et des Canadiens sur le consentement », mars 2017, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2017/por_201703_consent/

160 ACCOUTING TODAY. « One in four Americans victims of information security breaches », 21 avril 2015, en ligne : https://www.accountingtoday.com/opinion/one-in-four-americans-victims-of-information-security-breaches-aicpa-survey-finds

161 CONSUMERS COUNCIL OF CANADA. « Les appareils mobiles face aux cybermenaces », juin 2013, en ligne : https://www.consumerscouncil.com/site/consumers_council_of_canada/assets/pdf/509822_ccc_cyberthreatsfr.pdf

162 PARSONS, J. « Revealed: How much your stolen account IDs are worth online », Metro UK, 6 juin 2019, en ligne : https://metro.co.uk/2019/06/06/revealed-much-stolen-account-ids-worth-online-9837645/

163 MIGLIANO, S. « Dark Web Market Price Index 2019 », TOP10VPN, 5 juin 2019, en ligne : https://www.top10vpn.com/news/privacy/dark-web-market-price-index-2019-june-uk-update/ ; Pour des estimations plus générales, voir aussi ELLIS, W. « How Much Does Your Data Cost on the Dark Web? – We Checked », Privacy Australia, 2 juin 2019, en ligne : https://privacyaustralia.net/dark-web-personal-data/

2.1.3.2. Risques relatifs à la commercialisation

Des internautes se disent également inquiets par la commercialisation de leurs renseignements personnels en ligne. Ils craignent tout particulièrement le profilage[164], l'exposition à la publicité comportementale[165] et la vente de leurs renseignements personnels à des tiers[166], qui découleraient d'un suivi accru de leurs activités en ligne.

Le profilage

Considérant le développement rapide des technologies qui permet l'extraction et l'agrégation des renseignements personnels des internautes en ligne, il existe un risque que des profils détaillés soient élaborés à leur sujet à la manière d'un « effet mosaïque[167] ».

Dans le cadre d'un projet sur le profilage en ligne, la fondation Panoptykon a élaboré une classification des renseignements potentiellement utilisés à cette fin. Elle distingue trois niveaux, soit les renseignements personnels qu'un internaute partage de lui-même en ligne (sur les médias sociaux, sur des applications, etc.) et auprès des entreprises avec lesquelles l'internaute fait directement affaire, les renseignements obtenus à partir de ces données de base et qui permettent d'obtenir un portrait de son comportement en ligne et les renseignements obtenus par une analyse algorithmique, au moyen de l'intelligence artificielle[168]. Voici quelques exemples de ces renseignements (et de la progression du portrait qui peut être fait de l'internaute), selon les niveaux :

---

[164] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉ DU CANADA. Sondage 2018-2019, *supra* note 158 ; MATT, C. et PECKELSEN, P. « Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior », 49ème Hawaii International Conference on System Sciences, 2016, p.174 ; MOZILLA. « Hackers », *supra* note 153.
[165] OFCOM. « Internet users' experience », *supra* note 147, pp.7-19 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉ DU CANADA. Sondage 2018-2019, *supra* note 158, figure 10.
[166] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Recherche qualitative », *supra* note 159 ; KPMG. « Companies that fail », *supra* note 147.
[167] MATT. « Sweet Idleness », *supra* note 164, p.174.
[168] PANOPTYKON FOUNDATION. « Three layers of your digital profile », 18 mars 2019, en ligne : https://en.panoptykon.org/articles/three-layers-your-digital-profile ; SZYMIELEWICZ, K. « Your digital identity has three layers, and you can only protect one of them », Quartz, 25 janvier 2019, en ligne : https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/

Tableau 3

Des exemples de renseignements personnels recueillis ou déduits dans le cadre du profilage des consommateurs en ligne, selon leur niveau

<table>
<tr><th>Niveau 1</th><th>Niveau 2</th><th>Niveau 3</th></tr>
<tr><td>Numéro de carte de crédit</td><td>Historique et habitudes d’achats en ligne</td><td>Types de consommateur (impulsif, averti, loyal, etc.)
Estimation du niveau de revenu</td></tr>
<tr><td rowspan="2">Adresses</td><td>Habitudes de déplacement</td><td>Achat d’une nouvelle maison</td></tr>
<tr><td>Géolocalisation de l’appareil
Adresse IP</td><td>Présence d’une hypothèque, prêt-auto
Chômage</td></tr>
<tr><td>Historique de recherche</td><td>Sites visités et contenus vus en ligne</td><td rowspan="2">Évènements heureux dans la famille (naissance, mariage, etc.)
Intérêts amoureux
Appartenance politique et religieuse
Problèmes de santé</td></tr>
<tr><td>Mentions « j’aime » et autres « réactions »</td><td>Publicités sur lesquelles l’internaute a cliqué</td></tr>
<tr><td>Réglages de l’appareil connecté</td><td>Manière de faire défiler le contenu en ligne
Dynamique de frappe (vitesse, erreurs, etc.)</td><td>Signes de dépression</td></tr>
</table>

Certaines compagnies spécialisées dans le profilage des consommateurs ont développé des catégories de consommateurs – c’est-à-dire des profils types – vers lesquels les commerçants et les spécialistes du marketing et de la publicité peuvent ensuite concentrer leurs interventions. Pensons par exemple aux catégories suivantes développées aux États-Unis, qui incorporent des caractéristiques liées à l’emploi, à la région, à la culture, etc. : « Urban Cores (Single City Blues, Hispanic Mix, Inner Cities) », « Affluentials (Young Influentials, New Empty Nests, Boomers & Babies, Suburban Sprawl, Blue-Chip Blues) » et « Inner Suburbs (Upstarts & Seniors, New Beginnings, Mobility Blues, Gray Collars) »[169] .

[169] ELECTORNIC PRIVACY INFORMATION CENTER. « Privacy and Consumer Profiling », en ligne : https://epic.org/privacy/profiling/ (consulté le 5 juin 2020).

La publicité comportementale

Il est possible pour les publicitaires de personnaliser, en fonction du profil détaillé des consommateurs, la publicité qui leur est présentée en ligne. On parle alors de publicité comportementale ou de publicité ciblée. Les internautes sont ainsi exposés à de la publicité qui est susceptible de correspondre à leurs goûts et habitudes et de répondre à leurs besoins ou intérêts.

L'utilisation du profilage des consommateurs à des fins publicitaires peut également mener à un autre phénomène : la tarification des biens et services en ligne au moyen d'algorithmes qui tiennent compte des caractéristiques personnelles du client (parfois appelée tarification personnalisée)[170]. Les prix peuvent ainsi être adaptés en fonction de l'importance qu'accorde le consommateur aux prix dans ses habitudes de consommation en ligne (*price-sensitivity*). Notons que cette pratique commerciale est pour l'instant très peu utilisée par les entreprises et que son utilisation se concentrerait davantage présentement dans le secteur du tourisme[171].

La vente de données aux tiers

En plus de servir à cibler les consommateurs potentiels en ligne, la collecte et le traitement des renseignements à caractère personnel des internautes sont également une source de revenus importante pour certains sites Web et entreprises en ligne, puisque ces renseignements peuvent par la suite être vendus à des entreprises tierces.

Cette pratique est aujourd'hui largement répandue. À titre d'exemples, les données qui proviennent des transactions effectuées par carte de crédit sont régulièrement vendues[172], tout comme les données de géolocalisation des abonnés des grands fournisseurs de services de télécommunications, Telus, Rogers et Bell, déterminées en fonction des tours de téléphonie cellulaire à proximité[173].

---

[170] ZUIDERVEEN BORGESIUS, F. et POORT, J. « Online Price Discrimination and EU Data Privacy Law », Journal of Consummer Policy, vol. 40, 2017, p.348.
[171] EUROPEAN COMMISSION. DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS. « Consumer market study on online market segmentation through personalised pricing/offers in the European Union », juin 2018, pp.43-46, en ligne : https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf.
[172] COHAN, P. « Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data », Forbes, 22 juin 2018, en ligne: https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/#7dea37557722 ; STURGEON, J. « Grocers are collecting your shopping data–should consumers be wary? », Global News, 9 mai 2014, en ligne: https://globalnews.ca/news/1301367/grocers-are-collecting-your-shopping-data-should-consumers-be-wary/
[173] BRAGA, M. « How Rogers, Telus and Bell sell access to your location data to third-party companies », CBC, 18 mai 2018, en ligne: https://www.cbc.ca/news/technology/rogers-bell-telus-enstream-location-data-sharing-securus-1.4666739

Mais qui achète ces données ? En 2018, la coentreprise des trois fournisseurs en question, EnStream, avait refusé de dévoiler les noms des entreprises à qui étaient vendues ces données de géolocalisation.

L'enregistrement obligatoire des entreprises tierces qui vendent ou achètent des données personnelles dans l'État du Vermont depuis quelques années aura permis de dresser un portrait de la variété des entreprises en jeu, qui comprennent entre autres des agences d'évaluation du crédit et des entreprises spécialisées dans la recherche ou la localisation de personnes et, sans surprise, des entreprises spécialisées en publicité et marketing[174].

S'ajoutent à ces entreprises celles dont l'activité principale est spécifiquement l'achat et la vente de données, soit les entreprises de courtage de données. Il en existerait environ 4000 dans le monde[175], dont Axciom Corporation, l'une des plus importantes et vraisemblablement la plus connue. En 2012, l'entreprise affirmait détenir en moyenne 1500 types de renseignements à caractère personnel (*data points*) sur quelque 500 millions de consommateurs dans le monde et procéder annuellement à 5 milliards de transactions de données[176]. Le survol d'un document promotionnel récent de l'entreprise nous permet de constater qu'elle vend une immense variété de renseignements à caractère personnel, des renseignements sociodémographiques (ex. : éducation, âge, statut matrimonial) aux renseignements d'ordre financier (ex. : revenu annuel, niveau de stabilité financière, présence d'une hypothèque, d'épargnes, etc.), en passant par l'identification des biens consommés ou possédés par les individus (ex. : modèle de voitures et d'électroménagers, produits alimentaires et pharmaceutiques consommés)[177].

2.1.3.3. Risques relatifs à la réputation et à l'intégrité

Les internautes notent également plusieurs risques pour leur vie privée en ligne qui ont trait à leur réputation et à leur intégrité. Si les autres risques étaient plus susceptibles de se produire dans le cadre de transactions économiques, ces risques-ci sont plus généralement associés aux médias sociaux, bien qu'ils ne leur soient pas exclusifs. Ces sites Web sont généralement structurés de manière à faciliter l'identification des individus visés ou impliqués dans une publication. Qui plus est, ils permettent la reproduction rapide

[174] MELENDEZ, S. et PASTERNACK, A. « Here are the data brokers quietly buying and selling your personal information », Fast Company, 2 mars 2019, en ligne: https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information
[175] WEBFX. « What Are Data Brokers – And What Is Your Data Worth? », 16 mars 2020, en ligne: https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/
[176] KROFT, S. « The Data Brokers: Selling your personal information », CBS, 9 mars 2014, en ligne : https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ ; SINGER, N. « Mapping, and Sharing, the Consumer Genome », New York Times, 16 juin 2012, en ligne: https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0%20 ; WEBFX. « What Are Data Brokers », *supra* note 175.
[177] ACXIOM. « Auto: Driving Insights », en ligne: https://www.acxiom.com/wp-content/uploads/2013/10/Industry-Insights-DataPackages.pdf (consulté le 10 juillet 2021).

du contenu initialement publié au moyen de fonctions de partage et offrent des fonctions qui facilitent la recherche de personnes ou de renseignements précis[178].

Ainsi, plusieurs sondages réalisés par le passé rapportent une crainte générale des internautes de voir des renseignements compromettants ou gênants à leur sujet divulgués publiquement sur Internet, et ultimement, de voir leur réputation entachée[179]. Ces renseignements peuvent concerner leurs opinions politiques ou leur historique médical ou sexuel par exemple. Sur ce dernier point, on peut penser au phénomène de la *revenge porn*, qui consiste en la diffusion d'images ou de vidéos de nature sexuelle/intime sans le consentement du sujet (généralement, mais pas exclusivement, à la suite d'une rupture amoureuse). Selon une étude américaine de 2016, une personne sur 25 en aurait déjà été victime ou aurait été menacée de l'être[180]. Les victimes sont en grande majorité des femmes[181] et/ou des personnes issues de la communauté LGBTQ[182].

Les renseignements dévoilés sur autrui en ligne dans le but de nuire peuvent aussi concerner certains comportements jugés inacceptables en société ou à tout le moins par ceux qui les dénoncent. On trouve plusieurs sites Web destinés à identifier et humilier publiquement des personnes « fautives » (ex : *Don'tDateHimGirl.com* et *HollaBackNYC.com,* qui répertorient des hommes aux comportements inappropriés, notamment lors de rendez-vous galants ou en public[183], *BitterWaitress.com* qui répertorie des clients de restauration peu généreux[184] ou encore *CarpoolCheats.org* qui répertorie des « tricheurs du covoiturage »[185]).

Il est intéressant de noter que l'humiliation publique (*shaming*) et l'Internet ont une relation des plus paradoxales. Les auteurs Laidlaw et Solove l'expliquent ainsi :

> The internet is a particularly effective place to deploy shaming. In one way, shame sanctions have an important role to play online where laws can be easily circumvented and social norms have a weaker hold. Shaming here has normative force in regulating the rules of behaviour in

---

178 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Réputation en ligne Que dit-on à mon sujet ? », janvier 2016, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/or_201601/#fn5-rf

179 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. Sondage auprès des Canadiens sur la protection de la vie privée de 2016, décembre 2016, Figure 7, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/por_2016_12/ ; OFCOM. « Internet users' experience », *supra* note 147, pp.7-9.

180 LENHART, A., YBARRA, M. et PRICE-FEENEY, M. « Nonconsensual image sharing: one in 25 Americans has been a victim of "revenge porn" », Center for Innovative Public Health Research, mémo 12.13.2016, p.4, en ligne : https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf

181 LAIDLAW, E. B. « Online Shaming and the Right to Privacy », Laws 2017, vol. 6, no. 1, p.5.

182 LENHART. « Nonconsensual image sharing », *supra* note 180, p.5.

183 LEIBOVICH, L. « Don't date him, girl! », Salon, 7 août 2006, en ligne : https://www.salon.com/2006/08/07/dont_date_him_girl/ ; STONE, G. « Hey, Macho Man: Say Cheese! », Good Morning America, 12 mars 2016, en ligne : https://abcnews.go.com/GMA/Technology/story?id=1715494

184 MOSKIN, J. « The Waiter You Stiffed Has Not Forgotten », New York Times, 2 février 2005, en ligne : https://www.nytimes.com/2005/02/02/dining/the-waiter-you-stiffed-has-not-forgotten.html

185 CABANATUAN, M. et GATHRIGHT, A. « Commuters' Web site catches carpool cheats in the act », San Francisco Chronicle, 22 décembre 2003, en ligne : https://www.sfgate.com/bayarea/article/Commuters-Web-site-catches-carpool-cheats-in-the-2508620.php

> participating in an online space (…) This is the irony. It is the very weakening of norms in reining in some behaviour of users on social media that makes shame sanctions more powerful[186].
>
> Like gossip, shaming has long served as a common practice to keep people from violating society's rules and norms. Shaming helps maintain order and civility. Yet when transplanted to the Internet, shaming takes on some problematic dimensions[187].
>
> Instead of enhancing social control and order, Internet shaming often careens out of control. It targets people without careful consideration of all the facts and punishes them for their supposed infractions without proportionality. Shaming becomes uncivil, moblike, and potentially subversive of the very social order that it tries to protect[188].

Des sondages passés identifient également plusieurs comportements antisociaux dont les internautes craignent d'être victimes à la suite de la divulgation de leurs renseignements personnels : harcèlement[189] (*cyberstalking)*, intimidation[190], menaces[191] ou trollage[192] de la part d'autres internautes.

Une étude du Center for Innovative Public Health Research réalisée en 2016 auprès d'internautes américains concluait par exemple que plus du deux tiers des internautes avaient été témoin de harcèlement et d'intimidation sur Internet et que plus d'un tiers des internautes en avaient déjà été victimes[193]. On y énumère les multiples formes que peuvent prendre ces abus en ligne :

- Harcèlement verbal (insultes)
- Propagation de fausses rumeurs au sujet d'un internaute
- Menaces à l'intégrité physique ou sexuelle d'un internaute
- *Brigading* (encouragement et aide en vue d'amener des tiers à nuire à un internaute)
- Attaques en ligne de type *DoS* (*Denial of Service* – inondation ou perturbation d'un réseau ou d'un compte afin d'en empêcher le fonctionnement pour l'internaute visé)[194]

---

[186] LAIDLAW. « Online Shaming », *supra* note 181, p.7.
[187] SOLOVE, D. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet, Yale University Press, 2007, p.12.
[188] *Ibid.*, p.102.
[189] MOZILLA. « Hackers », *supra* note 153.
[190] OFCOM. « Internet users' experience », *supra* note 147, pp.7-9.
[191] NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION*, supra* note 130, figure 2.
[192] OFCOM. « Internet users' experience », *supra* note 147, pp.7-9.
[193] LENHART, A. *et al*. « Online Harassment, Digital Abuse, and Cyberstalking in America », Center for Innovative Public Health Research, rapport 11.21.16, pp.5 et 23, en ligne : https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf ; À noter qu'un sondage de Pew Research Center arrive à des résultats relativement similaires (41 % de victimes, 66 % de témoin) : DUGGAN, M. « Online harassment 2017 », Pew research Center, 11 juillet 2017, en ligne : https://www.pewinternet.org/2017/07/11/online-harassment-2017/
[194] *Ibid.,* pp.24, 31 et 34.

S'ajoute à cette liste, le phénomène tout récent du *swatting*, soit le signalement (mensonger) d'un crime à l'adresse d'un internaute afin qu'y soit envoyées des forces armées dans le but de lui créer des ennuis, de lui faire peur ou même de le mettre en danger[195].

Enfin, on assiste aussi à une montée des cas de *doxing* (ou *doxxing)*[196] en ligne dans les dernières années. Cette pratique à mi-chemin entre l'atteinte à la réputation et le harcèlement en ligne consiste en la divulgation, sans le consentement, de renseignements personnels concernant un individu (pas nécessairement collectés illégalement), dans le but de lui nuire ou de l'humilier[197]. On pense notamment au dévoilement de l'identité ou des coordonnées de manifestants[198] ou de commentateurs en ligne[199] à des internautes hostiles à ces derniers. La suite n'est que trop prévisible…

2.1.3.4 Risques relatifs à l'intrusion dans le quotidien

Les internautes identifient également des risques pour leur vie privée en ligne qui s'apparentent davantage à des intrusions (non sollicitées, bien sûr) dans leur quotidien[200]. Deux éléments ressortent davantage des sondages réalisés auprès des internautes à ce sujet, soit le pourriel et les décisions automatisées.

Les pourriels

Messages publicitaires, chaines de lettres, propositions de voyantes ou d'« héritages », offres d'affaires bidons, infolettre à laquelle un internaute ne s'est pourtant jamais abonné, etc. : les communications électroniques non sollicitées, dites pourriels ou *spam* en anglais, peuvent prendre de multiples formes[201].

---

[195] TOGNOTTI, C. « What Is "Doxxing" And "Swatting"? You Should Know These Terms & Their Victims », Bustle, 13 février 2015, en ligne : https://www.bustle.com/articles/64275-what-is-doxxing-and-swatting-you-should-know-these-terms-their-victims

[196] Expression qui regroupe le geste de « dropping documents » et le format .docx.

[197] « What doxxing is, and why it matters », The Economist, 10 mars 2014, en ligne : https://www.economist.com/the-economist-explains/2014/03/10/what-doxxing-is-and-why-it-matters ; VIGNEAULT, A. « Qu'est-ce que le doxxing? », La Presse, 30 mars 2019, en ligne : https://www.lapresse.ca/vivre/societe/201903/29/01-5220127-quest-ce-que-le-doxxing.php

[198] Sur le doxing entourant les évènements de Charlottville en 2017 : BOWLES, N. « How 'Doxxing' Became a Mainstream Tool in the Culture Wars », New York Times, 30 août 2017, en ligne : https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html

[199] WILLIAMS, G. « Twitter's alt-right retaliates against CNN journalist at center of so-called blackmail scandal », Vox, 5 juillet 2017, en ligne : https://www.vox.com/policy-and-politics/2017/7/5/15924434/twitter-reddit-alt-right-cnn-andrew-kaczynski ; HERN, A. « Felicia Day's public details put online after she described Gamergate fears », Guardian, 23 octobre 2014, en ligne : https://www.theguardian.com/technology/2014/oct/23/felicia-days-public-details-online-gamergate

[200] ARSHAD, J. « Towards a Taxonomy of Privacy Concerns of Online Social Network Sites Users », 2010, p.34, en ligne : https://pdfs.semanticscholar.org/8484/729358966fa3740d8a6e3d382677f6b8a48d.pdf ;

[201] Au sens la loi canadienne anti-spam, ces communications ont comme fondement d'encourager le récipiendaire à participer à une activité commercial (achat, investissement, etc.) : Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent

La réception de pourriels est couramment identifiée par les internautes comme une atteinte pour leur vie privée en ligne[202]. Ce risque doit être distingué des risques relatifs à la publicité ciblée (section 2.1.2.2). Il ne s'agit pas ici du sentiment dérangeant d'être spécifiquement visé ou « connu » de l'annonceur, mais plutôt de la présence indésirable de messages dans la boite de courriels ou sur les comptes de médias sociaux d'un internaute, dans ce qui peut constituer sa sphère privée et peut être associé à sa « maison » dans l'univers numérique. Notons que le fait de considérer ça comme un risque est étroitement lié aux conceptions de la vie privée qui se concentrent sur la capacité ou la possibilité des individus de s'isoler de la société, de ne pas être dérangés[203].

Car les pourriels sont indéniablement dérangeants. En 2018, environ 14.5 milliards de pourriels étaient envoyés chaque jour dans les boites courriel d'individus et d'entreprises[204]. Même si les filtres développés par les services de messagerie électronique (Gmail, Hotmail, etc.) sont aujourd'hui en mesure de supprimer automatiquement la grande majorité de ces messages[205], la réception de messages électroniques indésirables fait encore partie du quotidien des internautes.

Mais les pourriels sont parfois plus que simplement dérangeants. Ils peuvent même mener à des conséquences financières majeures, aussi importantes que celles qui feraient suite à un vol d'identité par exemple. Ils sont ainsi régulièrement utilisés afin d'hameçonner les consommateurs en ligne. Au moyen de courriels qui semblent provenir d'institutions familières ou respectables, les internautes sont encouragés à consulter des sites en apparence légitimes, mais en réalité frauduleux, sur lesquels ils fourniront des renseignements personnels à leur sujet[206]. Les pourriels sont également occasionnellement utilisés pour transmettre des logiciels malveillants, notamment des rançongiciels qui rendent impossible l'accès aux fichiers ou aux systèmes d'un utilisateur jusqu'à ce qu'il verse une somme d'argent aux responsables de l'attaque[207].

---

l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications, L.C. 2010, ch. 23, art 1(1).

[202] PAINE SCHOFIELD. « Internet users' perceptions », *supra* note 153, p.531, table 1 ; OFCOM. « Internet users' experience », *supra* note 147, pp.7-9 ; ELUEZE, I. et QUAN-HAASE, A. « Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited », American Behavioral Scientist, 2018, vol. 62, no. 10, p.1385.

[203] REJÓN-GUARDIA, F. et MARTÍNEZ-LÓPEZ, F. J. « Online Advertising Intrusiveness and Consumers' Avoidance Behaviors » dans MARTÍNEZ-LÓPEZ, F. J., dir, Handbook of Strategic e-Business Management, Springer Berlin Heidelberg, 2014, p.570 ; PAINE SCHOFIELD. « Internet users' perceptions », *supra* note 153, p.534 ; PODDAR, A., MOSTELLER, J. et ELLEN, P. S. « Consumers' Rules of Engagement in Online Information Exchanges », Journal of Consumer Affairs, vol. 43, no. 3, septembre 2009, p.429.

[204] WIGGERS, K. « Gmail is now blocking 100 million more spam emails a day, thanks to TensorFlow », VentureBeat, 6 février 2019, en ligne : https://venturebeat.com/2019/02/06/gmail-is-now-blocking-100-million-more-spam-emails-a-day-thanks-to-tensorflow/

[205] METZ, C. « Google Says Its AI Catches 99.9 Percent of Gmail Spam », Wired, 9 juillet 2015, en ligne : https://www.wired.com/2015/07/google-says-ai-catches-99-9-percent-gmail-spam/

[206] CANADIAN ANTI-FRAUD CENTER. « Phishing », en ligne: https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/phishing-hameconnage-eng.htm (consulté le 10 avril 2021).

[207] LYNN, S. et THORBECKE, C. « Why ransomware cyberattacks are on the rise », ABC News, 1 juin 2021, en ligne : https://abcnews.go.com/Technology/ransomware-cyberattacks-rise/story?id=77832650

La prise de décisions automatisées ou algorithmiques

Des risques d'intrusion dans la vie privée des individus peuvent également se présenter lorsque des décisions sont prises à leur sujet à partir de renseignements personnels. Plusieurs sondages exposent les préoccupations des internautes à l'égard de la prise de décisions automatisées à leur égard en ligne[208].

L'utilisation d'algorithmes à cet effet a gagné en importance dans les dernières années, notamment en raison du lot toujours croissant de données disponibles[209]. On peut penser par exemple à son utilisation dans le cadre de l'évaluation du risque en matière de crédit ou d'assurance[210]. Mais l'actualité récente fait aussi état d'exemples plus surprenants. La plateforme de location de logements Airbnb aurait par exemple mis au point un outil capable d'identifier les utilisateurs jugés « indignes de confiance », sur la base de la présence de certains traits de personnalité (narcissisme, psychopathie, etc.) que révélerait leur profil virtuel. L'entreprise se livrerait dorénavant à cette évaluation du risque à partir des données disponibles avant de confirmer chaque réservation[211].

Les craintes et critiques par rapport à la prise de décisions algorithmique sont multiples. D'une part, certains internautes craignent des résultats inexacts ou injustes, soit parce que l'analyse inclut des renseignements erronés[212], soit parce les algorithmes utilisés reflètent certains préjugés ou biais[213]. Dans les deux cas, l'absence de transparence au sujet de ce processus décisionnel dérange.

D'autre part, certains voient dans ces décisions automatisées une atteinte à leur dignité humaine. Réduire une personne (dans toute sa complexité) à un chiffre pourrait, selon une étude du Parlement européen, être considéré comme une forme d'aliénation ou de marginalisation[214].

---

[208] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉ DU CANADA. Sondage 2018-2019, *supra* note 158, figure 7 ; MATT. « Sweet Idleness », *supra* note 164, p.173.
[209] BARRETT, L. « Deconstructing Data Mining: Protecting Privacy and Civil Liberties in Automated Decision-Making », Georgetown Law Technology Review, vol. 1, no. 1, 2016, p.154.
[210] *Ibid.,* p.154 ; SWEDLOFF, R. « Risk classification's big data (r)evolution », Connecticut Insurance Law Journal, vol. 21.1, p.340.
[211] HOUSER, K. « Airbnb claims its AI can predict whether guests are psychopaths », The Byte, 4 janvier 2020, en ligne: https://futurism.com/the-byte/airbnb-ai-predict-psychopaths ; BLUNDEN, M. « Booker beware: Airbnb can scan your online life to see if you're a suitable guest », Evening Standard, 10 janvier 2020, en ligne: https://www.standard.co.uk/tech/airbnb-software-scan-online-life-suitable-guest-a4325551.html ; HOLMES, A. « Airbnb has patented software that digs through social media to root out people who display 'narcissism or psychopathy' », Insider, 6 janvier 2020, en ligne: https://www.businessinsider.com/airbnb-software-predicts-if-guests-are-psychopaths-patent-2020-1
[212] MATT. « Sweet Idleness », *supra* note 164, p.173 ; BELLMAN, S. *et al.* « International Differences in Information Privacy Concerns: A Global Survey of Consumers », The Information Society, vol. 20, no. 5, 2004, pp.317-318.
[213] SMITH, A. « Public Attitudes Toward Computer Algorithms », Pew Research Center, novembre 2018, p.8, en ligne : https://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/ ; Sur le sujet du biais des algorithms, voir BAROCAS, S. et SELBST, A. D. « Big Data's Disparate Impact », California Law Review, vol. 104, no. 3, 2016 : «Data is frequently imperfect in ways that allow these algorithms to inherit the prejudices of prior decision makers. In other cases, data may simply reflect the widespread biases that persist in society at large. In still others, data mining can discover surprisingly useful regularities that are really just preexisting patterns of exclusion and inequality ».
[214] PARLEMENT EUROPÉEN. « Understanding algorithmic decision-making: Opportunities and challenges », mars 2019, p.I, en ligne :

2.1.4. Quelques facteurs d'influence

En plus de dresser un portrait général des préoccupations des internautes pour leur vie privée en ligne, la littérature identifie certains éléments d'ordre personnel ou situationnel susceptibles d'influencer lesdites préoccupations. En voici un bref survol.

Soulignons que certaines de ces caractéristiques seront abordées dans le cadre de l'étude des résultats du sondage pancanadien, au chapitre 3. Elles semblent par ailleurs influencer davantage le comportement en ligne des répondants que leurs préoccupations.

2.1.4.1. Des différences selon les caractéristiques personnelles des consommateurs

Les traits de personnalité

Plusieurs chercheurs se sont penchés sur l'influence des traits de personnalité sur le niveau de préoccupation des internautes pour leur vie privée et ont identifié des tendances. Par exemple, les internautes introvertis[215], consciencieux[216], ouverts d'esprit[217], amènes[218], anxieux ou instables émotionnellement[219] seraient plus susceptibles d'être préoccupés par leur vie privée. À noter que les recherches se sont jusqu'ici grandement concentrées sur cette taxonomie des personnalités (le *Big five*)[220].

La conception de la vie privée et la valeur qui lui est accordé

Les différentes conceptions de la vie privée des internautes sont susceptibles d'avoir une influence sur la manière dont ils perçoivent les risques pour leur vie privée en ligne.

Un individu qui partagerait la conception de la vie privée de Warren et Brandeis (droit d'être laissé à soi-même) ou encore de Gavison (accès limité des tiers à soi-même et à son espace

---

http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf ; voir également MATT. « Sweet Idleness », *supra* note 164, p.173.

[215] Dans les situations de commerce en ligne seulement : BANSAL, G *et al*. « Do context and personality matter? Trust and privacy concerns in disclosing private information online », Information & Management, vol. 53, 2016, pp.9-10.

[216] JUNGLAS, I.A., JOHNSON, N.A. and SPITZMÜLLER, C. « Personality traits and concern for privacy: an empirical study in the context of location-based services », European Journal of Information Systems, 2008, vol. 17, no. 4, p.396 ; KORZAAN, M. L. et BOSWELL, K. T. « The influence of personality traits and information privacy concerns on behavioral intentions », Journal of Computer Information Systems, vol. 48, no. 4, p.19 ; OSATUYI, B. « Personality Traits and Information Privacy Concern on Social Media Platforms », Journal of Computer Information Systems, 2015, vol. 55, no. 4, p.16.

[217] JUNGLAS. « Personality Traits », *supra* note 216, pp.393 et 396.

[218] « Agreeableness is a personality trait that reflects social conformity. People with this trait are described as being warm, kind, cooperative, trusting, generous, flexible, considerate, and agreeable » : BANSAL. « Do context and personality matter? », *supra* note 215, pp.5 et 10 ; KORZAAN. « The influence of personality traits », *supra* note 216, p.19 ; OSATUYI. Personality Traits », *supra* note 216, p.16.

[219] BANSAL. « Do context and personality matter? », *supra* note 215, pp.6 et 11.

[220] JUNGLAS. « Personality Traits », *supra* note 216.

privé) pourrait fort bien percevoir la réception de courriels indésirables comme une violation sérieuse de sa vie privée, alors qu'elle en laisserait d'autres relativement indifférents.

De même, un internaute qui partagerait la définition de la vie privée de Posner et Parent (relative au secret des renseignements personnels) serait vraisemblablement très critique de l'utilisation des médias sociaux et de l'ampleur des renseignements qui y circulent. À l'inverse, cette utilisation serait beaucoup plus acceptable pour ceux qui adhèrent davantage aux points de vue de Moore, Westin et cie (relatifs au contrôle), puisqu'un internaute fait en principe le choix de divulguer ou non ses renseignements sur ces plateformes[221].

Il faut aussi considérer le fait que même chez ceux qui partagent une même conception de la vie privée, tous n'accorderont pas la même importance à sa protection, ce qui influencera ultimement leur perception des atteintes potentielles.

> [D]isposition to value privacy [the extent to which a person displays a willingness to preserve his or her private space or to disallow disclosure of personal information to others across a broad spectrum of situations and persons], as a personal characteristics, affects directly the perception of intrusion, and indirectly, through the latter, privacy concerns[222].

Westin a historiquement segmenté les consommateurs en trois grandes catégories selon l'importance qu'ils accordent à leur vie privée[223]. Il y a les internautes « fondamentalistes » (*data fundamentalist*), soit ceux qui refusent de fournir des renseignements personnels même en échange d'un service ou de l'amélioration d'un service. Les internautes « pragmatiques » (*data pragmatic*), eux, sont ouverts au partage de leurs renseignements personnels et évalueront au cas par cas si le service ou l'amélioration du service offert vaut ce qui est demandé. Les internautes « indifférents » (*data unconcerned*), comme leur nom l'indique, ne sont pas intéressés ou interpellés par ces questions.

Quan-Haase et Elueze ont depuis proposé une segmentation révisée qui distingue certaines attitudes en lien avec la protection des renseignements personnels au sein d'une même catégorie d'internautes [224]:

- Les internautes « fondamentalistes » (*data fundamentalist*)
- Les internautes « intensément pragmatiques » (*intense pragmatist*), qui sont dérangés par la divulgation de renseignements personnels en ligne, mais acceptent de faire occasionnellement des compromis lors de l'utilisation d'Internet

---

[221] TREPTE, S. et REINECKE, L. « The Social Web as a Shelter for Privacy and Authentic Living » dans TREPTE, S. et REINECKE, L., dir, Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web, Heidelberg: Springer Berlin Heidelberg, 2011, pp.69-70.
[222] XU, H. *et al.* « Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View », ICIS 2008 Proceedings. Paper 6, p.6.
[223] AXCIOM. « Global data privacy », *supra* note 130, p.6.
[224] ELUEZE. « Privacy Attitudes and Concerns in the Digital Lives of Older Adults », *supra* note 202, pp.1378-1383.

- Les internautes « modérément pragmatiques » (*relaxed pragmatist*), qui sont moins dérangés par la divulgation de renseignements personnels lors de l'utilisation d'un service en ligne et acceptent donc plus facilement de faire des compromis
- Les internautes « cyniques » (*cynical expert*), qui sont d'avis que les atteintes à leur vie privée en ligne sont indépendantes de leur volonté et inévitables
- Les internautes « peu soucieux » (*marginally concerned*), plutôt qu'« indifférents aux données ».

Les antécédents personnels en matière de vie privée

Des études confirment l'influence des antécédents personnels des internautes en matière de vie privée sur leur niveau de préoccupation à cet égard. L'expérience antérieure d'une atteinte à la vie privée entraînerait un plus grand niveau de préoccupation chez un consommateur, en ligne[225] et hors ligne[226].

Le niveau de littératie en matière de vie privée en ligne

La connaissance qu'ont les internautes des pratiques des entreprises en ligne serait également un facteur qui influencerait leur niveau de préoccupation pour la protection de leur vie privée en ligne et pour certains risques. Difficile, par contre, d'identifier une corrélation précise[227].

D'un côté, l'une des préoccupations les plus récurrentes des internautes est justement le manque général de connaissances et la faible compréhension du traitement des renseignements personnels en ligne. De l'autre côté, les auteurs ont noté que la valeur accordée par chacun à sa vie privée en ligne serait influencée positivement par son niveau de littératie sur le sujet[228]. Plus un internaute est conscient des risques, plus il accorde de l'importance à la protection de sa vie privée et est préoccupé par les pratiques de collecte de renseignements personnels en ligne, par les intrusions dans sa vie privée en ligne. Mais parallèlement, un internaute qui n'est pas informé des pratiques des entreprises, mais qui souhaiterait l'être, sera lui aussi, plus inquiet pour sa vie privée en ligne[229].

---

[225] AWAD, N. F. et KRISHNAN, M. S. « The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization », MIS Quarterly, vol. 30, no. 1, 2016, p. 24 ; XU, H. *et al.* « Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services », Information Systems Research, vol. 23, no. 4, 2012, p. 1358 ; YEH, C-H. *et al*. « What drives internet users' willingness to provide personal information? », Online Information Review, vol. 42, no. 6, 2018, p. 931 ; CHO H., RIVERA-SANCHEZ M. et LIM S. S. « A multinational study on online privacy: global concerns and local responses », New Media & Society, vol. 11, no. 3, p.406.
[226] HONG. Drivers and Inhibitors of Internet Privacy Concern », *supra* note 98.
[227] OMRANI, N. et SOULIÉ, N. « Culture, Privacy Conception and Privacy Concern: Evidence from Europe before PRISM », 2017, International Telecommunications Society, p.4.
[228] XU. « Examining the Formation of Individual's Privacy Concerns », *supra* note 222, pp.6-7.
[229] KUO. « Taiwan », *supra* note 133, p.13.

Le genre

Puisqu'il existe des différences dans l'utilisation d'Internet entre les hommes et les femmes, des auteurs se sont intéressés à l'influence du genre sur les préoccupations des internautes relativement à leur vie privée en ligne. Sans être unanime[230], la littérature soutient que de manière générale, les femmes seraient plus préoccupées par leur vie privée en ligne que les hommes[231].

Dans le cadre d'une étude spécifique aux différences de genre en matière de vie privée sur les médias sociaux, Tifferet proposait quelques pistes pour expliquer le niveau de préoccupation supérieur des femmes, dont un niveau généralement supérieur d'anxiété chez ces dernières[232] et une plus grande vulnérabilité face aux menaces à leur vie privée, en ligne et hors ligne (particulièrement celles relatives à leur réputation et leur intégrité physique et psychologique)[233].

L'âge et la génération

Il est reconnu que les membres des différentes générations peuvent présenter des différences considérables quant à leur expérience, leur éducation ou leur socialisation[234], mais qu'en est-il de leur utilisation d'Internet et, plus spécifiquement, de la protection de leur vie privée sur Internet aujourd'hui ?

Selon certains commentaires et éditoriaux, l'utilisation soutenue des médias sociaux par les plus jeunes générations serait un signe du peu de préoccupation qu'elles accordent à la protection de leur vie privée en ligne[235] ; il n'est toutefois pas si certain que ces conclusions soient appuyées par la littérature et les données disponibles. Les quelques

---

230 Voir à ce sujet : LEE, H. *et al*. « Information privacy concerns and demographic characteristics: Data from a Korean media panel survey », Government Information Quarterly, vol. 36, no. 2, 2019, p.296.
231 GRUBBS HOY, M. et MILNE, G. « Gender Differences in Privacy-Related Measures for Young Adult Facebook Users », Journal of Interactive Advertising, vol. 10, no. 2, 2010, p.33 ; BARTEL SHEEHAN, K. « An investigation of gender differences in on-line privacy concerns and resultant behaviors », Journal of Interactive Marketing, vo. 13, no. 4, 1999, pp.30-32 ; FOGEL, J. et NEHMAD, N. « Internet Social Network Communities: Risk Taking, Trust and Privacy Concerns », Computers in Human Behavior, vol. 25, 2009, p.157 ; MOSCARDELLI, D. et DIVINE, R. « Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors », Family and Consumer Sciences Research Journal, vol. 35, no. 3, 2007, p.243 ; WILLS, C. E. and ZELJKOVIC, M. « A personalized approach to web privacy: awareness, attitudes and actions », 2011, p.11, en ligne : http://web.cs.wpi.edu/~cew/papers/imcs11.pdf
232 TIFFERET, S. « Gender differences in privacy tendencies on social network sites: A meta-analysis », Computers in Human Behavior, vol. 93, 2018, p.4
233 *Ibid.*, p.6.
234 OBAL, M. et KUNZ, W. « Trust development in e-services: A cohort analysis of Millennials and Baby Boomers », Journal of Service Management, vol. 24, no. 1, 2013.
235 Voir par exemple : MCCULLAGH, D. « Why no one cares about privacy anymore », Cent, 12 mars 2010, en ligne : https://www.cnet.com/news/why-no-one-cares-about-privacy-anymore/ ; NUSSBAUM, E. « Say Everything », New York Magazine, 2 février 2007, en ligne : http://nymag.com/news/features/27341/ ; Mark Zuckerberg affirmait par exemple en 2010 que la protection de la vie privée n'était plus une norme sociale avec la montée en popularité des médias sociaux : JONHNSON, B. « Privacy no longer a social norm, says Facebook founder », the Guardian, 11 janvier 2010, en ligne : https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

études qui se sont penchées sur le sujet ont en effet obtenu des résultats contradictoires[236].

2.1.4.2. Des différences selon les régions et les cultures

Certains sondages internationaux ont noté des différences considérables dans le niveau de préoccupation des internautes selon leur nationalité ou leur lieu de résidence. À titre d'exemple, les internautes d'Europe de l'Est et d'Europe du Nord seraient généralement moins préoccupés par leur vie privée en ligne que ceux d'Europe centrale[237]. De même, les internautes de pays occidentaux, tels que les États-Unis ou l'Australie, seraient plus préoccupés par leur vie privée en ligne que ceux de pays asiatiques, tels que l'Inde ou la Corée du Sud[238]. Comment expliquer ces différences ?

À partir de la théorie des dimensions culturelles de Hofstede[239], plusieurs études ont noté l'influence particulière de trois dimensions sur les préoccupations des internautes relativement à leur vie privée, à savoir :

- L'individualisme ou le collectivisme d'une société
- L'égalité ou l'inégalité d'une société (« distance hiérarchique »)
- La « masculinité » d'une société

Ainsi, le niveau de préoccupation pour la vie privée en ligne serait généralement plus élevé au sein des sociétés caractérisées par un fort individualisme de ses membres[240]. Contrairement aux membres de sociétés collectivistes, qui adhèrent davantage à un destin, une organisation et des objectifs communs, les internautes issus de sociétés individualistes valoriseraient davantage leur indépendance de la collectivité, d'où un plus grand désir de protéger leur vie privée en ligne et hors ligne[241].

Les membres des sociétés qui accordent davantage d'importance aux « valeurs masculines stéréotypées » afficheraient également un niveau de préoccupation supérieur pour leur vie privée en ligne[242]. Ces valeurs se rapportent de manière générale au matérialisme, à

---

[236] BERGSTRÖM, A. « Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses », Computers in Human Behavior, vol. 53, 2015, p.420.
[237] CECERE, G., LE GUEL, F. et SOULIÉ, N. « Perceived Internet privacy concerns on social networks in Europe », Technological Forecasting and Social Change, vol. 96, 2015, pp. 284.
[238] CHO. « A multinational study », *supra* note 225, pp.404-405.
[239] HOFSTEDE, G. Culture's consequences : Comparing values, behaviors, institutions, and organizations across nations, 2e ed, Sage Publications, 2001.
[240] CHO. « A multinational study », *supra* note 225, p.411 ; MILTGEN C. L. et GUILLARD, D. P. « Cultural and generational influences on privacy concerns: a qualitative study in seven European countries », European Journal of Information Systems, vol. 23, 2014, p.21 *a contrario.* Il est à noter que Cecere *at al.* arrivent à un résultat different sur le sujet : CECERE. « Perceived Internet privacy concerns », *supra* note 237, p.284.
[241] HUANG, H-Y. et BASHIR, M. « Privacy by region: Evaluation online users' privacy perceptions by geographical region », 2016, p.974 ; CHO. « A multinational study », *supra* note 225, p.411.
[242] CECERE. « Perceived Internet privacy concerns », *supra* note 237, p.284.

l'ambition et à la compétitivité (par opposition aux valeurs féminines stéréotypes davantage centrées sur les relations humaines)[243].

Similairement, les membres d'une société dans laquelle le pouvoir est distribué de manière inégale seraient davantage préoccupés par leur vie privée en ligne[244]. On noterait un plus grand sentiment de méfiance envers les autres au sein de telles sociétés, ce qui pourrait expliquer encore une fois un désir plus grand de protéger sa vie privée[245].

Quelques études offrent tout de même des nuances additionnelles sur le sujet. Une étude de Bellman *et al*. concluait par exemple à l'influence des différences culturelles sur certaines préoccupations des internautes seulement (ex. : erreurs dans les bases de données) et non de manière généralisée[246]. La mondialisation et le développement des diasporas pourraient également réduire l'exactitude de ce genre d'analyse, selon Cho, Rivera-Sanchez et Lim[247].

Enfin, on note également des différences selon le lieu de résidence en raison de l'état de la réglementation en matière de vie privée. De manière générale, les internautes les plus préoccupés par leur vie privée en ligne proviennent d'États dont la réglementation est dite « modérée ». Les internautes qui proviennent d'un État qui intervient beaucoup sur les pratiques des entreprises en matière de vie privée seront moins préoccupés, vraisemblablement parce que les pratiques les plus répréhensibles y sont interdites et adéquatement réprimées. Mais les internautes issus d'États où il n'y a pas ou très peu de réglementation en la matière seront également moins préoccupés par leur vie privée en ligne[248]. Difficile dans ce cas-là de déterminer si l'inaction du législateur local découle du peu d'intérêt de l'opinion publique ou si c'est plutôt l'inverse…

2.1.4.3. Des différences selon les circonstances

Le niveau de préoccupation des internautes relativement à la protection de leur vie privée en ligne variera également de manière ponctuelle, selon les circonstances spécifiques dans lesquelles ils se trouvent.

Ainsi, la nature des renseignements personnels demandés à ou obtenus d'un internaute en ligne influencera son niveau de préoccupation pour sa vie privée au même moment. Les renseignements personnels qui peuvent être collectés en ligne se classent en trois catégories : les renseignements publics, privés et sensibles. Les renseignements

---

[243] OMRANI. « Culture, Privacy Conception and Privacy Concern», *supra* note 227, p.5 ; HOFSTEDE, G. « The 6-D model of national culture », en ligne : https://geerthofstede.com/culture-geert-hofstede-gert-jan-hofstede/6d-model-of-national-culture/ (consulté le 28 mars 2021).
[244] CECERE. « Perceived Internet privacy concerns », *supra* note 237, p.284 ; OMRANI. « Culture, Privacy Conception and Privacy Concern», *supra* note 227, p.12.
[245] CECERE. « Perceived Internet privacy concerns », *supra* note 237, p.278.
[246] BELLMAN. « International Differences », supra note 212, p.320.
[247] CHO. « A multinational study », *supra* note 225, p.411.
[248] MILBERG, S. J. *et al.* « Values, personal information privacy, and regulatory approaches », communications of the ACM, vol. 38, no. 12, 1995, p.72.

personnels dits sensibles représentent une catégorie restreinte de renseignements privés, en ce que leur divulgation est particulièrement susceptible de nuire à l'internaute sur les plans financiers ou sociaux[249].

Plus un renseignement est jugé sensible, plus sa collecte ou son utilisation éventuelle en ligne serait propre à augmenter le niveau général de préoccupation d'un internaute pour la protection de sa vie privée en ligne[250].

Il est à noter que, bien que certaines lois énumèrent ou définissent les renseignements qui seront qualifiés de sensibles[251], il n'existe pas de consensus généralisé sur les caractéristiques qui feraient en sorte qu'un renseignement personnel qui les possède serait systématiquement considéré comme étant un renseignement sensible[252]. L'évaluation de la « sensibilité » d'un renseignement pourrait donc varier d'un internaute à un autre. Nous y reviendrons dans le cadre de l'analyse des résultats de notre sondage pancanadien.

En plus de la nature des renseignements visés, l'entité qui est à l'origine de cette demande de consentement à la collecte ou à l'utilisation des données influence le niveau de préoccupation des internautes[253]. Par exemple, la réputation d'un site Web (expertise en matière de produits et services, etc.) et le sentiment de familiarité de l'internaute réduisent son niveau de préoccupation[254]. Et le type de sites Web impliqués influence également. De manière générale, la divulgation de renseignements personnels auprès d'un site Web transactionnel provoquera davantage d'inquiétude que celle faite auprès d'un site Web relationnel (médias sociaux)[255].

À partir des résultats du sondage mené dans le cadre de cette recherche, nous constatons qu'il y aurait aussi des différences dans le niveau de préoccupation et possiblement dans les types de préoccupations spécifiques des internautes selon le mode ou l'outil de connexion à Internet utilisé (ordinateurs, téléphones mobiles, objets connectés, etc.). La littérature n'offre que très peu de détails ou de précisions sur le sujet.

---

249 BANSAL. « Do context and personality matter? », *supra* note 215, p.3.
250 HONG. Drivers and Inhibitors of Internet Privacy Concern », *supra* note 98 ; KAYHAN, V. O. et DAVIS, C. J. « Situational Privacy Concerns and Antecedent Factors », Journal of Computer Information Systems, vol. 56, no. 3, 2016, p.233.
251 Voir par exemple : LPRPDE, supra note 76, annexe 1, art 4.3.4.
252 WIRTH, J. *et al*. « Perceived information sensitivity and interdependent privacy protection: A quantitative study », Electronic Markets, vol. 29, no. 3, 2019, p.362.
253 KAYHAN. « Situational Privacy Concerns », *supra* note 250, p.229.
254 LI, Y. « The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decision Support Systems », Decision Support Systems, 2013, p.350.
255 TANG, J-H. et LIN, Y-J. « Websites, Data Types and Information Privacy Concerns: A Contingency Model », Telematics and Informatics, vol. 34, 2017, p.1279.

2.2. Portrait des mesures de protection de la vie privée en ligne disponibles aux consommateurs

Les sondages réalisés auprès des internautes permettent d'identifier plusieurs des comportements ou mesures qu'ils favorisent afin de protéger leur vie privée en ligne[256]. S'ajoutent à cela les conseils fournis par des experts ou des médias. La présente section se veut un survol des principaux comportements et mesures que peut adopter un internaute qui désire protéger davantage sa vie privée, et ce, en fonction des différents risques identifiés précédemment. Signalons qu'il ne s'agit pas ici d'une étude technique sur l'efficacité réelle des mesures de protection potentiellement employées par les internautes.

Il est possible de distinguer les mesures de protection de la vie privée en deux grandes catégories : les mesures passives et les mesures actives[257]. On qualifie de passives les mesures qui consistent à éviter ou à réduire des utilisations possibles d'Internet. L'internaute tente ainsi d'échapper à des atteintes à sa vie privée en ligne en rejetant les situations ou les activités les plus à risque ou plus drastiquement encore, en se retirant tout simplement du réseau Internet. Les mesures dites actives, qui sont davantage d'ordre technique[258], concernent pour leur part des comportements d'autoprotection adoptés par les internautes dans le cadre de leur utilisation (continue) d'Internet.

2.2.1. Mesures passives de protection de la vie privée en ligne

2.2.1.1. Réduction de l'utilisation d'Internet

On comptait quelque 4,44 milliards d'internautes dans le monde en 2019[259]. Le plus draconien des comportements que pourraient adopter ces derniers en vue de protéger davantage leur vie privée serait de mettre entièrement fin à leur utilisation d'Internet. Bien entendu, ce comportement n'est pas des plus populaires ! Et de nos jours, il est même

---

[256] CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION. « Global Survey », *supra* note 101, partie I et II, p.55 ; MADDEN, M. et RAINIE, L. « Americans' Attitudes About Privacy, Security and Surveillance », Pew Research Center, 20 mai 2015, pp.33-34, en ligne : https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ ; MADDEN, M. et RAINIE, L. Anonymity, Privacy, and Security Online, Pew research Center, septembre 2013, en ligne : https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online ; NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *supra* note 130 ; MALWAREBYTES LABS. « Labs survey finds privacy concerns, distrust of social media rampant with all age groups », 5 mars 2019, en ligne : https://blog.malwarebytes.com/security-world/2019/03/labs-survey-finds-privacy-concerns-distrust-of-social-media-rampant-with-all-age-groups/

[257] BARTH, S. « The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review », Telematics and Informatics, vol. 34, no. 7, 2017.

[258] Park distingue d'ailleurs entre comportements techniques et sociaux plutôt que passifs et actifs : PARK, Y. J. « Digital literacy and privacy behavior online », Communication Research, vol. 40, no. 2, 2013, pp.222 et 226.

[259] MORGAN, S. « Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion », CyberSecurityVentures, 18 juillet 2019, en ligne : https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/

difficile de l'envisager. « Disconnection and remaining in society are mutually incompatible » : voilà comment l'exposait un expert consulté par le Pew Research Center[260].

Malgré tout, notons qu'il existe effectivement un mouvement vers la déconnexion temporaire d'Internet (ou plus spécifiquement des médias sociaux) parfois qualifiée de « digital detox[261] ». Cette pratique semble toutefois prendre sa source dans des considérations relatives à la santé des individus (dépendance, stress, posture, capacité d'attention, *fear of missing out*, insomnie, etc.)[262] et non à la protection de la vie privée.

Si la déconnexion volontaire à Internet demeure marginale, nous notons tout de même quelques illustrations concrètes.

Certains consommateurs font par exemple le choix d'acheter des modèles plus anciens de téléphones cellulaires ou des modèles plus récents, mais qui ne sont pas « intelligents », afin d'éviter la connexion à Internet et de limiter ainsi la collecte de renseignements à leur sujet par cette voie[263]. Un média britannique notait une augmentation plus importante de la vente de téléphones qui ne peuvent se connecter à Internet que de téléphones intelligents, en 2018[264].

Certains internautes évitent également d'accéder à Internet au moyen d'une connexion Wi-Fi publique, étant donné la sécurité réduite que ce type de connexion présente pour les renseignements personnels qui circulent par ce biais[265] (vu l'absence de chiffrement sur la plupart des points d'accès public[266]). Il existerait en effet des risques qu'un appareil qui se connecte à un réseau non sécurisé soit piraté ou détourné par la mise en place de points d'accès fictifs[267].

---

[260] RAINIE, L. et ANDERSON, J. « Theme 2: Unplugging isn't easy now, and by 2026 it will be even tougher», Pew Research Center, 6 juin 2017, en ligne : https://www.pewresearch.org/internet/2017/06/06/theme-2-unplugging-isnt-easy-now-and-by-2026-it-will-be-even-tougher/

[261] CHEN, B. X. « It's Time for a Digital Detox. (You Know You Need It.)», New York Times, 25 novembre 2020, en ligne : https://www.nytimes.com/2020/11/25/technology/personaltech/digital-detox.html

[262] FOX, M. « 8 Reasons Why You Should Unplug One Day A Week », Forbes, 24 septembre 2019, en ligne: https://www.forbes.com/sites/meimeifox/2019/09/24/8-reasons-why-you-should-unplug-one-day-a-week/?sh=75aa3b3b1b79 ; « The benefits of unplugging from electronics », Adventist Health, 14 mars 2019, en ligne: https://www.adventisthealth.org/blog/2019/march/the-benefits-of-unplugging-from-electronics/ ;

[263] VOINIGESCU, E. « Basic ways to help protect your personal data online », 11 avril 2019, en ligne : https://www.cbc.ca/life/culture/basic-ways-to-help-protect-your-personal-data-online-1.5094766 ; BOGOST, I. « The Wisdom of Nokia's Dumbphone », The Atlantic, 28 février 2017, en ligne : https://www.theatlantic.com/technology/archive/2017/02/the-wisdom-of-the-dumbphone/518055/

[264] HOSIE, R. « 'Dumbphone' sales rise as people seek to disconnect and be more mindful », the Independent, 20 août 2018, en ligne : https://www.independent.co.uk/life-style/dumb-phones-sales-rise-disconnect-technology-mindfulness-social-media-a8499086.html

[265] NIELD, D. « Simple Steps to Protect Yourself on Public Wi-Fi », Wired, 5 août 2018, en ligne : https://www.wired.com/story/public-wifi-safety-tips/

[266] FEDERAL TRADE COMMISSION. « Tips for Using Public Wi-Fi Networks », mars 2014, en ligne : https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks

[267] PIERCE, D. « Public Wi-Fi Is Safer Than Ever—But You Still Need to Be Careful », Wall Street Journal, 4 août 2019, en ligne : https://www.wsj.com/articles/public-wi-fi-is-safer-than-everbut-you-still-need-to-be-careful-11564923600

2.2.1.2. Réduction des activités de consommation en ligne

Sans renoncer entièrement à utiliser Internet ou certains de ses modes d'accès, des internautes choisissent de limiter leurs activités de consommation et les transactions qu'ils effectuent en ligne. Par exemple, 15 % des Canadiens ne font pas d'achats en ligne et un peu moins du tiers ne communiquent pas avec leur banque via Internet, selon les données les plus récentes de l'ACEI[268]. Précisons par ailleurs que, comme c'était le cas pour les mouvements de déconnexion temporaire d'Internet, les études ne démontrent pas que les considérations relatives à la protection de la vie privée soient déterminantes dans le choix de certains de ne pas participer au commerce électronique (les difficultés d'utilisation et le manque d'intérêt pour les biens et services offerts le seraient davantage)[269].

Le choix des sites Web sur lesquelles les consommateurs vont effectivement faire des achats et autres transactions semble, lui, davantage influencé par ces considérations. Sur recommandations des experts, plusieurs consommateurs ont uniquement recours à des sites ou plateformes chiffrés afin de réduire les risques de piratage des renseignements personnels qu'ils fourniront[270]. L'adresse Web de ces sites sera précédée de la dénomination *HTTPS*, soit une extension sécurisée du protocole *HTTP,* et un symbole de cadenas ou de clé se trouvera à proximité de ladite adresse.

2.2.1.3. La réduction de la divulgation de renseignements personnels en ligne

Au-delà de la minimisation des gestes de consommation, qui vise principalement la protection des renseignements personnels d'ordre financier, les consommateurs peuvent adopter une variété de mesures afin de réduire la diffusion en ligne d'autres types de renseignements qui les concernent.

Sans grande surprise, ce sont, cette fois-ci, les médias sociaux qui sont particulièrement visés, allant de l'utilisation de faux noms lors de l'enregistrement[271] jusqu'à la fermeture complète des comptes sur ces plateformes[272]. De manière plus générale, plusieurs

---

[268] ACEI. « Dossier documentaire sur Internet au Canada 2020 », 2020, en ligne : https://www.cira.ca/fr/resources/dossier-documentaire/dossier-documentaire-sur-internet-au-canada-2020

[269] Voir par exemple : MOHAMMED, Z. A., et TEJAY, G. P. « Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology », Computers & Security, vol. 67, 2017, p.267 (hypothèses 3(b) et 3(c) rejetées) ; MCCLOSKEY, D. « Evaluating Electronic Commerce Acceptance with the Technology Acceptance Model », Journal of Computer Information Systems, vol. 44, no. 2, 2004, p.53.

[270] FEDERAL TRADE COMMISSION. « Computer Security », juin 2017, en ligne : https://www.consumer.ftc.gov/articles/0009-computer-security ; SILVER, J. « 20 ways to keep your internet identity safe from hackers », The Guardian, 12 mai 2013, en ligne : https://www.theguardian.com/technology/2013/may/12/20-ways-keep-internet-identity-safe ; ÉDUCALOI. « Achats en ligne: 6 précautions à prendre », en ligne : https://www.educaloi.qc.ca/capsules/achats-en-ligne-6-precautions-prendre (consulté le 14 septembre 2021).

[271] O'REILLY, D. « Enhance privacy by being deliberately inaccurate », CNET, 10 octobre 2013, en ligne : https://www.cnet.com/how-to/enhance-privacy-by-being-deliberately-inaccurate/

[272] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Utilisation sécuritaire des médias sociaux », 1er août 2019, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-

consommateurs choisissent de réduire la quantité de renseignements personnels qu'ils diffusent quotidiennement à leurs abonnés sur ces plateformes. Comme le rappelle la FTC, certains renseignements en apparence banals peuvent ultimement servir à des fraudeurs qui tenteraient de voler l'identité de la personne[273].

Certaines pratiques de diffusion de renseignements inexacts sur les médias sociaux sont particulièrement élaborées. Le site Web *Fakenamegenerator.com* propose par exemple, gratuitement, la création d'une identité fictive complète. Nom, adresse, date de naissance, signe astrologique, nom de la mère, voiture préférée, groupe sanguin, employeur, adresse courriel, etc. : tout y est… et tout est faux, mais plausible ! Pour le numéro de téléphone, il est recommandé de fournir des numéros utilisés dans des films et séries, qui ont alors très peu de chance d'être réellement en service[274].

D'autres choisissent plutôt de « noyer » leurs renseignements personnels réels en ajoutant des passe-temps ou préférences inexacts sur leur compte ou en s'abonnant à des pages ou des comptes de personnalités ou d'entreprises qui ne correspondent pas à leurs intérêts réels. « The trick is to populate your Facebook with just enough lies as to destroy the value and compromise Facebook's ability to sell you", rapporte Forbes[275].

Enfin, il est recommandé d'éviter de se connecter directement à d'autres services au moyen d'un compte de média social[276]. Cette manière de faire, appelée le *social login*, simplifie certes la vie de l'internaute en lui évitant de devoir remplir des formulaires et de mémoriser des mots de passe, mais elle n'est pas sans conséquence. Elle permet aux entreprises auprès desquelles l'individu se connecte d'avoir accès à son profil et conséquemment à davantage de renseignements personnels – sur ses centres d'intérêt, préférences et affiliations politiques et religieuses, par exemple – qu'il n'en aurait fournis en s'inscrivant manuellement.

2.2.1.4. La non-consultation de certains contenus

Face aux risques d'être victime d'un virus informatique et de voir son ordinateur, sa tablette ou son téléphone intelligent compromis et les renseignements personnels qui s'y trouvent piratés, de nombreux consommateurs se montrent prudents quant aux contenus qu'ils consultent. Ils renoncent à explorer certains sites Web ou à utiliser des applications qui

privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/protection-de-la-vie-privee-en-ligne/medias-sociaux/02_05_d_74_sn/#s09

[273] FEDERAL TRADE COMMISSION. « How to Keep Your Personal Information Secure », juillet 2012, en ligne : https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

[274] HOPPING, C. et IRVINE, R. « How to stay anonymous online », IT Pro, 9 août 2018, en ligne : https://www.itpro.co.uk/privacy/30584/how-to-stay-anonymous-online

[275] HILL, K. « Fooling Facebook: Telling Lies To Protect Your Privacy », Forbes, 7 septembre 2012, en ligne : https://www.forbes.com/sites/kashmirhill/2012/09/07/fooling-facebook-telling-lies-to-protect-your-privacy/#49622531158b

[276] DREBES, L. « How Social Login Is Changing Business--and Your Privacy », Forbes, 28 février 2012, en ligne : https://www.forbes.com/sites/forbesleadershipforum/2012/02/28/how-social-login-is-changing-business-and-your-privacy/#43497a2d7485 ; MATSAKIS, L. « The Security Risks of Logging in With Facebook », Wired, 19 avril 2018, en ligne : https://www.wired.com/story/security-risks-of-logging-in-with-facebook/

leur semblent moins sécuritaires[277] et évitent d'ouvrir des courriels de destinateurs inconnus ou encore d'ouvrir les hyperliens qu'ils comportent[278].

2.2.2. Mesures actives de protection de la vie privée en ligne

2.2.2.1. Utilisation d'un logiciel antivirus et mise en place d'un pare-feu

Parmi les mesures actives de protection de la sécurité des appareils connectés et de la protection de la vie privée en ligne que peut prendre un internaute, on compte bien sur l'utilisation d'un antivirus et d'un pare-feu sur les ordinateurs, tablettes et téléphones intelligents. Nous verrons plus loin qu'il s'agit d'un outil de protection très prisé des consommateurs canadiens.

Un antivirus est un logiciel qui peut détecter, supprimer ou prendre d'autres mesures pour contrer l'action des fichiers logiciels malveillants (*malwares*), tels que les virus informatiques, les chevaux de Troie et les vers informatiques (*worms*)[279]. Un pare-feu, quant à lui, filtre le trafic provenant de l'extérieur et protège un système informatique contre des menaces externes uniquement. Un pare-feu peut ainsi empêcher un pirate informatique d'accéder à un appareil et de l'utiliser à l'insu de son propriétaire[280]. Notons que la plupart des antivirus comprennent un pare-feu. De même, les systèmes d'exploitation Microsoft et Mac OS possèdent des pare-feu intégrés.

Signalons malheureusement que l'utilisation d'un antivirus peut parfois entraîner, paradoxalement, des atteintes à la vie privée de ses utilisateurs, du fait du fournisseur de l'outil lui-même ! L'antivirus gratuit AVG (Avast), qui compte quelque 400 millions d'utilisateurs, a ainsi fait les manchettes dans les dernières années en reconnaissant qu'il vendait l'historique de navigation et de recherche de ses utilisateurs à des tiers[281]. Il est normal qu'un antivirus surveille le trafic Internet d'un usager en vue d'identifier et bloquer des intrusions informatiques potentielles ; le fait qu'il vende ensuite ces données à des entreprises telles que L'Oréal, Home Depot et Pepsi l'est considérablement moins[282] !

---

[277] Voir à ce sujet : MEDIATI, N. « The 17 Most Dangerous Places on the Web », PCWorld, 26 septembre 2010, en ligne : https://www.pcworld.com/article/206107/most_dangerous_places_on_the_web.html
[278] Voir par exemple : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Protection des renseignements personnels en ligne », août 2018, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/protection-de-la-vie-privee-en-ligne/protection-des-renseignements-personnels-en-ligne/
[279] DÉPARTEMENT DE LA JUSTICE (ÉTAT DE LA CALIFORNIE). « Protect Your Computer From Viruses, Hackers, and Spies », en ligne : https://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer (consulté le 15 juillet 2021).
[280] *Ibid.*
[281] TAYLOR, S. « Is Your Antivirus Software Spying on You? », Restore Privacy, 4 février 2019, en ligne : https://restoreprivacy.com/antivirus-privacy/ ; TEMPERTON, J. « AVG can sell your browsing and search history to advertisers », Wired UK, 18 septembre 2015, en ligne : https://www.wired.co.uk/article/avg-privacy-policy-browser-search-data ; MIHALCIK, C. « Antivirus firm Avast is reportedly selling users' web browsing data », CNET, 27 janvier 2020, en ligne : https://www.cnet.com/news/antivirus-firm-avast-is-reportedly-selling-users-web-browsing-data/
[282] COX, J. « Leaked Documents Expose the Secretive Market for Your Web Browsing Data », Vice, 27 janvier 2020, en ligne : https://www.vice.com/en_us/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation

2.2.2.2. Mise à jour des logiciels

Il est également recommandé de mettre à jour régulièrement - manuellement ou automatiquement lorsque possible - les logiciels et systèmes d'exploitation de ses appareils. Ces mises à jour servent bien souvent à remédier à une faille ou vulnérabilité du système qui pourrait être exploitée par un pirate informatique et qui a été découverte ou signalée à l'entreprise[283]. Selon un article du New York Times, « these security updates are typically far better at thwarting hackers than antivirus software[284]. »

2.2.2.3. Personnalisation des paramètres de confidentialité (privacy settings)

De même, il est recommandé d'adapter les paramètres de confidentialité des différentes composantes impliquées dans l'utilisation d'Internet (systèmes d'exploitation des appareils de connexion, objets connectés, navigateurs, applications, pare-feu, service d'infonuagique, etc.) afin de s'assurer de l'application des normes de protection maximale disponibles[285]. Le Commissariat à la protection de la vie privée du Canada recommande d'ailleurs de procéder régulièrement à une révision des paramètres sélectionnés[286].

Le resserrement des paramètres par défaut est également d'intérêt lorsqu'il est question des médias sociaux, où l'accès du public aux publications peut notamment être modifié ou adapté au choix de l'utilisateur[287].

2.2.2.4. Suppression de l'historique de navigation et des témoins

Lorsqu'un individu surfe sur Internet, son navigateur stocke généralement bon nombre de données, telles que le lieu de connexion, les sites Web consultés et les mots de passe et autres renseignements entrés sur ces sites. Il est recommandé de supprimer régulièrement l'historique de navigation, le cache (un système de mémoire temporaire qui facilite

---

[283] GOSAFEONLINE (SINGAPORE GOVERNMENT AGENCY). « Cyber Tip - Update Your Software Promptly », 4 septembre 2019, en ligne : https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/update-software-asap ; IDENTITY THEFT RESSOURCE CENTER. « What are security patches and why are they important? », 17 juin 2012, en ligne : https://www.idtheftcenter.org/what-are-security-patches-and-why-are-they-important/

[284] KLOSOWSKI, T. « How to Protect Your Digital Privacy, Privacy Project », New York Times, en ligne : https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

[285] *Ibid.* ; HODGE, R. « Browser privacy settings you need to change right away: Chrome, Firefox and more », CNET, 6 juin 2021, en ligne: https://www.cnet.com/tech/services-and-software/browser-privacy-settings-you-need-to-change-right-away-chrome-firefox-and-more/ ; OSBORNE, C. et WHITTAKER, Z. « Cybersecurity 101: Protect your privacy from hackers, spies, and the government », ZDNet, 8 décembre 2020, en ligne: https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/ ; GERMAIN, T. « How to Use Google Privacy Settings », Consumer Reports, 11 juin 2021, en ligne : https://www.consumerreports.org/privacy/how-to-use-google-privacy-settings/

[286] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Conseils pour utiliser les paramètres de confidentialité », mars 2019, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/protection-de-la-vie-privee-en-ligne/gd_ps_201903/

[287] STERN, T. et KUMAR, N. « Improving privacy settings control in online social networks with a wheel interface », Journal of the Association for Information Science and Technology, vol. 65, no. 3, 2014, p.525 ; GERMAIN. « How to Use Facebook Privacy Settings », *supra* note 285.

l'affichage de pages Web préalablement consultées) et les témoins de navigation de ses différents appareils.

Notons par ailleurs que le suivi des internautes demeure possible malgré la suppression des témoins de navigation, notamment par l'utilisation de techniques d'empreinte digitale d'appareils (ex. : *canvas fingerprinting*)[288]. Ces techniques ont d'ailleurs été développées en réponse au rejet de plus en plus fréquent des témoins par les internautes et de l'imprécision desdits témoins[289].

2.2.2.5. Variété des mots de passe utilisés et changement régulier

La majorité des internautes réutilisent les mêmes mots de passe pour plusieurs comptes ou utilisent des mots de passe jugés « faibles » ou peu sécuritaires[290]. Selon une analyse réalisée par NordPass de centaines de milliers de mots de passe d'internautes, le mot de passe le plus courant demeure encore aujourd'hui « 123456 »[291]. Le mot de passe « password » (« mot de passe » en anglais) figure également parmi les favoris.

L'utilisation de mots de passe simples et prévisibles expose les internautes au risque de voir leur compte (facilement) piraté et les données personnelles qui s'y trouvent volées et utilisées à leur insu. L'adoption du même mot de passe pour plusieurs comptes amplifie à son tour ce risque, étant donné les cyberattaques de type *credential stuffing.* Celles-ci consistent à faire des demandes de connexion à large échelle sur le Web après avoir obtenu l'identifiant de connexion et le mot de passe d'un compte d'un individu en ligne. Si l'individu réutilise lesdits identifiant et mot de passe, ces autres comptes seront possiblement à leur tour compromis[292].

---

[288] TANNER, A. « The creepier web tracking technology that will replace cookies », Globe & Mail, 18 juin 2013, en ligne : https://www.theglobeandmail.com/technology/business-technology/the-creepier-web-tracking-technology-that-will-replace-cookies/article12632904/
[289] *Ibid.*
[290] Voir à ce sujet : WASH, R. *et al.* « Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites », Symposium on Usable Privacy and Security, 12e ed, 2016, en ligne : https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-wash.pdf
[291] HO, S. « If your password is on this list, you should change it », CTV News, 18 novembre 2020, en ligne : https://www.ctvnews.ca/sci-tech/if-your-password-is-on-this-list-you-should-change-it-1.5193720
[292] *Ibid.* ; MUELLER, N. « Credential stuffing, Open Web Application Security Project », en ligne : https://owasp.org/www-community/attacks/Credential_stuffing# (consulté le 15 juin 2021).

En plus de recommander la sélection d'un mot de passe complexe distinct pour chaque compte[293], certains experts encouragent la mise à jour régulière des mots de passe[294]. Notons que cette dernière proposition ne fait toutefois pas l'unanimité puisque des voix s'élèvent depuis quelques années en opposition au changement de mot de passe à moins qu'il ne soit compromis[295]. Les internautes seraient en effet portés à opter pour des mots de passe moins sécuritaires après quelques changements, faute d'idées.

Le recours à un gestionnaire de mots de passe

Plusieurs internautes ont recours à des gestionnaires de mots de passe afin d'assurer la diversification et la complexité de leurs mots de passe[296]. Ces outils peuvent générer de multiples mots de passe sécuritaires (combinaisons de chiffres, lettres et symboles) pour l'internaute et les conserver en un seul et même endroit. Un internaute aura donc un seul mot de passe à retenir, celui de l'application, dont l'accès est par ailleurs chiffré. Certains gestionnaires offrent aussi le changement automatique de mots de passe sur certains sites après une période prédéterminée[297]. En 2019, les quatre gestionnaires de mots de passe les plus populaires, 1Password, Dashlane, KeePass et LastPass, comptaient quelque 61,5 millions d'utilisateurs individuels dans le monde[298].

Si l'utilisation de ces outils est généralement recommandée par les experts, elle n'est pas entièrement sans risque ; si le mot de passe de l'application est compromis, alors tous les mots de passe de l'utilisateur le sont également ! Et plusieurs études, dont une parue en

---

[293] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Renforcez votre vie privée : Utilisez des mots de passe forts », 29 juillet 2019, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/protection-de-la-vie-privee-en-ligne/video_pw/ ; LORD, N. « 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2019 », Digital Guardian, 15 juillet 2019, en ligne : https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe ; ELLIOTT, M. « 7 common security mistakes you're probably making », CNET, 9 juillet 2017, en ligne : https://www.cnet.com/how-to/online-security-mistakes-youre-probably-making/ ; POLK, R. « The Lazy Person's Guide to Better Online Privacy », Internet Society, 28 janvier 2018, en ligne : https://www.internetsociety.org/blog/2018/01/lazy-persons-guide-better-online-privacy/

[294] FOWLER, B. « Tips for Better Passwords », Consumer Report, 2 mai 2019, en ligne : https://www.consumerreports.org/digital-security/tips-for-better-passwords/ ; COMMISSION D'ACCÈS À L'INFORMATION. « Le courrier électronique », en ligne : http://www.cai.gouv.qc.ca/documents/CAI_FI_courrier_electronique.pdf (consulté le 15 juin 2021).

[295] EVANS, J. « Password expiration is dead, long live your passwords », Techncrunch, 2 juin 2019, en ligne : https://techcrunch.com/2019/06/02/password-expiration-is-dead-long-live-your-passwords/ ; CRANOR, L. « Time to rethink mandatory password changes », FTC, 2 mars 2016, en ligne ; https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes ; HOFFMAN, C. « Should You Change Your Passwords Regularly? », How-to-Geek, 22 septembre 2016, en ligne : https://www.howtogeek.com/187645/htg-explains-should-you-regularly-change-your-passwords/

[296] CHAIKIVSKY, A. « Everything You Need to Know About Password Managers », Consumer Report, 7 février 2017, en ligne : https://www.consumerreports.org/digital-security/everything-you-need-to-know-about-password-managers/

[297] *Ibid.*

[298] À noter que cette statistique ne tient pas des entreprises qui utilisent ces gestionnaires de mots de passe. ISE. « Password Managers: Under the Hood of Secrets Management », 19 février 2019, en ligne : https://www.ise.io/casestudies/password-manager-hacking/

2020 et produite par des chercheurs de l'Université de York, ont justement constaté une série de failles de sécurité susceptibles d'être exploitées par des pirates informatiques, notamment chez les applications de ce type destinées au système d'exploitation Windows 10 et aux téléphones intelligents[299]. Notons tout de même qu'après avoir été avisés par les chercheurs impliqués, plusieurs gestionnaires de mots de passe auraient corrigé rapidement certains des problèmes constatés[300].

2.2.2.6. Recours à la double authentification

Une autre mesure de protection de la sécurité des appareils et des comptes en ligne, et indirectement de la vie privée des internautes, concerne la mise en place d'une double authentification ou d'une vérification de l'identité en deux étapes (*two-factor authentication,* dit *2FA*). Cette mesure a notamment été mise de l'avant par la Maison-Blanche en 2016 dans le cadre d'une campagne de sensibilisation des Américains à la cybersécurité[301].

Cette mesure est complémentaire à la sélection et à la mise à jour d'un mot de passe sécuritaire, en ce qu'elle ajoute un niveau de sécurité lors de l'accès à un appareil ou un compte en ligne[302]. Après avoir entré correctement son mot de passe, l'internaute devra valider son identité au moyen d'un second « facteur d'authentification ». Il existe trois types de facteurs possibles[303] :

- Les facteurs de connaissance (ex. : question de sécurité)
- Les facteurs de possession (ex. : code de sécurité reçu par SMS sur un appareil mobile, clé de sécurité)
- Les facteurs héréditaires (ex. : empreinte digitale, reconnaissance faciale)

---

[299] UNIVERSITY OF YORK. « Researchers expose vulnerabilities of password managers », 16 mars 2020, en ligne : https://www.york.ac.uk/news-and-events/news/2020/research/expose-vulnerabilities-password-managers/
[300] OWAIDA, A. « Security flaws found in popular password managers », We live security – ESET, 19 mars 2020, en ligne: https://www.welivesecurity.com/2020/03/19/security-flaws-found-in-popular-password-managers/
[301] WHITE HOUSE - OFFICE OF THE PRESS SECRETARY. « Fact sheet: Cybersecurity National Action Plan », 9 février 2016, en ligne : https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
[302] RONFAUT, L. et FERRAN, B. « La double authentification, un geste simple pour se protéger du piratage », Le Figaro, 9 juin 2016, en ligne : https://www.lefigaro.fr/secteur/high-tech/pratique/2016/06/09/32002-20160609ARTFIG00117-la-double-authentification-un-geste-simple-pour-se-proteger-du-piratage.php
[303] « [T]here are three generally recognized factors for authentication: something you know (such as a password), something you have (such as a hardware token or cell phone), and something you are (such as your fingerprint). Two-factor means the system is using two of these options. » : GRIFFITH, E. « Two-Factor Authentication: Who Has It and How to Set It Up », PCMag, 11 mars 2019, en ligne : https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up ; HIGGINS, P. « How to Enable Two-Factor Authentication on Twitter (And Everywhere Else) », Electronic Frontier Foundation, 28 mai 2013, en ligne : https://www.eff.org/deeplinks/2013/05/howto-two-factor-authentication-twitter-and-around-web

La double authentification peut être activée (directement ou au moyen d'applications) sur la plupart des téléphones intelligents, des comptes de médias sociaux, des boites de courriels, des grands sites Web transactionnels, etc[304].

À noter que l'usage de la double authentification améliore la protection de la vie privée de son utilisateur du point de vue de la cybersécurité, mais peut malheureusement être nuisible en ce qui concerne d'autres éléments de la vie privée en ligne. Il s'agit après tout de la divulgation à une entité de données supplémentaires (et de données généralement très privées). À titre d'exemple, il est possible de s'authentifier auprès de Facebook, au moyen, en plus du mot de passe, d'un code de sécurité reçu par SMS sur un appareil mobile. Ce faisant, Facebook acquiert par cette opération le numéro de téléphone de ses usagers. Et il a reconnu en 2018 - après avoir été exposé par un groupe de chercheurs[305] - qu'il s'en sert dans le cadre de son programme de publicité ciblée[306].

2.2.3. Les technologies d'amélioration de la confidentialité en ligne

Une autre mesure active de protection de la vie privée est le recours à l'une des technologies d'amélioration de la confidentialité disponibles sur le marché. Il en existe plusieurs types qui sont présentés dans la section suivante.

La formule « technologies d'amélioration de la confidentialité » (*privacy enhancing technologies*) a été d'abord utilisée en 1995 dans le cadre d'un rapport conjoint du Commissaire à l'information et à la protection de la vie privée de l'Ontario et de l'autorité néerlandaise de protection de la vie privée (nommée *Registratiekamer* à l'époque) qui explorait les technologies de protection de la vie privée, et particulièrement celles relatives à l'anonymat en ligne[307].

À la lumière des différentes définitions existantes[308], nous formons la définition suivante des technologies d'amélioration de la confidentialité en ligne :

---

[304] GARUN, N. « How to set up two-factor authentication on all your online accounts », The Verge, 27 mars 2019, en ligne : https://www.theverge.com/2017/6/17/15772142/how-to-set-up-two-factor-authentication ; KLOSOWSKI, T. « How to Protect Your Digital Privacy », New York Times, en ligne : https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

[305] VENKATADRI, G *et al.* « Investigating sources of PII used in Facebook's targeted advertising », Proceedings on Privacy Enhancing Technologies, 19 avril 2018, en ligne : https://mislove.org/publications/PII-PETS.pdf ; Les constatations des chercheurs ont par la suite été reprises dans HILL, K. « Facebook Is Giving Advertisers Access to Your Shadow Contact Information », Gizmodo, 26 septembre 2018, en ligne : https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051

[306] LOMAS, N. « Yes Facebook is using your 2FA phone number to target you with ads », Techcrunch, 27 septembre 2018, en ligne : https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/

[307] INFORMATION AND PRIVACY COMMISSIONER FOR THE PROVINCE OF ONTARIO et REGISTRATIEKAMER. « Privacy-Enhancing Technologies: The Path to Anonymity », vol 1, août 1995, en ligne : http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf

[308] *Ibid,* section 1.3 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Technologies d'amélioration de la confidentialité – Un survol des outils et des techniques », novembre 2017, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2017/pet_201711/ ; COMMISSION NATIONALE POUR LA PROTECTION

> Ensemble d'outils, d'applications et de mécanismes techniques intégrés aux instruments de connexion à Internet, aux services ou aux plateformes en ligne et destinés à atténuer les risques pour la sécurité et la vie privée des internautes.

Notons que les technologies d'amélioration de la confidentialité sont parfois perçues comme des substituts à la mise en place d'instruments législatifs ou réglementaires[309]. Nous sommes d'avis que, bien au contraire, il s'agit d'une protection complémentaire qui n'enlève en rien toute l'importance d'un encadrement solide en matière de vie privée.

2.2.3.1. Outils d'anonymisation

Les outils d'anonymisation ont pour but de permettre aux internautes de ne pas être identifiés lors de la navigation. Ils servent à masquer leur identité en ligne[310]. Des données seront collectées (sites consultés, heures des visites, préférences, etc.), mais ne pourront être ultimement rattachées à l'individu.

Il existe plusieurs manières d'identifier un internaute, que ce soit par exemple au moyen de son adresse courriel ou de son adresse IP (numéro d'identification unique de sa connexion à Internet[311]). Des outils sont disponibles pour anonymiser ces différents éléments.

Il est à noter que certains navigateurs privés agissent également comme anonymiseurs. Ils sont abordés plus bas, à titre d'outils de limitation des données.

Réseaux privés virtuels

Il existe de multiples services de réseaux privés virtuels (communément appelés VPN, de l'anglais, *Virtual Private Network*) qui permettent de masquer l'adresse IP d'un internaute. Un VPN fonctionne ainsi : tout le trafic de l'internaute qui l'utilise se fera via un « tunnel

---

DES DONNÉES. « Usage de Privacy-Enhancing Technologies (PETS) », en ligne : https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Usage-de-Privacy-enhancing-Technologies-_PETs_.html (consulté le 10 avril 2021) ; THE ROYAL SOCIETY. « Protecting privacy in practice », mars 2019, p.14, en ligne : https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf ; DANEMARK. Ministry of Science Technology and Innovation, « Privacy Enhancing Technologies », META Group Report v 1.1, 28 mars 2005, p.4, en ligne : https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf ; COMMISSION DES COMMUNAUTÉS EUROPÉENNES. « Communication de la Commission au Parlement Européen et au Conseil », COM(2007) 228, 2007, p.3, en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52007DC0228&from=EN

309 PISA CONSORTIUM. « Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents », 2003, p.34, en ligne : https://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

310 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Technologies », *supra* note 308.

311 Un nom et une adresse d'un individu ou d'une entreprise sont liés à l'adresse IP. Il s'agit normalement de la personne responsable du paiement de l'abonnement au service d'accès à Internet.

sécurisé » (chiffré) vers le réseau Internet[312]. Ce faisant, les sites consultés ne seront pas en mesure d'identifier d'où provient réellement la connexion et le fournisseur de service d'accès Internet de l'internaute ne saura pas ce qu'a consulté l'internaute.

Il existe aussi des services de serveurs mandataires (proxy) qui, similairement aux réseaux privés virtuels, permettent aux internautes qui les utilisent d'accéder à des sites Web au moyen d'une adresse IP qui n'est pas la leur mais celle du serveur tiers, qui agit comme intermédiaire entre les différents réseaux[313]. Contrairement aux VPN, les serveurs mandataires ne chiffrent pas les données transmises entre l'appareil de connexion et le serveur[314].

Il est à noter que les réseaux privés virtuels et les serveurs mandataires sont parfois plus connus pour l'utilisation qu'en font certaines organisations afin de permettre à leurs employés d'accéder à distance au serveur de l'organisation. Ces outils sont également utilisés par certains afin d'accéder à du contenu non accessible depuis leur position géographique, mais accessible ailleurs dans le monde (accès des contenus bloqués par certains états, accès à des contenus de divertissement géolocalisés, etc.).

Malheureusement, il arrive à l'occasion que ces outils ne fonctionnent pas comme prévu et qu'ils portent ultimement atteinte à la vie privée de l'utilisateur. La faille la plus courante concerne le dévoilement occasionnel de l'adresse IP par l'outil lui-même en raison d'une vulnérabilité dans le système informatique ou d'une interruption de la connexion à l'outil[315].

Adresses courriel jetables

Un autre outil d'anonymisation en ligne est l'adresse courriel jetable ou temporaire. Ce type d'outil permet aux utilisateurs de se créer une nouvelle adresse courriel et d'y accéder pendant une courte période de temps (généralement quelques minutes). Ces adresses courriel peuvent être utilisées lorsqu'un internaute doit remplir un formulaire en ligne ou fournir une adresse courriel pour accéder à un contenu particulier en ligne ; une adresse temporaire élimine le risque de recevoir par la suite des courriels indésirables (pourriels) dans sa véritable boite de courriel[316].

---

[312] EUROPEAN UNION AGENCY FOR CYBERSECURITY. « PETs controls matrix - A systematic approach for assessing online and mobile privacy tools », 20 décembre 2016, pp.35-36, en ligne : https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools

[313] FITZPATRICK, J. « What's the Difference Between a VPN and a Proxy? », How To Geek, 18 juin 2019, en ligne : https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/ ; KURNIADI, D. The Difference Between Using Proxy Server and VPN », 2015, en ligne : https://www.researchgate.net/publication/317809198_The_Difference_Between_Using_Proxy_Server_and_VPN

[314] *Ibid.*

[315] Une étude réalisée en 2015 concluait que 10 des 14 VPN populaires étudiés étaient susceptibles de divulguer l'adresse IPv6 d'un utilisateur. Voir à ce sujet : « Researchers Reveal Top VPN Services Leak IP Data, Vulnerable to DNS Hijacking », TripWire, 30 juin 2015, en ligne: https://www.tripwire.com/state-of-security/latest-security-news/researchers-reveal-top-vpn-services-leak-ip-data-vulnerable-to-dns-hijacking/ ; Voir similairement : VIJAYAN, J. « Port Fail Vulnerability Exposes Real IP Addresses of VPN Users », Security Intelligence, 1er décembre 2015, en ligne: https://securityintelligence.com/news/port-fail-vulnerability-exposes-real-ip-addresses-of-vpn-users/

[316] TUFNELL, N. « 21 tips, tricks and shortcuts to help you stay anonymous online », The Guardian, 6 mars 2015, en ligne : https://www.theguardian.com/technology/2015/mar/06/tips-tricks-anonymous-privacy

2.2.3.2. Outils de limitation des données

Comme leur nom l'indique, les outils de limitation des données ont pour but de réduire la quantité de données collectées par un site Web consulté par un internaute ou par une application utilisée par ce dernier. Ces outils assurent que seules les données minimales, dont la collecte est nécessaire à la navigation ou à l'utilisation, sont recueillies[317].

Navigateurs privés

De manière générale, les navigateurs les plus populaires (Chrome, Explorer/Edge, Safari, Firefox, etc.) enregistrent des données sur les activités de navigation de leurs usagers (sites visités, date et heure de chaque visite, etc.)[318]. Il existe des navigateurs dits privés qui permettent d'échapper à une telle collecte et à la conservation des données.

Le plus célèbre de ces navigateurs est Tor, dont le développement a été partiellement financé par Electronic Frontier Foundation[319]. Tor est en fait un acronyme pour *The Onion Router*, en référence à son fonctionnement par « routage en oignon ». Les communications transmises sur le réseau Internet sont intégrées à des couches de chiffrement des données et circulent à travers différents relais intermédiaires aléatoires (sur différents serveurs), ce qui assure entre autres que l'adresse IP à l'origine de la communication ne soit pas divulguée[320].

Mode de navigation privée

Même dans les navigateurs qui ne sont pas privés, il est possible d'utiliser un mode privé (parfois appelé *mode incognito* ou *inPrivate*)[321]. Ces modes sont avant tout destinés à empêcher l'enregistrement automatique sur l'appareil de l'utilisateur de données telles que l'historique de navigation ou les témoins (*cookies*)[322]. Ils agissent comme des sessions de navigation temporaires distinctes de la navigation régulière d'un utilisateur. Notons que la simple activation du mode de navigation privée est généralement jugée insuffisante – et assure une protection moindre que les navigateurs privés – parce qu'elle permet tout de même à certains serveurs de suivre l'activité d'un internaute en ligne[323].

---

317 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Technologies », *supra* note 308.
318 *Ibid.*
319 TOR. « History », en ligne: https://www.torproject.org/about/history/
320 ALQAHTANI, A. A. et EL-ALFY, E-S. M. « Anonymous Connections Based on Onion Routing: A Review and a Visualization Tool », Procedia Computer Science, vol. 52, 2015, pp.123 et ss.
321 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Technologies », *supra* note 308.
322 JOHANSEN, A. G. « Is Private Browsing Really Private? Short answer: No », Norton, en ligne : https://us.norton.com/internetsecurity-privacy-your-private-browser-is-not-so-private-after-all.html ; DICKSON, B. « Private Browsing Won't Protect You From Everything », PC Magazine, 16 septembre 2019, en ligne : https://www.pcmag.com/news/370703/private-browsing-wont-protect-you-from-everything
323 DELEON, N. « What Your Web Browser's Incognito Mode Really Does », Consumer Reports, 19 juin 2018, en ligne : https://www.consumerreports.org/internet/incognito-mode-web-browser-what-it-really-does/ ; MATHEWS, L. « What Is Private Browsing And Why Should You Use it? », Forbes, 27 janvier 2017, en ligne : https://www.forbes.com/sites/leemathews/2017/01/27/what-is-private-browsing-and-why-should-you-use-it/#53e0308325b1 ; AGGARWAL, G *et al.* « An Analysis of Private Browsing Modes in Modern Browsers » ,

Moteurs de recherche privés

Il existe plusieurs moteurs de recherche qui se présentent comme étant « privés », c'est-à-dire qu'ils collectent très peu de données lorsqu'un internaute fait une recherche en ligne. Ainsi, ils ne collectent généralement pas les adresses IP des utilisateurs et n'archivent pas de renseignements relatifs aux recherches réalisées (mots-clés, date et heure, etc.)[324]. Et puisqu'ils ne les « profilent » pas, ils n'ont pas pour pratique de filtrer les résultats de recherche en fonction des utilisateurs ou de présenter de la publicité comportementale[325]. Ils sont généralement mis en opposition aux moteurs de recherche de Google, de Bing ou de Yahoo qui, eux, suivent à la trace leurs utilisateurs et adaptent le moteur de recherche en conséquence[326].

Le plus connu de ces moteurs de recherche est DuckDuckGo, auquel renvoie d'ailleurs automatiquement le navigateur Tor, mentionné plus haut[327].

Bloqueurs de témoins

Il est à noter que d'autres outils peuvent également bloquer l'installation de témoins (cookies) sur un navigateur et ainsi réduire la quantité de données collectées au sujet d'un internaute. C'est le cas par exemple de certains outils de filtrage de contenu que nous aborderons plus loin[328].

2.2.3.3. Outils de chiffrement des données et des communications

Il existe aujourd'hui de nombreux logiciels et applications destinés à chiffrer les données des internautes sur leurs appareils de connexion (ordinateur, téléphone, etc.). De même, certains services de messagerie ou de partage de contenus en ligne offrent le chiffrement

Proceedings of Usenix Security, 2010, en ligne : https://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf

[324] CRAWFORD, D. « The Best Private Search Engines That Respect Your Privacy », ProPrivacy, 13 mai 2020, en ligne: https://proprivacy.com/cloud/private-search-engines ; MORRIS, J. « DuckDuckGo: The search engine taking on Google and making the internet 'less creepy' with its privacy mission », Evening Standard, 12 mai 2019, en ligne: https://www.standard.co.uk/news/world/duckduckgo-the-search-engine-taking-on-google-and-making-the-internet-less-creepy-with-its-privacy-a4138911.html ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Technologies », supra note 308.

[325] CHAN, K. « European privacy search engines aim to challenge Google », Associated Press, 21 novembre 2018, en ligne : https://www.apnews.com/dd8824e6f9424439b66e3992882b5c0b

[326] TENE, O. « What Google Knows: Privacy and Internet Search Engines », Utah Law Review, en ligne : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021490

[327] LOMAS, N. « Tor switches to DuckDuckGo search results by default », Techcrunch, 31 mai 2016, en ligne : https://techcrunch.com/2016/05/31/tor-switches-to-duckduckgo-search-results-by-default/

[328] Section 2.2.3.7.

automatique des communications[329] et des extensions compatibles avec les boites de courrier électronique des grands fournisseurs sont facilement accessibles[330].

Des experts recommandent aussi plus largement l'utilisation d'outils de chiffrement lors de la navigation même sur Internet, tel *HTTPS Everywhere* qui sécurise les sites Web non sécurisés[331].

2.2.3.4. Outils de suppression des données

Il existe des outils qui, plutôt que d'empêcher la collecte de données lors de la navigation, en éliminent les effets après coup, à la fin de la session de navigation par exemple. Ils effacent alors l'historique de navigation et/ou éliminent les témoins (*cookies*) qui peuvent avoir été installés lors de la navigation[332], rendant plus difficile le profilage de l'internaute (et ultimement l'exposition à de la publicité comportementale). Pensons par exemple au logiciel CCleaner[333] ou à l'extension de navigation *Cookie* AutoDelete[334]

2.2.3.5. Outils d'assombrissement des données

Il existe des outils destinés à « assombrir » *(obfuscating)* les données des internautes en créant en parallèle des données inexactes dans lesquelles les données réelles de l'internaute sont « noyées ». Le tout, afin de rendre plus difficile la création d'un profil sur l'internaute ou de rendre ce profil totalement inexact et, donc, inutilisable[335] :

> This signal-jamming offers just one modest example of the larger theory of obfuscation, the idea that if you can't disappear online at least you can hide yourself in a miasma of noise[336].

Ces outils qui n'influencent pas la navigation d'un internaute - les actions lui sont généralement invisibles - offrent une myriade de possibilités :

---

[329] Pour une recension des services existants, consulter le scoreboard d'Electronic Frontier Foundation : ELECTRONIC FRONTIER FOUNDATION. « Secure Messaging Scorecard », en ligne : https://www.eff.org/fr/pages/secure-messaging-scorecard (consulté le 13 juin 2021).
[330] VINCENTE, M. « Comment crypter des e-mails ? », TechAdvisor, 21 avril 2020, en ligne : https://www.techadvisor.fr/tutoriel/ordinateurs/crypter-emails-3689941/
[331] LAWRENCE, J. et RINTEL, S. « Eight ways to protect your privacy online », The Guardian, 3 décembre 2013, en ligne : https://www.theguardian.com/commentisfree/2013/dec/03/eight-ways-to-protect-your-privacy-online
[332] DANEMARK. « Privacy Enhancing Technologies », *supra* note 308, p.17.
[333] CCleaner, en ligne: https://www.ccleaner.com/fr-fr/
[334] Cookie AutoDelete, en ligne : https://chrome.google.com/webstore/detail/cookie-autodelete/fhcgjolkccmbidfldomjliifgaodjagh?hl=en
[335] POWLES, J. « Obfuscation: how leaving a trail of confusion can beat online surveillance », The Guardian, 24 octobre 2015, en ligne : https://www.theguardian.com/technology/2015/oct/24/obfuscation-users-guide-for-privacy-and-protest-online-surveillance
[336] DREYFUSS, E. « Wanna Protect Your Online Privacy? Open a Tab and Make Some Noise », Wired, 29 mars 2017, en ligne : https://www.wired.com/2017/03/wanna-protect-online-privacy-open-tab-make-noise/

- Simuler des clics sur les publicités disponibles (ex : extension de navigateur AdNauseam[337])
- Simuler des recherches Web aléatoires en continu (ex. : application TrackMeNot[338]),
- Simuler des visites de sites Web aléatoires en continu (ex. : application Noise[339])
- Signaler des positions géographiques multiples (ex. : application CacheCloak[340]).

Il est à noter que certains navigateurs tentent régulièrement de bloquer l'utilisation d'outils d'assombrissement parce qu'ils augmentent le trafic en ligne, mais aussi parce qu'ils nuisent à l'exactitude de leur publicité ciblée et *de facto* à leurs revenus publicitaires[341].

2.2.3.6. Outils de marquage des données

Un autre type de technologies d'amélioration de la confidentialité concerne le marquage des données personnelles des internautes. Les données transmises en ligne sont ainsi associées à « des étiquettes comportant des instructions ou des préférences pour le traitement des données par les fournisseurs de services[342] ». Les internautes indiquent par exemple s'ils acceptent le traitement des données à des fins de recherche, de transactions financières, etc.[343] Ces instructions sont indiquées dans un format lisible par un ordinateur (ex. : le langage E-P3P auparavant pris en charge par Windows) afin que le traitement se fasse automatiquement[344].

Si cette technologie est très intéressante, il faut admettre qu'elle est surtout présente dans la littérature scientifique, mais n'a pour l'instant que peu de répercussions concrètes, n'ayant pas été adoptée par les consommateurs.

2.2.3.7. Outils de filtrage du contenu en ligne

Nous recensons finalement des outils de filtrage de contenus, une méthode qui protège de manière indirecte la vie privée des internautes.

---

[337] ADNAUSEAM. En ligne: https://adnauseam.io/
[338] TRACKMENOT. En ligne: https://trackmenot.io/
[339] INTERNET NOISE. En ligne : http://makeinternetnoise.com/index.html
[340] CACHECLOAK. En ligne` https://dl.acm.org/doi/pdf/10.1145/1710130.1710138
[341] CIMPANU, C. « Google to no longer allow Chrome extensions that use obfuscated code », ZDNet, 1er octobre 2018, en ligne : https://www.zdnet.com/article/google-to-no-longer-allow-chrome-extensions-that-use-obfuscated-code/ ; CIMPANU, C. « Mozilla announces ban on Firefox extensions containing obfuscated code », ZDNet, 2 mai 2019, en ligne : https://www.zdnet.com/article/mozilla-announces-ban-on-firefox-extensions-containing-obfuscated-code/
[342]COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Technologies », *supra* note 308.
[343] PEARSON, S. *et al.* « Sticky Policies: An Approach for Managing Privacy across Multiple Parties », Computer, vol. 44 , no. 9, Sept. 2011, p.61.
[344] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Technologies », *supra* note 308.

Bloqueurs de pourriels

Certains fournisseurs de boites courriel offrent d'emblée une fonction de filtrage des courriels indésirables ; il existe aussi des bloqueurs de pourriels tiers, qui peuvent être ajoutés aux boites de courriel des utilisateurs. Ces outils utilisent diverses techniques afin d'identifier et d'écarter les courriels indésirables (analyse du contenu des courriels, des expéditeurs de pourriels répertoriés, etc.)[345].

Bloqueurs de publicités et fenêtres pop-up

Les internautes ont également accès à des bloqueurs de publicités, outils qui se présentent généralement sous forme d'extensions de navigateurs (Adblock Plus[346], Privacy Badger[347], Ghostery[348], uBlock Origin[349], etc.). Certains bloquent toutes les publicités identifiées sur la page Web consultée par l'internaute et les fenêtres pop-up associées à la page, alors que d'autres outils limitent le filtrage aux publicités susceptibles d'exécuter des logiciels malveillants (*malwares, spywares*) ou d'effectuer le suivi des internautes[350].

Malheureusement, les différents bloqueurs de publicités offrent une protection inégale et généralement incomplète, puisque plusieurs des outils les plus utilisés ont conclu des ententes commerciales avec certains publicitaires qui voulaient éviter le filtrage de leurs publicités[351]. L'efficacité des bloqueurs de publicités est également malmenée par les politiques de certains navigateurs et sites Web, qui en bloquent ou complexifient grandement le fonctionnement ou qui refusent l'accès, afin d'assurer leurs revenus publicitaires[352].

---

345 DANEMARK. « Privacy Enhancing Technologies », *supra* note 308, p.16.
346 ADBLOCK PLUS. En ligne: https://adblockplus.org/fr/
347 PRIVACY BADGER. En ligne: https://privacybadger.org/
348 GHOSTERY. En ligne : https://www.ghostery.com/
349 UBLOCK ORIGIN. En ligne: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=fr
350 BISCHOFF, P. « 75+ free tools to protect your privacy online », Comparitech, 26 janvier 2016, en ligne : https://www.comparitech.com/blog/vpn-privacy/75-free-tools-to-protect-your-privacy-online/#Ad_Blockers ; CHAIKIVSKY, A. « Want to Protect Against Websites That Spy on You? Get an Ad Blocker », Consumer Report, 15 février 2018, en ligne : https://www.consumerreports.org/digital-security/to-protect-against-websites-that-spy-on-you-get-an-adblocker/ ; HENRY, AL. « The Best Browser Extensions that Protect Your Privacy », Lifehacker, 31 août 2015, en ligne : https://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034
351 COOKSON, R. « Google, Microsoft and Amazon pay to get around ad blocking tool », Financial Time, 1er février 2015, en ligne : https://www.ft.com/content/80a8ce54-a61d-11e4-9bd3-00144feab7de ; NATEOG. « Google reportedly paid Adblock Plus not to block its ads », The Verge, 5 juillet 2013, en ligne : https://www.theverge.com/2013/7/5/4496852/adblock-plus-eye-google-whitelist
352 HAY NEWMAN, L. « Google Says It Isn't Killing Ad Blockers. Ad Blockers Disagree », Wired, 12 juin 2019, en ligne : https://www.wired.com/story/google-chrome-ad-blockers-extensions-api/ ; ROGERS, K. « Why Your Ad Blocker Doesn't Block Those 'Please Turn Off Your Ad Blocker' Popups », Vice, 12 décembre 2018, en ligne : https://www.vice.com/en_us/article/j5zk8y/why-your-ad-blocker-doesnt-block-those-please-turn-off-your-ad-blocker-popups

Bloqueurs d'objets-fenêtres de médias sociaux

Enfin, il existe également des extensions de navigateur destinées à bloquer les objets-fenêtres (*widgets*) des médias sociaux (ex. : Facebook Container)

De nombreux sites Web permettent aux internautes de partager directement la page Web consultée sur les médias sociaux, en utilisant les boutons « j'aime » de Facebook et « Tweet » de Twitter intégrés à l'interface de pages Web de sites tiers. Pratiques en apparence, ces boutons ont toutefois le vilain défaut de permettre aux médias sociaux concernés de suivre à la trace leurs abonnés en ligne. Ils sont avisés de chaque site consulté par l'internaute qui comprend un de ses objets-fenêtres, même s'il ne clique par sur le bouton[353].

2.3. Qu'est-ce que le paradoxe de la vie privée ?

Un survol de la littérature scientifique relative à la protection de la vie privée par les consommateurs permet d'identifier un phénomène régulièrement soulevé par les auteurs, soit le paradoxe de la vie privée en ligne.

Ce phénomène a été identifié dans la littérature scientifique au tournant des années 2000. Premier auteur à aborder le sujet, Barry Brown examine en 2001 les craintes de certains consommateurs pour la protection de leur vie privée et leur utilisation, en parallèle, de cartes de fidélité dans les épiceries. Il conclut que la situation « presents something of a paradox, in that while our participants seemed to be willing to volunteer general worries about privacy, in turn they were also willing to loose that privacy for very little gain[354] ».

L'existence potentielle d'un paradoxe de la vie privée a par la suite été reprise par plusieurs auteurs qui ont à leur tour fait des tests auprès de consommateurs, notamment auprès d'internautes. Les résultats contradictoires de certaines études sont survolés dans les pages qui suivent.

Retenons que le paradoxe de la vie privée est généralement décrit comme un décalage entre les préoccupations des consommateurs pour la protection de leur vie privée et leur comportement réel à ce sujet[355]. S'il n'est pas exclusif au réseau Internet, les manifestations du paradoxe y seraient plus présentes[356], notamment parce que l'accès à de nombreux services en ligne requiert la divulgation de renseignements personnels. Le

---

[353] EFRATI, A. « 'Like' Button Follows Web Users », Wall Street Journal, 18 mai 2011, en ligne : https://www.wsj.com/articles/SB10001424052748704281504576329441432995616
[354] BROWN, B. « Studying the Internet Experience », Hewlett Packard, 26 mars 2001, pp.17-18, en ligne : https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf
[355] HALLAM, C. et ZANELLA, G. « Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards », Computers in Human Behavior, vol. 68, 2017, p.217.
[356] CHEN, H-T. « Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management », American Behavioral Scientist, vol. 62, no. 10, 2018, p.1395.

phénomène est d'ailleurs parfois qualifié plutôt de dilemme de la vie privée en ligne, en raison de ce « choix » auquel font régulièrement face les internautes[357].

Peu importe le nom qui lui est donné, plusieurs types de comportements des internautes ont été identifiés en ligne pour appuyer l'existence du phénomène, comme :

- L'adoption de comportements risqués, dont la divulgation (volontaire ou insouciante) de nombreux renseignements à caractère personnel sur les médias sociaux[358]
- L'absence totale de mesures prises en vue de protéger sa vie privée en ligne[359]
- La faiblesse ou l'inadéquation des mesures prises en vue de protéger la vie privée en ligne[360].

2.3.1. Des études variées sur le sujet

Néanmoins, un survol des études réalisées sur le paradoxe de la vie privée en ligne depuis 2006 permet de constater que l'existence du phénomène en ligne est encore bien loin de faire l'unanimité.

[357] GOULDING, A. « The identity and privacy dilemma », Newsroom, 26 août 2019, en ligne : https://www.newsroom.co.nz/@ideasroom/2019/08/26/770241/the-identity-and-privacy-dilemma# ; BURKHARDT, K. « The privacy paradox is a privacy dilemma », Mozilla Firefox, 24 août 2018, en ligne : https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/

[358] NORBERG, P. A., HORNE, D. R. et HORNE, D. A. « The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors », Journal of Consumer Affairs, vol. 41, nº 1, 2007, p.101 ; XIE, W., FOWLER-DAWSON, A. et TVAURI, A. « Revealing the relationship between rational fatalism and the online privacy paradox », Behaviour & Information Technology, vol. 38, no. 7, 2019, p.744 ; BAEK, Y., KIM, E. et BAE, Y. « My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns », Computers in Human Behavior, vol. 31, no. 1, 2014, p.49.

[359] BAEK, Y. « Solving the privacy paradox: A counter-argument experimental approach », Computers in Human Behavior, vol. 38, 2014, p.34.

[360] GERBER, N., GERBER, P. et VOLKAMER, M. « Explaining the Privacy Paradox - A systematic review of literature investigating privacy attitude and behavior », Computers & Security, vol. 77, 2018, p.227.

Tableau 4

Présentation sommaire de certaines études relatives au paradoxe de la vie privée en ligne

Études qui rejettent ou nuancent fortement l'existence du paradoxe	Études qui reconnaissent l'existence du paradoxe
L'étude de Dienlin *et al*. des Universités Mainz et Hohenheim[361] Plus de 1400 internautes allemands ont été sondés en 2014 et 2015 dans le cadre d'une étude longitudinale (6 mois entre les périodes de questions) relative à leurs habitudes et perception de la divulgation de renseignements personnels en ligne. Les chercheurs ont observé que des changements au niveau de préoccupation pour leur vie privée en ligne étaient partiellement corrélés à des changements aux comportements de divulgation en ligne. Par exemple, les internautes dont le niveau de préoccupation augmenterait partageaient un peu moins de renseignements qu'avant (quantité et fréquence) et inversement[362].	L'étude d'Oomen et Leenes de l'Université Tilburg[363] Un peu plus de 5500 étudiants néerlandais ont été sondés en 2006 et 2007 au sujet de leurs stratégies de protection de leurs renseignements personnels en ligne. Les deux chercheurs concluent que l'adoption de comportements et d'outils de protection est rarement supérieure chez ceux qui perçoivent davantage de risques pour leur vie privée en ligne. On y note certaines exceptions, dont le recours aux technologies de cryptage et aux adresses courriel jetables, qui est associé à un niveau de préoccupation supérieure chez les internautes concernés[364].
L'étude de Lutz et Strathoff de l'Université de St Gallen[365] Plus de 1000 internautes suisses ont été sondés en 2012 relativement à l'adoption de comportements de protection de la vie privée en ligne et de sécurité informatique.	L'étude de Tufekci de l'Université du Maryland[368] Plus de 700 étudiants de la côte Est américaine utilisateurs des réseaux sociaux Facebook et Myspace ont été sondés en 2006 et 2007 sur leurs habitudes de

[361] DIENLIN, T., MASUR, P. K. et TREPTE, S. « A Longitudinal Analysis of the Privacy Paradox », septembre 2019, en ligne : https://www.researchgate.net/publication/335948948_A_Longitudinal_Analysis_of_the_Privacy_Paradox
[362] *Ibid*., p.22.
[363] OOMEN, I. et LEENES, R. « Privacy risk perceptions and privacy protection strategies » dans LEEUW E, FISCHER-HÜBNER S, TSENG J, BORKING J, dir. Policies and research in identity management, Springer, 2008, p. 121–138.
[364] *Ibid,* pp.129-132.
[365] LUTZ, C. et STRATHOFF, P. « Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses », avril 2014, en ligne : https://www.researchgate.net/publication/259470061_Privacy_Concerns_and_Online_Behavior_-_Not_so_Paradoxical_After_All_Viewing_the_Privacy_Paradox_through_Different_Theoretical_Lenses
[368] TUFEKCI, Z. « Can you see me now? Audience and disclosure regulation in online social network sites » Bulletin of Science Technology & Society, vol. 28, no. 1, 2018, en ligne : https://www.researchgate.net/publication/249990380_Can_You_See_Me_Now_Audience_and_Disclosure_Regulation_in_Online_Social_Network_Sites

Les conclusions des deux chercheurs sont à l'effet qu'il existe une corrélation forte entre l'adoption de comportement de protection et le niveau de préoccupation pour l'utilisation des renseignements personnels à des fins commerciales en ligne[366]. Par ailleurs, les chercheurs ne constatent qu'un lien faible entre les préoccupations des personnes sondées relativement à l'utilisation de renseignements personnels à des fins de géolocalisation et l'adoption de comportements de protections efficaces à ce sujet[367], ce qui n'est pas sans rappeler les résultats de l'étude de Zafreiropoulou *et al*.	divulgation de renseignements personnels sur ces réseaux et leurs préoccupations relatives à la vie privée en ligne, notamment en ce qui a trait à la visibilité de leur profil auprès d'un public non désiré. L'étude conclut que le niveau de préoccupation et la crainte particulière de visibilité n'ont que très peu d'impact sur le choix d'utiliser les plateformes et d'y divulguer des renseignements (à l'exception du numéro de téléphone cellulaire, de la religion et du nom, dans certains cas)[369].
<u>L'étude de Joinson *et al.* des Universités de Zurich, de Westminster et de Bath et de la Hult International Business School[370]</u> Environ 750 étudiants issus d'un panel de recherche en ligne de l'Open University (du Royaume-Uni) ont été questionnés au sujet de leurs préoccupations pour leur vie privée et de leurs comportements en ligne dans le cadre de deux sondages à six semaines d'intervalle. Les chercheurs arrivent à la conclusion que le niveau général de préoccupation pour la protection de la vie privée affirmé par les répondants permet de prédire leur volonté de divulguer des renseignements personnels en ligne dans les semaines suivantes[371]. L'étude est à l'effet que l'impact des préoccupations sur la divulgation en ligne est modeste, mais existe bel et bien[372].	<u>L'étude d'Acquisti et Gross de l'Université Carnegie Mellon[373]</u> Plus de 500 étudiants américains utilisateurs de la plateforme Facebook ont été sondés sur leurs préoccupations en matière de vie privée, leur utilisation de la plateforme et la visibilité de leur profil en ligne en 2006. Les chercheurs concluent que si les préoccupations des internautes pour leur vie privée peuvent influencer leur choix d'adhérer ou non aux réseaux sociaux, une fois inscrits, elles n'ont pas réellement d'impact sur l'ampleur des renseignements qui y sont divulgués par chacun[374].

366 *Ibid,* p.91.
367 *Ibid.*
369 *Ibid,* p.27.
370 JOINSON, A. N., REIPS, U.-D., BUCHANAN, T. et PAINE SCHOFIELD, C. B. « Privacy, trust, and self-disclosure online », Human–Computer Interaction, vol. 25, no. 1, 2010.
371 *Ibid.,* p.12.
372 *Ibid.,* p.18.
373 ACQUISTI, A. et GROSS, R. « Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook », Lecture Notes in Computer Science book series, vol. 4258, 2006.
374 *Ibid.*, p.51.

L'étude de Krasnova *et al.* de l'Université Humboldt de Berlin et de l'European School of Management and Technology[375]	L'étude de Zafreiropoulou *et al.* de l'Université de Southampton[376]
Quelque 250 utilisateurs allemands des plateformes de médias sociaux StudiVZ et Facebook ont été sondés en 2008 au sujet desdites plateformes (utilisation, préoccupations, confiance, etc.).	Environ 150 internautes utilisateurs d'applications mobiles (Foursquare, IMDB, Facebook, etc.) ont été sondés en 2013 au moyen de différents scénarios relatifs à la divulgation de leurs données de géolocalisation.
Les conclusions de l'étude sont à l'effet que les répondants ajustent l'information qu'ils divulguent en ligne en fonction des risques qu'ils perçoivent pour leur vie privée. Les auteurs notent que le niveau de confiance envers les médias sociaux influence indirectement l'ampleur de la divulgation de renseignements personnels puisqu'il affecte la perception des risques pour la vie privée par les usagers des plateformes.	Les chercheurs arrivent à la conclusion qu'il n'y a pas de corrélation significative entre le niveau de préoccupation et la volonté de partager ses données de géolocalisation, et ce, bien qu'il existe une corrélation entre le niveau général de préoccupation pour la protection de la vie privée et le niveau de préoccupation spécifique relatif aux données de localisation[377].

Il existe donc des résultats contradictoires en ce qui concerne l'existence d'un paradoxe de la vie privée chez les internautes américains et européens. Rappelons que la présente recherche comprend également les résultats d'un sondage réalisé auprès d'internautes canadiens en 2020. Nous aborderons en détail les résultats ainsi que les indices de la présence ou non d'un paradoxe de la vie privée chez nos répondants (section 3.3.5).

2.3.2. Quelques explications possibles

Puisque plusieurs recherches appuient l'existence d'un paradoxe de la vie privée, il est pertinent de s'attarder aux différentes explications possibles de ce phénomène. Nous aborderons brièvement celles qui sont les plus susceptibles de s'appliquer aux internautes canadiens.

De manière générale, les modèles théoriques s'appuient sur la prémisse qu'un internaute qui transmet des renseignements personnels en ligne, le fait à la suite d'un choix rationnel,

---

[375] KRASNOVA, H. *et al.* « Online social networks: Why we disclose », Journal of Information Technology, vol. 25, no. 2, 2010.
[376] ZAFEIROPOULOU, A. M. *et al.* « Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? », 2013, en ligne : https://www.researchgate.net/publication/266653696_Unpicking_the_privacy_paradox_Can_structuration_theory_help_to_explain_location-based_privacy_decisions
[377] *Ibid.,* p.469.

c'est-à-dire qu'il prend cette décision à la suite d'une évaluation des risques et bénéfices d'une telle transmission (qualifié de *privacy calculus*)[378]. Or, le consommateur, on le sait, est plus souvent impulsif que froidement calculateur[379]. Cela dit, même dans le cadre d'une évaluation rationnelle, certains éléments sont susceptibles d'affecter les choix et de mener à une évaluation erronée ou déformée des risques ou des bénéfices, d'où la présence potentielle d'un paradoxe.

2.3.2.1. Un manque de connaissances ?

Le paradoxe de la vie privée pourrait d'abord s'expliquer par une mauvaise évaluation des risques et bénéfices de la divulgation de renseignements personnels causée par un manque d'information ou de connaissances de l'internaute.

Rappelons qu'il existe une importante asymétrie d'information entre les consommateurs et les entreprises qui cherchent à collecter et traiter leurs renseignements personnels[380]. Les consommateurs connaissent peu ou pas les pratiques des entreprises qui les sollicitent. Ils connaissent également très peu l'encadrement législatif et réglementaire en place et leurs droits en matière de protection des renseignements personnels.

Cet important déficit d'information est fortement susceptible d'induire le consommateur en erreur lors de son évaluation des risques et bénéfices qui précède la divulgation de ses renseignements personnels à une entité privée[381].

2.3.2.2. Des raisons psychologiques ?

La distance psychologique

La fracture entre les craintes des consommateurs et leurs comportements peut également s'expliquer par la façon différente qu'ont les individus de concevoir les risques et les bénéfices en ce qui concerne la protection de leur vie privée en ligne.

Les bénéfices potentiels d'une divulgation de renseignements personnels auprès d'une entreprise sont généralement beaucoup plus tangibles que les risques potentiels. L'accès à des rabais ou l'amélioration, par la personnalisation, de services ou d'outils de socialisation sont beaucoup plus faciles à percevoir ou à concevoir pour les individus que

---

[378] Selon des théories économiques, les décisions des consommateurs seraient toutes motivées par un désir de maximiser leurs bénéfices Théorie de l'*homo oeconomicus*. GERBER. « Explaining the Privacy Parado », *supra* note 360, p.229.
[379] Les tribunaux du Québec ont défini à plusieurs reprises le consommateur moyen comme une personne pressée, crédule et inexpérimentée par opposition à prudente et diligente. La Cour suprême a confirmé le bien-fondé de cette approche. *Richard* c *Time* Inc., 2012 CSC 8, [2012] 1 R.C.S. 265.
[380] BANDARA, R., FERNANDO, F. et AKTER, S. « The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance ». Procedia Computer Science, vol. 121, 2017, pp. 564-565.
[381] *Ibid.*, p. 564 ; TREPTE, S. *et al.* « Do people know about privacy and data protection strategies? Towards the 'online privacy literacy scale' (OPLIS) » dans GUTWIRTH, S., LEENES, R. and DE HERT, P., dir, Reforming European Data Protection Law, Springer, lignes 491 et ss.

des situations négatives (et parfois hautement techniques) de bris de sécurité informatique, d'accès aux données par des tiers ou de profilage en ligne, par exemple[382]. Qui plus est, les risques dont doit tenir compte l'individu sont perçus comme incertains et hypothétiques et parfois identifiables uniquement après qu'une atteinte à la vie privée se soit produite[383], alors que les bénéfices, eux, sont souvent garantis et immédiats[384].

Ces distinctions sont importantes puisque les consommateurs accordent naturellement une plus grande importance aux éléments tangibles et maintiennent une certaine distance psychologique avec les éléments d'ordre plus abstrait[385]. Ils priorisent également les conséquences (positives ou négatives) rapprochées dans le temps, comme le rapportent Hallam et Zanella :

> [...] the privacy risk associated with information self-disclosure is perceived as abstract and psychologically distant, more related to distant-future intentions, while the social rewards are perceived as psychologically near and more concrete, related to short-term intentions. Our model shows that the near-future intentions are significantly related to the self-disclosure behavior, while the distant-future ones are not[386].

Le biais d'optimisme

La sous-évaluation des risques pour la vie privée en ligne pourrait également s'expliquer par la présence d'un biais d'optimisme, parfois qualifié d'optimisme comparatif ou encore décrit comme l'attitude « ça ne m'arrivera pas à moi[387] ».

Ainsi, des études démontrent que les individus évaluent distinctement les risques pour eux-mêmes et les risques pour les autres membres de la société dans laquelle ils évoluent. Et ils ont tendance à percevoir leur niveau de risques pour la protection de leur vie privée en ligne comme étant inférieur à celui des autres[388].

Les normes sociales

Le paradoxe de la vie privée en ligne pourrait également s'expliquer par la pression sociale exercée sur les internautes afin qu'ils participent à l'environnement social numérique[389].

---

[382] GERBER. « Explaining the Privacy Parado », *supra* note 360, p.229.
[383] HALLAM. « Online self-disclosure », *supra* note 355, p.219 ; ACQUISTI, A. et GROSSKLAGS, J. « Privacy and rationality in individual decision making », IEEE Security & Privacy, vol. 3, no. 1, 2005, p.26.
[384] BANDARA. « The Privacy Paradox», *supra* note 380, p. 565.
[385] *Ibid.* ; HALLAM. « Online self-disclosure », *supra* note 355, p.219.
[386] *Ibid.,* p.223.
[387] GILLESPIE, K. « It Won't Happen to Me: The Psychology Behind Optimism Bias », Vice, 16 octobre 2018, en ligne : https://www.vice.com/en/article/a3an4a/it-wont-happen-to-me-the-psychology-behind-optimism-bias
[388] Voir par exemple : CHO, H., LEE, J. S. et CHUNG, S. « Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience », Computers in Human Behavior, vol. 26, no. 5, 2010, p.990 ; CAMPBELL, J. *et al.* « Unrealistic optimism in internet events », Computers in Human Behavior, vol. 23, no. 3, 2007, pp.1280-1281 ; BANDARA. « The Privacy Paradox», *supra* note 380, p. 565.
[389] BANDARA. « The Privacy Paradox», *supra* note 380, p 563.

Selon des chercheurs, plusieurs internautes utiliseraient les médias sociaux et surtout y partageraient des renseignements à leur sujet afin de se conformer aux attentes de leurs pairs et ainsi faire partie d'une communauté en ligne, et ce, au détriment de leurs préoccupations relatives à la vie privée[390]. L'internaute divulgue dès lors ses renseignements personnels, non pas à la suite d'un choix rationnel, mais à la suite et en raison de la pression de ses pairs.

> It has been found that social norms and social rewards more often overwhelm consumers to undermine their privacy[391].
>
> Members of social groups using social networks as their primary communication medium put pressure on their peer group members to do likewise, i.e. share information and conform to social norms. Peer group members not conforming to communication and information sharing rituals are sanctioned with attention deprivation and exclusion from the social group. Opting out (…) becomes increasingly difficult the more group members agree on information sharing as a basic principle constituting their affiliation[392].

La fatigue relative à la protection de la vie privée en ligne

Des chercheurs pointent aussi vers le phénomène de la fatigue ou de l'apathie relative à la protection de la vie privée pour expliquer l'existence du paradoxe de la vie privée en ligne. Un sentiment de fatigue peut se produire lorsque l'internaute est continuellement interpellé par des demandes de consentement à la divulgation de renseignements personnels et qu'il n'arrive plus à y répondre comme il le désirerait (soit parce qu'il n'a aucun réel choix, soit parce qu'il ne peut réalistement prendre connaissance de l'information offerte en vue de prendre une décision éclairée)[393]. L'internaute dépassé (et désensibilisé) par cette situation risque alors d'adopter une stratégie de « désengagement » par rapport à la protection de sa vie privée en ligne afin de réduire le stress ressenti[394].

> […] consent overload, information overload, and the absence of meaningful choice leads to 'consent desensitisation'. Users no longer make active, informed choices when confronted with a consent situation, but instead simply provide consent when consent is asked[395].

---

390 GERBER. « Explaining the Privacy Parado », *supra* note 360, p.230 ; HALLAM. « Online self-disclosure », *supra* note 355, p.219.
391 BANDARA. « The Privacy Paradox», *supra* note 380, pp. 562-567.
392 FLENDER, C. et MÜLLER, G. « Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited » dans BUSEMEVER, J. R. *et al.,* dir, QI 2012: Quantum Interaction, Conference proceedings, 2012, pp.153-154.
393 CHOI, H., PARK, J. et JUNG, Y. « The role of privacy fatigue in online privacy behavior », Computers in Human Behavior, vol. 81, avril 2018, p.43 ; SCHERMER, B. W., CUSTERS, B. et VAN DER HOF, S. « The crisis of consent: How stronger legal protection may lead to weaker consent in data protection », Ethics and Information Technology, vol. 16, no. 2, 2014, p.176.
394 *Ibid.,* p.43 ; WIRTH, J., MAIER, C. et LAUMER, S. « The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: An Empirical Analysis », research Papers. 161, 2018, p.5.
395 SCHERMER. « The crisis of consent », *supra* note 393, p.178.

Le cynisme relatif à la protection de la vie privée en ligne

Enfin, certains chercheurs avancent la possibilité qu'un certain cynisme soit responsable de ce qui est perçu comme un paradoxe de la vie privée. Le sentiment d'impuissance ou de résignation ressenti par de nombreux internautes face aux risques pour leurs renseignements personnels en ligne aurait parfois pour effet ultime de rendre futile à leurs yeux toute tentative de les protéger[396].

> Privacy cynicism allows users to take advantage of online services without trusting providers while aware of privacy threats by forming the conviction that effective privacy protection is out of their hand[397].

Cette explication est appuyée entre autres par les résultats d'un sondage mené auprès de plusieurs milliers d'internautes américains et britanniques : le deux tiers des répondants jugeaient impossible de protéger leur vie privée en ligne en 2019, un chiffre fortement en hausse par rapport à l'année précédente[398]. Notons aussi que cette explication du paradoxe de la vie privée basée sur un sentiment d'impuissance concorde avec l'une des grandes préoccupations des internautes, exposées à la section 2.1.1, soit le sentiment d'avoir perdu le contrôle sur leurs renseignements personnels en ligne.

Xie *et al.* parlent quant à eux d'un « fatalisme rationnel » des internautes qu'ils associent principalement à l'incapacité (perçue) de la loi, des entreprises et des outils technologiques d'assurer une réelle protection de leurs renseignements personnels en ligne[399].

---

[396] XIE. « Revealing the relationship », *supra* note 358, p.745.
[397] HOFFMANN, C., LUTZ, C. et RANZINI, G. « Privacy cynicism: A new approach to the privacy paradox », Cyberpsychology: Journal of Psychosocial Research on Cyberspace, vol. 10, 2016, p.7.
[398] STERLING, G. «Most consumers believe online privacy is impossible, survey finds », MarTech, 10 juillet 2019, en ligne : https://marketingland.com/most-consumers-believe-online-privacy-is-impossible-survey-finds-263538 ; une étude similaire (mais limitée au marketing des renseignements personnels en ligne) a été réalisée en 2015 par des chercheurs de l'Université de Pennsylvanie et arrive à des résultats fort similaires : « When we investigated the overlap that designates resignation, we found that a majority of the population—58%— is resigned. » : TUROW, J., HENNESSY, M. et DRAPER, N. « The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them up to Exploitation », Communication, University of Pennsylvania, 2015, p.14.
[399] XIE. « Revealing the relationship », *supra* note 358, p.754.

LA PAROLE AUX CONSOMMATEURS CANADIENS

3.1 Sondage pancanadien

Nous avons mandaté une firme spécialisée afin de mener un sondage auprès de répondants canadiens au courant du mois de janvier 2020. L'échantillon, composé de 1519 résidents du Canada âgés de 18 à 97 ans et représentatif de la population, présente une marge d'erreur de 2,5 % 19 fois sur 20.

La représentation des différentes générations auxquelles appartiennent les répondants se détaille comme suit[400] :

- 12 % des répondants sont issus de la génération Z
- 26,7 % des répondants sont issus de la génération Y ou Z
- 28,8 % des répondants sont issus de la génération X
- 29,3 % des répondants sont des baby-boomers
- 3,3 % des répondants sont issus de la génération silencieuse ou précédente

Mentionnons d'emblée quelques limites du sondage et du bassin de répondants.

Puisque le sondage a été réalisé en ligne, les résultats pourraient dresser un portrait qui surreprésente quelque peu les opinions et comportements des internautes plus expérimentés[401]. Les Canadiens qui n'utilisent pas Internet n'ont pu être sondés. Cette exclusion, quoique regrettable, nous semble tout de même acceptable considérant qu'il s'agit d'une étude (et d'un sondage) sur la protection de la vie privée en ligne et que d'autres études tendent à démontrer que la non-adoption d'Internet ne découlerait généralement pas de considérations relatives à la vie privée[402].

Aussi, il est possible que les résultats sous-estiment quelque peu le niveau de préoccupation des Canadiens étant donné que les personnes qui participent à des sondages sont généralement moins soucieuses du respect de leur vie privée que les non-participants[403]. Notons néanmoins que ce risque ne semble pas avéré en l'espèce, étant donné les très hauts taux de préoccupation révélés par le sondage.

---

[400] Génération silencieuse (personnes nées entre 1928-1945), génération boomer (1946-1964), génération X (1965-1980), génération Y (1981-1996) et génération Z (1997-2012). Selon la catégorisation du Pew research Center : DIMOCK, M. « Defining generations: Where Millennials end and Generation Z begins », Pew research Center, 17 janvier 2019, en ligne : https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/

[401] HONG. « Drivers and Inhibitors », *supra* note 98, p.3.

[402] La non-adoption d'Internet par certains serait généralement liée aux coûts et à l'indisponibilité des services de télécommunication : STATISTIQUE CANADA. « Enquête canadienne sur l'utilisation de l'Internet, 29-10-2019 », en ligne : https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.htm ; HORRIGAN, J. B. et DUGGAN, M. « Home Broadband 2015 », Pew Research Center, 31 décembre 2015, en ligne : https://www.pewresearch.org/internet/2015/12/21/home-broadband-2015/

[403] ACQUISTI. « Imagined Communities », *supra* note 373, p.50.

3.1.1 Mise en contexte : les affaires *Desjardins* et *Capital One*

Avant d'aborder les résultats du sondage, il importe aussi de résumer brièvement deux évènements majeurs qui se sont produits dans les mois précédant la réalisation du sondage. Le cas qui implique Desjardins semble d'ailleurs avoir particulièrement marqué les répondants québécois et francophones, qui se distinguent des autres répondants sur plusieurs questions. Après tout, Desjardins est une des marques les plus influentes dans la province[404].

En juillet 2019, la banque américaine Capital One a révélé publiquement avoir fait l'objet d'un vol massif de données. Cette fuite de données survenue en mars et avril 2019, concerne environ 100 millions d'Américains et 6 millions de consommateurs canadiens. Les renseignements personnels divulgués touchaient des demandes de carte de crédit reçues entre 2005 et 2019 et comprenaient entre autres les noms et coordonnées des consommateurs et leurs cotes et historiques de crédit. Un million de numéros d'assurance sociale canadiens auraient également été piratés[405]. Une pirate informatique surnommée « Erratic », qui aurait exploité la mauvaise configuration d'un pare-feu de l'entreprise, a depuis été arrêtée et accusée par la justice américaine[406].

À la même époque, en juin 2019, un corps policier québécois a découvert qu'un ancien employé du Mouvement des caisses Desjardins avait obtenu et transmis illicitement des renseignements personnels de tous les 4,2 millions de clients particuliers de l'entreprise (date de naissance, numéro d'assurance sociale, numéro de téléphone, adresse courriel, etc.)[407]. Les personnes touchées ont été contactées en juillet ou novembre 2019, soit quelques mois à peine avant la tenue de notre sondage.

---

[404] DALLAIRE, S. « Indice Ipsos-Infopresse: Hydro-Québec en 3e place, juste derrière Google et Facebook », Infopresse, 25 mars 2019, en ligne : https://www.infopresse.com/article/2019/3/25/indice-ipsos-infopresse-hydro-quebec-en-3e-place-juste-derriere-les-geants-google-et-facebook

[405] ABEDI, M. « Capital One data breach: here's what Canadians need to know », Global News, 30 juillet 2019, en ligne : https://globalnews.ca/news/5702026/capital-one-data-breach-what-to-know/ ; MCLEAN, R. « A hacker gained access to 100 million Capital One credit card applications and accounts », CNN, 30 juillet 2019, en ligne : https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html ; BENNARDO, M. « Everything Canadians need to know about the Capital One data breach », CBC, 30 juillet 2019, en ligne : https://www.cbc.ca/news/business/capital-one-data-breach-1.5230287

[406] HAY NEWMAN, L. Everything We Know About the Capital One Hacking Case So Far », Wired, 29 août 2019, en ligne : https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/

[407] « Vol de données chez Desjardins : tous les membres particuliers touchés, Radio-Canada », 1er novembre 2019, en ligne : https://ici.radio-canada.ca/nouvelle/1371366/vol-de-donnees-desjardins-cormier-point-presse

3.1.2 Faits saillants

3.1.2.1 Qu'est-ce que la vie privée ?

Pour mieux saisir les préoccupations des internautes canadiens pour leur vie privée, il nous faut d'abord comprendre la signification qu'ils donnent à cette notion. Pour ce faire, nous avons proposé aux répondants cinq définitions qui touchent aux grands thèmes identifiés par la littérature (contrôle, accès, secret, dignité, etc.[408]). Les répondants avaient la possibilité de sélectionner une ou deux définitions qui les rejoignaient davantage.

Nous constatons que les définitions de la vie privée qui se rapportent aux renseignements personnels sont de loin les plus populaires chez les internautes sondés, peu importe leurs caractéristiques sociodémographiques. Sans se démarquer réellement l'une de l'autre, les trois définitions suivantes obtiennent toutes l'aval de plus de la moitié des répondants :

- Le contrôle du partage et de l'utilisation des renseignements personnels (58,8 %)
- La possibilité de déterminer l'utilisation du domicile, du corps et des renseignements personnels (56,2 %)
- La possibilité de garder secrets les renseignements personnels (53,3 %)

Les deux autres définitions proposées qui se rapportent à l'isolement et au contrôle de l'image sont peu populaires, avec des taux d'adhésion d'à peine 10 % et 4 % respectivement. Notons que la définition de la vie privée relative à la possibilité de s'isoler de l'espace public plait tout de même à une partie des répondants les plus jeunes. Elle correspond ainsi à la définition de la vie privée de 14,9 % des internautes de 18-34 ans sondés contre seulement 6,2 % de ceux âgés de 55 ans et plus. Elle est également davantage privilégiée par les résidents du Québec que par ceux des autres régions du pays.

3.1.2.2 Qu'est-ce qu'un renseignement privé ?

Les répondants associent en majorité la vie privée au contrôle ou à la protection de leurs renseignements personnels. Il importe donc de définir ce qu'est, à leurs yeux, un renseignement personnel ou un renseignement privé. Pour ce faire, nous avons soumis aux répondants une liste de 22 types de renseignements qu'ils devaient classer selon leur caractère privé ou public. Les renseignements qui sont jugés privés par le plus grand nombre de répondants sont les suivants :

- Mots de passe (98 %)
- Renseignements bancaires (97 %)
- Numéro de carte de crédit (97 %)
- Dossier de crédit (92 %)

[408] Voir section 1.2.1.

- Niveau de revenu annuel (91 %)
- Contenu des courriels (91 %)
- Sources de revenus (87 %)
- Photographies ou vidéos d'eux (80 %)

Sans être exclusifs à ces plateformes, nous constatons que les renseignements qui font l'objet d'opinions partagées quant à leur nature privée ou publique sont souvent ceux qui sont susceptibles d'être disponibles sur les médias sociaux. Pensons par exemple au nom, à l'âge, aux lieux fréquentés ou aux affiliations et opinions politiques, qui sont perçus comme privés par seulement 43 %, 57 %, 55 % et 64 % des répondants, respectivement. Qui plus est, les profils sur les médias sociaux sont au dernier rang du sondage. À peine 2 répondants sur 5 croient qu'il s'agit de renseignements privés, peu importe les paramètres de confidentialité mis en place par les usagers.

Les types de renseignements qui sont plus couramment disponibles sur les médias sociaux, à l'exception des photographies et de la localisation géographique, sont d'ailleurs les seuls pour lesquels nous constatons des différences significatives selon les groupes d'âge des répondants. Par exemple, moins de 35 % des internautes âgés de moins de 34 ans sont d'avis que le nom est un renseignement privé, contre près de 50 % de ceux qui ont 55 ans et plus. Même chose pour l'âge, qui est perçu comme une donnée de nature privée par 45 % des plus jeunes, mais par 60 % des plus âgés. Selon Statistiques Canada, 90 % des Canadiens âgés de 15 à 34 ans utilisent régulièrement au moins un média social, comparativement à 60 % des Canadiens âgés de 64 ans et plus[409].

Il n'existe pas de différences similaires selon les âges lorsqu'il est question de la perception des renseignements d'ordre financier (numéro de carte de crédit, dossier de crédit, niveau de revenu, etc.).

3.1.2.3 Qu'est-ce qui préoccupe les répondants ?

En moyenne, les répondants évaluent leur niveau de préoccupation pour la protection de leur vie privée en ligne à 7 sur 10. Notons que les répondants âgés de 55 ans et plus sont beaucoup plus nombreux à évaluer leur niveau de préoccupation au-delà de la barre du 9 sur 10 que leurs homologues plus jeunes (34,4 % contre 17,7 % chez les 18-35 ans et 24,4 % chez les 35-54 ans).

En plus de l'âge des répondants, le niveau de préoccupation varie également considérablement selon leur lieu de résidence. Si près de la moitié des répondants du Québec situent leur niveau de préoccupation à 9 ou 10 sur 10, c'est à peine un répondant sur cinq de l'Ontario ou de l'Ouest qui fait de même. Cette préoccupation particulièrement élevée des Québécois se reflète tout au long des résultats du sondage. Nous verrons plus

[409] SCHIMMELE, C., FONBERG, J. et SCHELLENBERG, G. « Canadians' assessments of social media in their lives, Economic and Social Reports », Statistiques Canada, 24 mars 2021, en ligne : https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm

loin que parmi les répondants québécois ultérieurement interviewés dans le cadre de cette étude, le nom de Desjardins était sur toutes les lèvres…

Tableau 5
Le niveau général de préoccupation des répondants pour la protection de la vie privée en ligne

Aucunement préoccupé — Extrêmement préoccupé

1	2	3	4	5	6	7	8	9	10
1,6 %	0,7 %	3,2 %	4,2 %	11,1 %	12,5 %	21,6 %	19,5 %	10,9 %	14,7 %
9,7 %				23,6 %		41,1 %		25,6 %	

Aucune des trois grandes catégories de préoccupation de Malhotra *et al*. ne se démarque. Les répondants affichent un niveau de préoccupation similaire (environ 7 sur 10 en moyenne) qu'il soit question de l'ampleur de la collecte de renseignements personnels en ligne, de la perte de contrôle sur lesdits renseignements ou de l'état de leurs connaissances sur le sujet. Un niveau de préoccupation plus élevé est encore une fois observable chez les répondants de 55 ans et plus et les résidents du Québec.

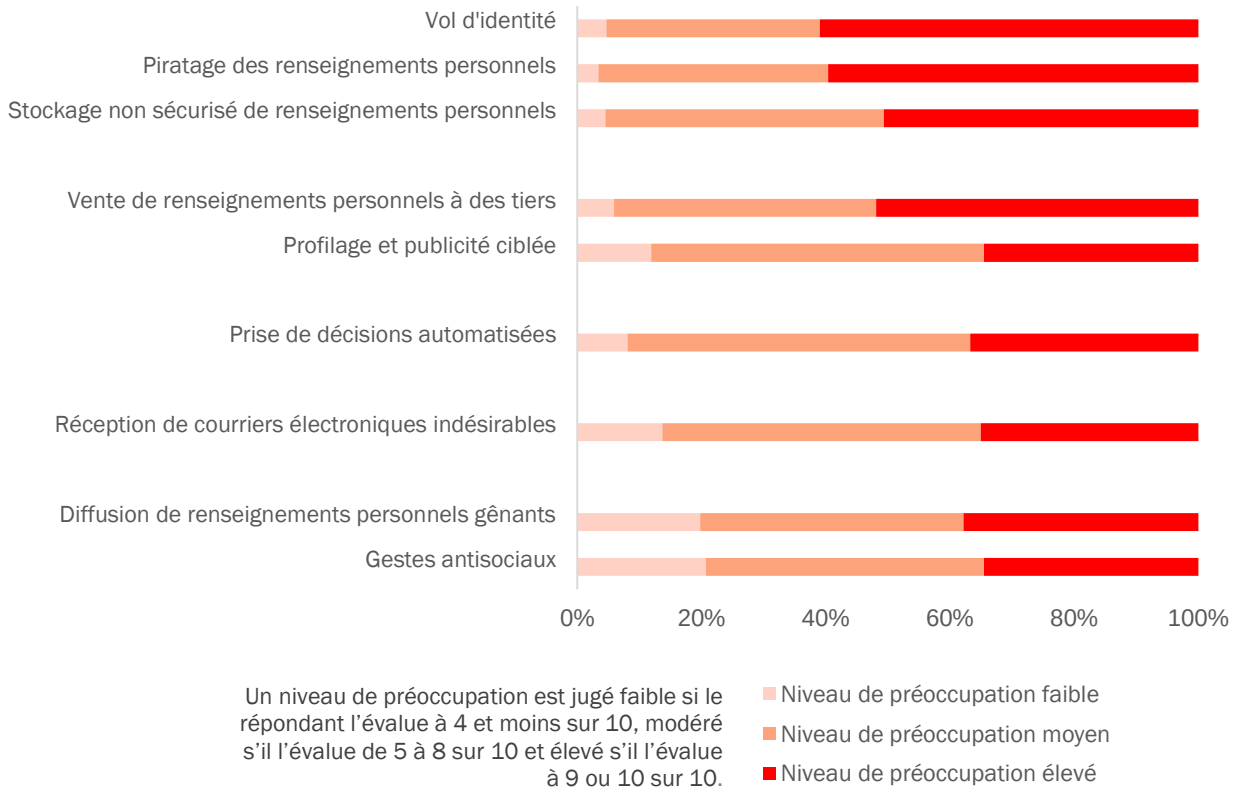
Le vol d'identité avant tout

Sans grande surprise, les risques liés au vol d'identité et au piratage des renseignements personnels sont ceux qui préoccupent le plus les répondants canadiens. Ils obtiennent tous les deux un niveau moyen de préoccupation d'environ 8,5 sur 10. En fait, aucun des risques soumis aux répondants n'obtient une note inférieure à 6 sur 10.

Les risques qui préoccupent le moins les répondants sont ceux qui concernent la perpétration de gestes antisociaux (menaces, harcèlement, intimidation) au moyen des renseignements personnels d'une personne, la diffusion de renseignements ou contenus personnels audio et vidéos gênants ou compromettants et la réception de courriers électroniques indésirables. Ces risques rejoignent davantage des définitions de la vie privée élaborée par la littérature qui ont été peu soutenues par les répondants, à savoir l'isolement de l'espace public et le contrôle de l'image (et de la réputation).

Les deux risques qui se rapportent davantage aux relations avec les autres (diffusion de contenus gênants, perpétration de gestes antisociaux) présentent tout de même des résultats intéressants. Ils divisent davantage les répondants. Ceux qui s'en préoccupent s'en préoccupent beaucoup et inversement, les autres s'en préoccupent particulièrement peu. Moins de répondants se montrent modérément préoccupés par ce risque que par bien d'autres risques (ex. : publicité ciblée, décision automatisée, etc.).

Tableau 6
Le niveau de préoccupation des répondants pour certains risques liés la protection de leur vie privée en ligne



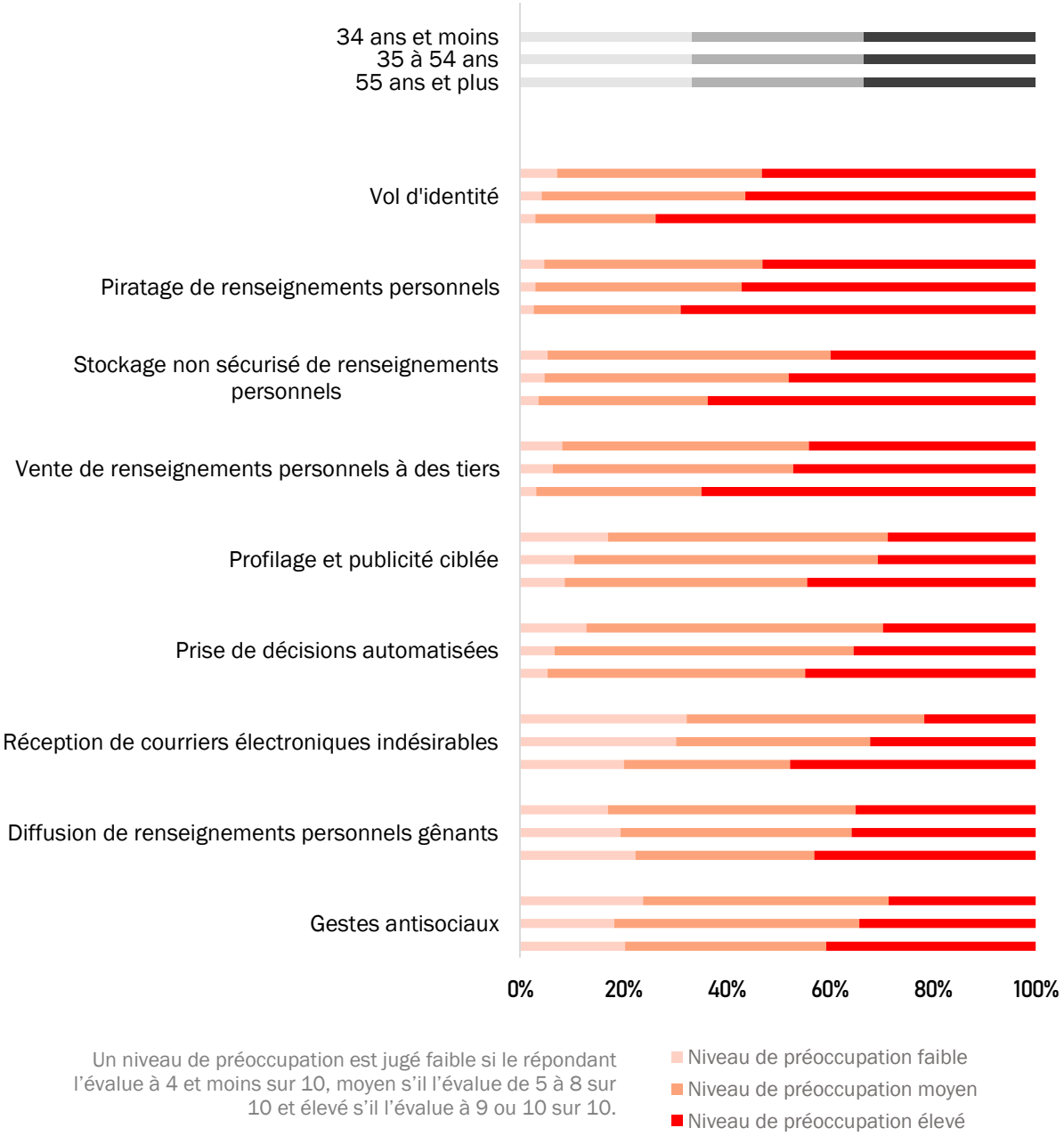
Tout comme pour le niveau de préoccupation général pour la protection de leur vie privée en ligne, les répondants âgés de 55 ans et plus se montrent généralement plus préoccupés par les différents risques que leurs homologues plus jeunes.

Ainsi, pour tous les risques présentés, à l'exception du risque de diffusion de contenus gênants ou compromettants, les répondants âgés de 55 ans et plus se disent davantage préoccupés que la moyenne des répondants. Pour ce dernier risque, nous notons ce résultat surprenant : on retrouve dans ce groupe d'âge à la fois les plus grands pourcentages de ceux qui sont les plus préoccupés et de ceux qui le sont le moins[410] !

[410] 42,9 % d'entre eux étaient très préoccupés (contre 34,9 % et 35,7 % chez les répondants âgés de 18-34 et de 35-54 ans, respectivement) et 22,4 % d'entre eux était peu préoccupés (contre 17,1 % et 19,5 % chez les répondants âgés de 18-34 ans et de 35-54 ans, respectivement).

Tableau 7

Le niveau de préoccupation des répondants pour certains risques liés à la protection de leur vie privée en ligne, selon leur groupe d'âges

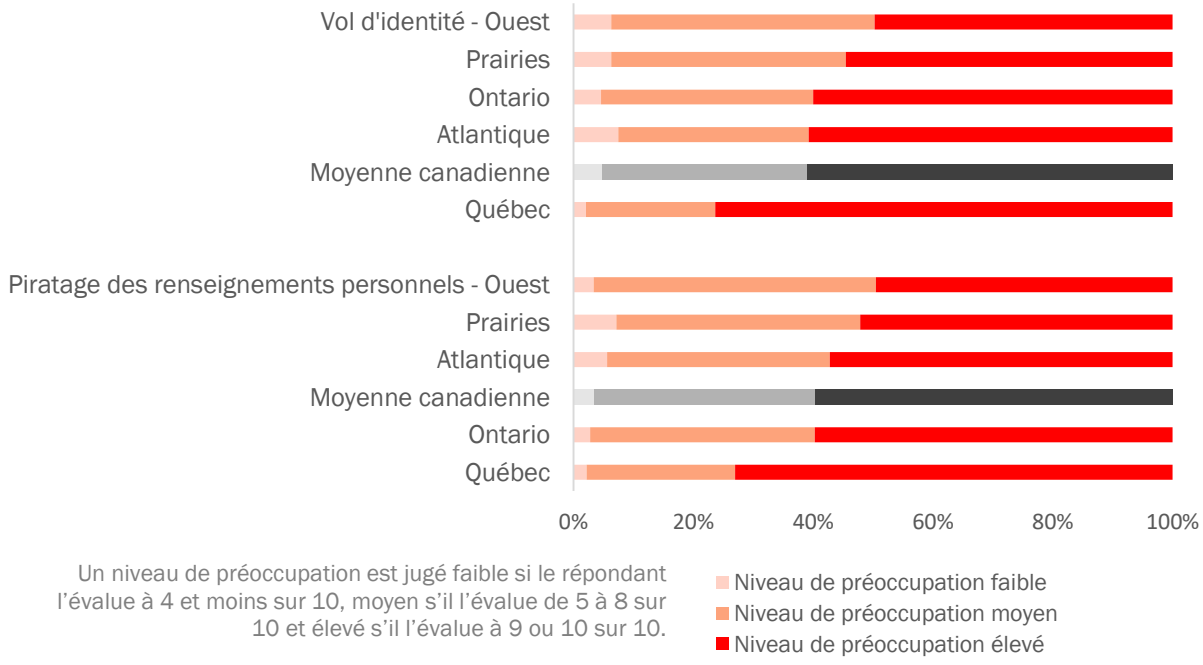


Un niveau de préoccupation est jugé faible si le répondant l'évalue à 4 et moins sur 10, moyen s'il l'évalue de 5 à 8 sur 10 et élevé s'il l'évalue à 9 ou 10 sur 10.

Les différences identifiées précédemment selon la région dans laquelle résident les répondants (Québec, Ontario, Prairie, Ouest ou Atlantique) sont maintenues. Systématiquement, les répondants québécois se disent plus préoccupés par les différents risques qui leur sont présentés que les répondants des autres régions. Et systématiquement, ceux qui sont issus des provinces de l'Ouest (et parfois des Prairies) font état du niveau moyen de préoccupation le plus bas pour ces mêmes risques. L'écart est marqué ; il est de près de 15 % en moyenne. Même pour les risques associés à la sécurité des renseignements personnels qui divisent certainement moins les répondants, les écarts sont notables entre les régions canadiennes.

Tableau 8

Le niveau de préoccupation des répondants pour certains risques liés à la protection de leur vie privée en ligne, selon leur région



Un niveau de préoccupation est jugé faible si le répondant l'évalue à 4 et moins sur 10, moyen s'il l'évalue de 5 à 8 sur 10 et élevé s'il l'évalue à 9 ou 10 sur 10.

Tout comme pour leur niveau général de préoccupation pour la protection de leur vie privée en ligne, les femmes ont un niveau moyen de préoccupation plus élevé que les hommes sondés pour chacun des risques qui leur sont présentés. Par exemple, les femmes sont 23 % plus nombreuses à se dire très préoccupées par le piratage de leurs renseignements personnels. L'écart atteint 32 % lorsqu'il est question de la diffusion de renseignements ou contenus audio et vidéo gênants ou compromettants. Il est difficile de ne pas établir de lien

avec l'effet disproportionné des phénomènes de la « revenge porn[411] » ou des « deepfakes[412] » sur les femmes en ligne[413].

Une crainte accrue associée aux téléphones intelligents

La moitié des répondants étaient d'avis que leur niveau de préoccupation variait selon l'appareil utilisé pour se connecter à Internet. Sans surprise, l'écart est moindre chez les répondants qui sont peu préoccupés par la protection de leur vie privée en ligne.

Trois répondants sur cinq sont plus préoccupés lorsqu'ils accèdent à Internet au moyen d'un téléphone intelligent que d'un ordinateur personnel. Cette tendance s'explique possiblement par les risques accrus liés à la sécurité de ce type d'appareil, tel que le décrit l'Electronic Frontier Foundation :

> Unfortunately, mobile phones were not designed for privacy and security. Not only do they do a poor job of protecting your communications, they also expose you to new kinds of surveillance risks—especially location tracking. Most mobile phones give the user much less control than a personal desktop or laptop computer would; it's harder to replace the operating system, harder to investigate malware attacks, harder to remove or replace undesirable bundled software, and harder to prevent parties like the mobile operator from monitoring how you use the device[414].

Les avis sont partagés en ce qui concerne les tablettes et les autres objets connectés (haut-parleurs intelligents, montres intelligentes, etc.). Un pourcentage similaire de répondants est d'avis que leur utilisation est plus préoccupante et moins préoccupante que celle d'un ordinateur pour la protection de la vie privée en ligne.

---

411 Parfois appelé « Pornodivulgation » en français ; il s'agit de la diffusion de vidéo ou d'image à caractère sexuel sans le consentement de la personne qui y est présenté, et ce, dans un but de vengeance ou de harcèlement : OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. « Pornodivulgation », en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552451 (consulté le 15 juillet 2021) ; MERRIAM WEBTERS. « Revenge porn », en ligne : https://www.merriam-webster.com/dictionary/revenge%20porn (consulté le 15 juillet 2021).

412 Parfois appelé « Hypertrucage » en français ; il s'agit d'un procédé de manipulation ultra crédible d'un enregistrement audio et/ou video qui permet de faire croire qu'une ou des personnes font ou disent des choses qu'elles n'ont pas faites ou dites en réalité : OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. « Hypertrucage », en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552557 (consulté le 15 juillet 2021) ; MERRIAM WEBSTER. « Deepfake », en ligne : https://www.merriam-webster.com/dictionary/deepfake (consulté le 15 juillet 2021).

413 WANG, C. « Deepfakes, Revenge Porn, And The Impact On Women », Forbes, 1er novembre 2019, en ligne : https://www.forbes.com/sites/chenxiwang/2019/11/01/deepfakes-revenge-porn-and-the-impact-on-women/?sh=552560191f53 ; SHARRATT, E. « Intimate image abuse in adults and under 18s », University of Exeter et Economic and Social Research Council, 2019, en ligne : https://swgfl.org.uk/assets/documents/intimate-image-abuse-in-adults-and-under-18s.pdf

414 ELECTRONIC FRONTIER FOUNDATION. « The Problem with Mobile Phones », 30 octobre 2018, en ligne : https://ssd.eff.org/en/module/problem-mobile-phones

3.1.2.4 Que font les répondants en vue de protéger leur vie privée en ligne ?

Questionnés sur les stratégies adoptées en vue de protéger leur vie privée en ligne, les répondants pointent d'abord les éléments suivants :

- L'utilisation d'un logiciel antivirus et/ou d'un pare-feu (69 % des répondants)
- L'utilisation d'un bloqueur de courriels indésirables (66 %)
- La réduction des renseignements personnels fournis ou partagés en ligne (62 %)
- L'utilisation de mots de passe différents pour la majorité des comptes en ligne (61 %)
- L'utilisation d'un bloqueur de publicités en ligne (60 %)
- La suppression manuelle de l'historique de navigation et des témoins (54 %)
- L'adaptation des paramètres de confidentialité des appareils, des sites et des applications (54 %)

Parmi les 23 comportements et outils que nous leur proposions dans le sondage, les répondants ont affirmé prendre chacun, en moyenne, un peu plus de 5 mesures différentes en vue de protéger leur vie privée en ligne.

Les internautes de 55 ans et plus se démarquent particulièrement des internautes plus jeunes lorsqu'il est question de comportements de retrait de la sphère numérique. Ils réduisent davantage les renseignements partagés en ligne (73 % contre 57 % chez les internautes de moins de 55 ans) et évitent certains contenus en ligne qui leur apparaissent risqués (56 % contre 45 %). Ils sont également plus nombreux à limiter ou à éviter entièrement les achats ou autres transactions financières en ligne (39 % contre 25 %).

Mais l'utilisation d'outils d'amélioration de la confidentialité en ligne semble, pour sa part, inversement proportionnelle à l'âge des répondants. Les jeunes internautes, ceux âgés de moins de 34 ans et dans certains cas ceux âgés de 35 à 54 ans, les connaissent et les utilisent davantage. Les hommes se démarquent également pour leur utilisation des outils et technologies présentés dans le sondage.

Tableau 9
La connaissance et l'utilisation des outils d'amélioration de la vie privée en ligne par les répondants

Outils	% de répondants qui **connaissent** l'outil				% de répondants qui ont déjà **utilisé** l'outil			
	Moyenne	Selon le groupe d'âge			Moyenne	Selon le groupe d'âge		
		18-34	18-34	55 et +		18-34	35-54	55 et +
Bloqueur de courriels indésirables	83 %	85 %	87 %	77 %	66 %	65 %	71 %	62 %
Bloqueur de publicités	83 %	90 %	85 %	75 %	60 %	71 %	59 %	52 %
Gestionnaire de mots de passe	73 %	75 %	77 %	66 %	50 %	75 %	49 %	29 %
Fonction ou mode de navigation privée	69 %	89 %	72 %	47 %	35 %	36 %	41 %	28 %
Réseau virtuel privé (VPN)	64 %	78 %	68 %	47 %	35 %	38 %	37 %	30 %
Bloqueur ou effaceur de témoins et d'historiques de navigation	62 %	71 %	66 %	51 %	32 %	43 %	35 %	19 %
Messagerie électronique chiffrée	59 %	64 %	64 %	48 %	24 %	27 %	27 %	18 %
Services de chiffrement des données	53 %	60 %	57 %	42 %	20 %	26 %	20 %	14 %
Adresse courriel temporaire	51 %	58 %	53 %	41 %	19 %	21 %	21 %	15 %
Navigateur privé	38 %	50 %	40 %	23 %	17 %	20 %	19 %	12 %
Moteur de recherche privé	36 %	47 %	40 %	22 %	16 %	22 %	17 %	8 %

* Les pourcentages ont été arrondis à l'unité.

3.1.2.5 Quel est l'état des connaissances des internautes ?

81 % des répondants affirment s'être déjà renseignés au sujet de la protection de leur vie privée en ligne. Ils s'informent auprès d'une variété de sources sur les risques pour leur et les comportements et outils à adopter afin de se protéger. En fait, aucune des sources qui leur étaient proposées ne se démarque réellement :

- Familles et proches : 38,5 % des répondants
- Médias traditionnels (journaux, télévision, radio, etc.) : 33 %
- Médias numériques (blogues, podcasts, etc.) : 30,5 %
- Fournisseurs d'accès Internet : 31 %
- Entreprises sur Internet (Google, Yahoo, Facebook, etc.) : 29,5 %
- Organismes gouvernementaux : 24 %

Un niveau de connaissance modeste

Nous avons demandé aux répondants d'évaluer l'état de leurs connaissances relativement aux pratiques des entreprises en matière de collecte et d'utilisation de renseignements personnels en ligne.

Environ un répondant sur deux est d'avis qu'il a une bonne connaissance de ces pratiques. C'est davantage le cas chez les hommes, les anglophones et les consommateurs âgés de 18 à 34 ans. Les Québécois font encore une fois bande à part puisqu'ils autoévaluent leurs connaissances beaucoup plus sévèrement que la moyenne.

Nous constatons par ailleurs que ce portrait des connaissances des répondants n'est pas aussi tranché qu'il n'y parait. En fait, très peu de répondants se disent « très bien informés » ou « très mal informés » (7 % et 10 % respectivement). La forte majorité des répondants ont une confiance modérée quant à l'état de leurs connaissances (42 % se disent « plutôt bien informés » et 41 % se disent « plutôt mal informés »).

Bien que cette étude ne se veuille pas une évaluation du degré de littératie des Canadiens en matière de vie privée, la seule autoévaluation de leurs connaissances par les répondants nous paraissait insuffisante et elle aurait à notre avis dressé un portrait trop inexact de la situation. Afin de tester le niveau de connaissance réel des répondants, nous leur avons soumis cinq affirmations qu'ils devaient qualifier de « vraies » ou « fausses ». Le test était très sommaire et le niveau de difficulté relativement bas. Toutes les affirmations soumises étaient fausses.

Nous constatons avec surprise que les répondants qui se disent bien ou très bien informés relativement aux pratiques des entreprises en matière de collecte et d'utilisation de renseignements personnels en ligne obtiennent généralement de moins bons résultats que les autres, tel qu'il appert du tableau 10 ! De même, alors que les femmes, les Québécois et les consommateurs de plus de 55 ans évaluent bien plus sévèrement leurs connaissances que leurs contreparties respectives, ils obtiennent sensiblement les mêmes scores au test et s'en sortent même mieux pour certaines affirmations.

De manière générale, ce test « vrai ou faux » nous permet de constater que la majorité des répondants, peu importe le degré de connaissances qu'ils croient détenir, sont conscients de la possibilité d'être identifié et suivis en ligne, malgré certaines précautions. Mais les situations présentées aux répondants étant assez simples et il y a tout de même lieu de s'inquiéter que de 19 % à 31 % des répondants fassent fausse route. On peut facilement imaginer que ce pourcentage augmente en flèche lorsqu'il est question de pratiques de collecte plus subtiles ou complexes (ex. : *browser fingerprinting, canvas fingerprinting, zombie cookies, supercookies, evercookies, etc.*[415]). D'autant plus que le niveau de

[415] Pour une description de ces différentes technologies : GHOSTERY. « Cookies and fingerprinting: tracking methods clearly explained », 6 mars 2018, en ligne : https://www.ghostery.com/cookies-fingerprinting-co-tracking-methods-clearly-explained/ ; AVAST. « What Is Browser Fingerprinting and How Can You Prevent It? », en ligne: https://www.avast.com/c-what-is-browser-fingerprinting (consulté le 15 mai 2021).

méfiance des répondants au sondage a pu être artificiellement exagéré en raison de leur exposition à plusieurs questions préalables sur la vie privée en ligne.

Tableau 10
Les réponses des répondants selon leur niveau de connaissance (autoévalué)

Affirmations	**% de répondants d'avis que c'est faux**	% des répondants « bien informés » d'avis que c'est faux[416]	% des répondants « mal informés » d'avis que c'est faux	**% de répondants d'avis que c'est vrai**
« Si vous ne divulguez pas votre nom, vos coordonnées ou votre image en ligne, il est impossible de vous identifier lors de la navigation. »	**84 %**	81 %	86 %	16 %
« Les données collectées par un objet connecté à Internet (comme une montre, un frigo ou un téléviseur intelligent) sont transmises uniquement au fabricant de l'objet. »	**75 %**	74 %	77 %	25 %
« La présence d'une politique de confidentialité sur un site Web garantit que les renseignements personnels collectés ne seront pas partagés à d'autres entreprises. »	**73 %**	71 %	74 %	27 %
« Les plateformes de médias sociaux collectent uniquement des renseignements personnels de la part des internautes membres de leur site Web. »	**70 %**	68 %	72 %	30 %
« Il est impossible de géolocaliser un internaute lorsqu'il a désactivé la fonction de localisation de son appareil connecté à Internet. »	**69 %**	69 %	69 %	31 %

[416] Les répondants « bien informés » sont ceux qui ont affirmé, dans le cadre d'une autre question du sondage, « très bien » ou « plutôt bien » connaitre les pratiques des entreprises relatives à la collecte et à l'utilisation de renseignements personnels en ligne. Ils représentent 48,8 % de l'ensemble des répondants. Les répondants « mal informés » sont ceux qui ont affirmé « très mal » ou « plutôt mal » connaitre les pratiques des entreprises relatives à la collecte et à l'utilisation de renseignements personnels en ligne. Ils représentent 51,2 % de l'ensemble des répondants.

3.1.2.6 Quel est l'état de la confiance des répondants ?

La perception des répondants quant à leur protection actuelle

56 % des répondants ont l'impression de ne pas protéger suffisamment leur vie privée en ligne et désirent en faire davantage. C'est particulièrement le cas des Québécois et des femmes. À l'inverse, 43 % des répondants sont d'avis qu'ils protègent suffisamment leur vie privée en ligne. Cette fois, ce sont les résidents des provinces de l'Atlantique et de l'Alberta qui se démarquent. Contrairement à ce que l'on observe dans beaucoup d'autres thèmes abordés dans le sondage, nous ne notons ici aucune différence significative selon l'âge des répondants.

Les répondants qui sont d'avis qu'ils n'en font pas assez pour protéger leur vie privée en ligne sont invités à choisir parmi une liste d'explications possibles. Plus de la moitié d'entre eux considèrent que leur manque de connaissances en ce qui a trait aux comportements à adopter et outils ou technologies à utiliser les empêche d'en faire plus. Rappelons que certains outils, comme les moteurs de recherche privée et les navigateurs privés, étaient connus d'à peine le tiers des répondants. Une proportion similaire des répondants est d'avis que les technologies et outils disponibles sont trop complexes.

Les autres raisons proposées aux répondants pour expliquer pourquoi ils ne protègent pas suffisamment, selon eux, leur vie privée en ligne ont été choisies dans les proportions suivantes :

- Le sentiment d'impuissance face à la collecte et l'utilisation de leurs renseignements personnels : 38 %
- Le manque de temps ou de motivation pour s'informer des pratiques en matière de vie privée des sites Web consultés et des applications utilisées : 35 %
- La difficulté à identifier et à comprendre les risques : 21 %
- Le désir de ne pas modifier sa routine ou son quotidien en ligne : 18 %

Notons que le sentiment d'impuissance affecte plus de 50 % des répondants résidant au Québec, une statistique qui s'explique probablement en partie par le scandale de la fuite de données chez Desjardins, qui en a surpris plus d'un. De même, le manque de temps ou de motivation affecte plus de 50 % des répondants âgés de 34 ans et moins.

Les risques acceptables

Nous avons également interrogé les répondants sur les situations dans lesquelles ils acceptent de fournir des renseignements personnels en ligne. Plus de 50 % des répondants, peu importe leur âge, acceptent de le faire afin de conclure des transactions en ligne, l'achat d'un bien, par exemple. Les autres situations privilégiées par les répondants sont toutes liées à des gains financiers ou matériels potentiels : participation

à des concours (44 %), gratuité d'un service (29 %) et rabais sur des produits et services en ligne (27 %).

La personnalisation de l'expérience en ligne convainc beaucoup moins les répondants (service à la clientèle personnalisé, recommandations personnalisées de biens et services, etc.). À peine plus de 5 % des répondants accepteraient de fournir des renseignements personnels en ligne afin de personnaliser la publicité à laquelle ils sont exposés, ce que la plupart font pourtant tous les jours en ligne…

Soulignons que près du quart des répondants n'accepteraient de fournir des renseignements personnels dans aucune des circonstances décrites plus haut. Là encore, ce résultat détonne avec la réalité des internautes d'aujourd'hui.

3.2 Entrevues semi-dirigées auprès de certains répondants

Nous avons réalisé des entrevues d'environ 25 minutes auprès de 30 participants au sondage. Ces entrevues, en français et en anglais, ont eu lieu dans les jours suivant la tenue du sondage, soit du 23 au 30 janvier 2020, afin de s'assurer d'une bonne participation de la part des répondants. Les individus interviewés ont été contactés uniquement après avoir répondu par l'affirmative à une question du sondage sollicitant leur intérêt à participer à une entrevue de suivi. Ils ont reçu un montant de 50 $ pour les remercier de leur participation à l'entrevue téléphonique.

3.2.1 Portrait des répondants

Nous avons interviewé presque autant de femmes (14) que d'hommes (16), malgré le fait qu'un nombre beaucoup plus élevé d'hommes avaient signalé leur intérêt à participer aux entrevues (27 % supérieur). Les individus interviewés étaient âgés de 23 à 77 ans, représentant ainsi les générations Z, Y, X et boomers. Certaines données démographiques sur les répondants sont fournies dans le tableau qui suit :

Tableau 11
Portrait des participants aux entrevues

Tranches d'âges	Sexe	Région	Langue
29 et -	♀	Atlantique	Fr
	♀	Ouest	En
	♂	Québec	Fr
30-39	♂	Atlantique	Fr
	♀	Ontario	En
	♀	Ouest	En
	♀	Québec	Fr
	♀	Atlantique	Fr
	♀	Ontario	En
	♂	Québec	Fr
40-49	♂	Québec	Fr
	♂	Québec	Fr
	♀	Ontario	En
	♂	Québec	Fr
	♂	Ontario	En
	♀	Ontario	En
	♂	Ouest	En
50-59	♂	Prairie	Fr
	♂	Ontario	En
	♂	Ontario	En
	♀	Atlantique	En
60-69	♂	Québec	Fr
	♂	Québec	Fr
	♀	Atlantique	En
	♂	Ontario	En
	♂	Québec	Fr
	♂	Québec	Fr
	♀	Ontario	En
70 et +	♀	Québec	Fr
	♀	Québec	Fr

3.2.2 Faits saillants

D'entrée de jeu, nous avons demandé aux répondants d'évaluer (de nouveau) leur niveau général de préoccupation pour la protection de leur vie privée sur une échelle de 1 à 10. La moyenne des réponses obtenues est un peu plus élevée qu'au sondage (presque 8 sur 10), ce qui s'explique peut-être par le caractère volontaire des entrevues ; ceux qui ont choisi d'y participer à la suite du sondage avaient possiblement un intérêt plus marqué que la moyenne pour le sujet. Soulignons d'ailleurs que deux des répondants ont indiqué avoir étudié dans le domaine des nouvelles technologies et/ou de l'informatique et que plusieurs autres ont affirmé s'être renseignés sur le sujet par eux-mêmes.

Nous ne constatons aucune corrélation entre le temps d'utilisation d'Internet des consommateurs interviewés (de 1h30 à plus de 12h par jour selon les répondants) et leur niveau de préoccupation pour la protection de leur vie privée en ligne. Notons qu'une étude de Paine Schofield *et al*. de 2007 conclut également à l'absence de corrélation entre ces éléments[417].

Pour la plupart, les consommateurs interviewés accèdent à Internet au moyen de plusieurs appareils, ordinateur, téléphone intelligent ou tablette. Dans le cadre des entrevues, nous n'avons pas noté d'impact du type d'appareil utilisé sur le niveau général de préoccupation pour la protection de leur vie privée sur Internet. On se rappellera pourtant que les résultats du sondage indiquaient un niveau de préoccupation plus grand lors de l'utilisation de téléphones intelligents. Il faut dire qu'aucun des répondants n'utilisait uniquement son téléphone intelligent pour accéder à Internet. Notons par ailleurs que les comportements et mesures rapportés par les consommateurs interrogés en vue de protéger leur vie privée en ligne se rapportent davantage à leur ordinateur. Ils semblent moins outillés ou enclins à adopter des mesures de protection pour leur vie privée pour leurs tablettes ou leurs téléphones intelligents. Nous y reviendrons.

Aucun des trente répondants ne mentionne spontanément ses objets connectés ou quelque préoccupation particulière à leur sujet.

3.2.2.1 Les fuites de données récentes à l'origine de l'augmentation du niveau de préoccupation

Un peu plus de la moitié des consommateurs interrogés se disent plus préoccupés par la protection de leur vie privée en ligne qu'à la même période l'an dernier.

Une seule personne s'est dite moins préoccupée qu'avant. Cette personne avait d'ailleurs un niveau de préoccupation général très bas (2 sur 10). Il est devenu clair au fil de la discussion avec cette dernière qu'elle avait acquis ce sentiment de confiance en ligne, non pas parce qu'elle ne voyait plus/pas de risque pour sa vie privée, mais bien parce qu'elle avait adopté dans les dernières années davantage des mesures de protection en ligne et se sentait davantage en mesure de faire face aux risques.

Ceux qui se disent davantage préoccupés par la protection de leur vie privée en ligne qu'au cours de l'année précédente pointent du doigt leur prise de conscience accrue des risques. Quelques participants réfèrent à des problèmes rencontrés par des proches, mais la grande majorité mentionne de manière plus générale les plus récentes fuites de données rapportées dans les médias : Desjardins, Capital One et dans une moindre mesure, Cambridge Analytica et Equifax. L'impression que les médias abordent davantage la question du traitement des renseignements personnels en ligne est répandue chez les participants. Les avis sont partagés à savoir s'il existe plus de risques qu'avant ou si ces derniers sont simplement plus connus et publicisés.

---

[417] PAINE SCHOFIELD. « Internet users' perceptions », *supra* note 153, p.530.

Nous constatons que les « géants du Web » sont relativement peu pointés du doigt par les répondants, malgré un traitement des renseignements personnels sévèrement critiqué par certains experts et médias[418]. De même, malgré l'association que font certains entre les enjeux de vie privée en ligne et les médias sociaux, rares sont les participants qui mentionnent Facebook, Instagram, Twitter ou TikTok sans que le sujet ne soit directement soulevé par l'intervieweur. Et Amazon et Google font l'objet de commentaires étonnamment positifs dans le contexte d'une entrevue sur la protection de la vie privée en ligne et soulèvent très peu d'inquiétudes chez les répondants[419]. Nous y reviendrons.

3.2.2.2 Les risques financiers d'abord et avant tout

Tout comme dans le sondage, le vol d'identité est le premier risque en importance pour la très forte majorité des personnes interviewées. Nous notons d'ailleurs que presque tous les répondants issus du Québec mentionnent la situation de Desjardins. Et lorsque les répondants ne mentionnent pas d'abord le risque de vol d'identité, c'est parce qu'ils mentionnent une situation pouvant découler de ce vol, par exemple une tache à leur dossier de crédit ou une transaction frauduleuse en leur nom.

Seuls deux répondants font exception à cette règle et se montrent assez peu préoccupés par le vol d'identité et ses impacts éventuels, financiers et autres. Les deux figurent parmi les plus jeunes des participants aux entrevues. L'un d'eux explique d'ailleurs se soucier assez peu de la question puisqu'« à son âge », il n'aurait pas encore « réellement » de dossier de crédit à protéger.

Lorsqu'ils sont questionnés sur ce qu'ils craignent du vol d'identité, les participants pointent principalement les conséquences suivantes :

- L'utilisation frauduleuse de leurs renseignements bancaires ou de crédit (ouverture de comptes, demande de crédit, achats, etc.)
- Les pertes financières
- La « destruction » de leur dossier de crédit
- La responsabilité pour des prêts contractés en leur nom
- Les pertes de temps ou la nécessité de devoir faire d'innombrables démarches afin de rétablir leur situation financière

---

[418] Voir par exemple : AMNESTY INTERNATIONAL. « Surveillance giants: how the business model of Google and Facebook threatens human rights », 2019, en ligne : https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF ; KAKAES, K. « Zuckerberg's new privacy essay shows why Facebook needs to be broken up », MIT Technology Review, 7 mars 2019, en ligne : https://www.technologyreview.com/2019/03/07/1248/zuckerbergs-new-privacy-essay-shows-why-facebook-needs-to-be-broken-up/ ; CAMERON, D. « Amazon's Favorite New Word Is 'Privacy,' But Does It Even Know the Meaning? », Gizmodo, 25 septembre 2019, en ligne : https://gizmodo.com/amazons-favorite-new-word-is-privacy-but-does-it-even-1838460901

[419] Google et Amazon figurent même en tête des marques technologiques auxquelles les Canadiens font le plus confiance d'après l'Index CanTrust de 2020 (taux de confiance de 58 % et 53 % respectivement) : SHANKAR, B. « Google and Amazon are the most trusted tech brands in Canada: study », Mobilesyrup, 23 avril 2020, en ligne : https://mobilesyrup.com/2020/04/23/2020-proof-cantrust-index/

Quelques répondants soulèvent également des préoccupations plus générales liées à leur place en société. L'un craint de devoir « refaire son nom » après un vol d'identité, alors qu'un autre avance qu'il pourrait tout simplement « ne plus exister ».

3.2.2.3 La publicité ciblée et le pourriel divisent les répondants

Aussitôt que les répondants sont interrogés sur les risques qu'ils entrevoient pour leur vie privée en ligne qui ne sont pas directement liés à l'utilisation de leurs renseignements financiers, les réponses deviennent plus vagues. Plusieurs répondants disent ouvertement que ces « autres risques » leur importent peu, comme c'est le cas de ce participant :

> « It's mostly identity theft. Apart from that, I'm not that worried about it. Except for anything financial, anything else I'm not worried about! »
> *Participant - 40 à 50 ans*

Ces réponses détonnent avec les résultats du sondage, qui font tout de même état d'un haut niveau de préoccupation pour les risques associés à la publicité ciblée, au profilage et à la prise de décision automatisée en ligne.

Plus encore, plusieurs répondants ramènent naturellement la discussion concernant d'autres risques soulevés par l'intervieweur au vol d'identité et à ses conséquences financières potentielles. Lorsqu'il est question du profilage en ligne et de la vente de renseignements personnels collectés à des entreprises tierces, une répondante se dit inquiète que ses renseignements soient également vendus par erreur à des « malfaiteurs » qui s'en serviraient pour voler son identité. Une autre s'inquiète de la sécurité des serveurs sur lesquels sont gardées les données traitées à des fins de profilage et des risques que celles-ci soient éventuellement volées et utilisées par un pirate informatique… en vue de voler son identité. Lorsqu'il est question de la réception de courriers électroniques indésirables, plusieurs soulignent le risque d'hameçonnage. Lorsqu'il est question de harcèlement sur les médias sociaux, plusieurs évoquent les arnaques (*scams*) sur ces plateformes.

La publicité ciblée

La publicité ciblée dérange une majorité des répondants. Les expressions « annoying », « fatiguant » et « agaçant » reviennent régulièrement dans les discussions. Par contre, les avis divergent, au-delà du malaise initial.

Quelques répondants seulement se disent inquiets par la pratique parce qu'elle expose l'ampleur de la collecte de renseignements personnels à leur égard et du traitement qui en est fait et/ou parce que leurs intérêts et habitudes de consommation sont des renseignements intimes qui ne devraient pas être aussi connus et utilisés ainsi à leur insu.

Les autres sont plutôt résignés. « It's more annoying, than concerning », dit l'un d'eux. La publicité ciblée est agaçante, au même titre que toutes les autres publicités, mais serait inoffensive. Plusieurs signalent d'ailleurs qu'il est facile de l'ignorer (ou même de la

bloquer). D'autres défendent les entreprises qui emploient cette pratique commerciale puisqu'elle serait logique dans la société capitaliste qui favorise la maximisation des profits et l'exploitation des données disponibles à cette fin.

Enfin, quelques répondants voient même des avantages à la publicité ciblée, en ce qu'elle faciliterait leurs démarches de magasinage en ligne et leur permettrait d'économiser à l'occasion. Un répondant souligne qu'il se sent beaucoup moins « agressé » par une publicité personnalisée que par une publicité qui concerne un produit ou un service qui ne lui convient pas du tout (et qu'il qualifie d'inutile).

Tableau 12
Extraits des entrevues au sujet de la publicité ciblée

LE MALAISE	L'INDIFFÉRENCE	L'ACCEPTATION	L'INTÉRÊT
« It gets a little bit too personal sometimes… Too much information that they know. » « It's like they are spying on you or something. It makes me uncomfortable. » « Ce n'est pas nécessairement terrible qu'ils sachent ce que j'achète, mais ça remet en question le concept même de vie privée. C'est à moi, ces renseignements-là. » « It's kind of creepy ! »	« Je comprends que ça peut en déranger certains, mais moi, je n'ai pas de problème avec ça. » « Le fait qu'ils sachent que j'aime quelque chose en particulier : ils ne feront pas grand-chose avec cette information-là ! » « It's annoying, but it's not a major concern. I'm not upset that they know what I like to buy. » « C'est fatigant parce que tu sens écouté, mais je ne pense pas qu'avec ça ils peuvent vraiment faire de quoi de malin. Ce ne sont pas des données importantes, des données sensibles. »	« If you're going to use Facebook or Snapchat, you go to a website that is provided for free, then they are going to use your data. If you don't want them to use tour data, don't use their services. » « I think that's just them advertising to the best of their abilities. It doesn't mean you have to buy it. It doesn't hurt anyone in any way. You can just ignore it super easily." « Quand on s'amuse sur Internet, il faut s'attendre à ça. »	« It's kind of good in a way. You see ads that you might be interested in. it's an advantage actually. » « Je pourrais même avoir un spécial. » « Parfois, ça peut être bénéfique pour moi. Je fais le choix d'embarquer ou non. »

Au sujet de l'acceptabilité de la publicité ciblée chez les consommateurs canadiens, nous notons qu'une étude d'Option consommateurs de 2015 arrive à un constat général similaire[420]. Cette étude approfondie sur la publicité comportementale (qui comprenait la

[420] « Malgré leurs préoccupations, les consommateurs semblent aussi trouver un intérêt dans le modèle d'affaires des entreprises en ligne, dont le financement repose en partie sur la PCL [publicité comportementale en ligne]. (…) Quelques-uns ajoutent que cette forme de publicité peut même s'avérer avantageuse, leur permettant de

tenue de groupes de discussion à Montréal et Toronto) permet tout de même d'apporter certaines nuances quant à la position relativement favorable de nombreux consommateurs, notamment lorsque certains renseignements jugés plus intimes sont utilisés.

Enfin, soulignons que plusieurs répondants semblent aussi se croire immunisés contre le profilage en ligne puisqu'ils ne feraient pas de magasinage ou d'achats en ligne. Les répondants font preuve d'un détachement fort similaire en ce qui concerne les courriers électroniques indésirables et les comportements antisociaux sur les médias sociaux.

Les courriers électroniques indésirables

Comme pour l'exposition à la publicité ciblée, les répondants se montrent agacés par la réception de courriers électroniques indésirables. Tous semblent par contre résiliés et soulignent l'efficacité des mécanismes mis en place par les fournisseurs de boite courriel pour atténuer le désagrément.

> « It bothers me, but not to a great extend because I have mechanisms to filter that away. »
> *Participant - 60 à 70 ans*

> « It takes exactly a second and a half to hit delete. No big deal. »
> *Participant - 40 à 50 ans*

Mais s'agit-il tout de même d'une atteinte à leur vie privée en ligne ? Les avis des répondants sont partagés sur cette question, mais une majorité croit que non, qu'il s'agit tout simplement d'une pratique de marketing agaçante - comme bien d'autres - mais sans plus. Quelques-uns se montrent davantage troublés par la pratique et y voient une preuve de la vente de leur adresse courriel à des entités tierces sans leur consentement.

3.2.2.4 Les médias sociaux : un risque pour les autres seulement

Les participants aux entrevues se montrent encore plus nonchalants en ce qui concerne les risques de comportements antisociaux en ligne (menaces, harcèlement ou intimidation basés sur les renseignements personnels des internautes). Une seule répondante le mentionne spontanément (en abordant le risque spécifique du *catfishing* sur les médias sociaux) et peu se disent préoccupés lorsqu'ils sont directement interrogés sur le sujet.

Ceux qui se montrent sensibles à ce risque critiquent surtout l'ampleur des renseignements personnels divulgués volontairement par les abonnés des médias sociaux et collectés par d'autres moyens par les plateformes et la facilité avec laquelle ces renseignements peuvent ensuite être utilisés.

> « Strangers know too much information about your private life. »

---

connaître des rabais pertinents, de découvrir de nouvelles idées d'achat ou de comparer les produits » : OPTION CONSOMMATEURS. « Le prix de la gratuit », *supra* note 599, p.33.

Participant - 20 à 30 ans

« I just don't want people to know what I'm doing or where I am. »
Participant - 30 à 40 ans

Il est intéressant de voir les différences de points de vue et d'expériences à ce sujet. Alors qu'un répondant doute que ces situations se produisent réellement, un autre affirme les « voir régulièrement sur Facebook ».

Nous constatons que, sauf exception, les participants ne se sentent pas à risque d'être victimes de comportements antisociaux en ligne, notamment parce qu'ils n'ont pas de comptes de média social ou parce qu'ils affirment n'y divulguer que peu de renseignements personnels ou y avoir resserré les paramètres de confidentialité. Plusieurs craignent toutefois pour les générations « plus jeunes » et leurs proches (enfants, petits-enfants), ce qui n'est pas sans rappeler le phénomène du biais d'optimisme (décrit brièvement à la section 2.3.2.2.2).

« I am not concerned on a personal level, but I could see the danger, how it could affect others. »
Participante - 30 à 40 ans

3.2.2.5 Des comportements de protection difficilement expliqués

Plusieurs participants admettent d'emblée ne pas avoir adopté beaucoup de comportements spécifiquement en vue de protéger davantage leur vie privée ou leurs renseignements personnels en ligne.

Selon les résultats du sondage, les Canadiens adopteraient un peu plus de 5 mesures en vue de protéger leur vie privée en ligne. Lorsqu'on demande aux participants des entrevues d'identifier les mesures (comportements ou outils) qu'ils prennent, sans suggestion ou choix de réponse, ils en nomment de 2 à 3 en moyenne. L'utilisation d'un antivirus revient presque systématiquement.

Il y a donc en apparence un écart entre les résultats du sondage et des entrevues quant à l'ampleur des comportements de protection de la vie privée réellement adoptés par les internautes canadiens. Il ne nous est pas possible de déterminer si les personnes sondées ont « embelli » leurs habitudes en ligne (en cochant des comportements qu'ils n'adoptent pas réellement ou que très rarement) ou si ces comportements sont plutôt à ce point intégrés à leur routine en ligne qu'ils ne sont pas toujours en mesure de les distinguer et de les identifier comme spécifiques à la protection de leur vie privée en ligne.

Notons par ailleurs qu'il existe une confusion importante entre certains outils d'amélioration de la confidentialité en ligne. C'est particulièrement le cas entre les navigateurs privés, les modes de navigation privée sur les navigateurs et les moteurs de recherche privés. Les participants qui les connaissent ou les utilisent mêlent régulièrement les termes. Les gestionnaires de mots de passe sont parfois confondus avec des antivirus, vraisemblablement parce certains antivirus offrent aujourd'hui des fonctions de gestion des mots de passe. Les résultats du sondage quant à la connaissance et l'utilisation de ces outils devraient donc être accueillis avec réserve. La connaissance générale des outils

qui était modérée et leur utilisation qui était plutôt faible le sont vraisemblablement bien davantage.

Mis à part l'antivirus, dont les bienfaits semblent dorénavant universellement reconnus, les participants ont régulièrement de la difficulté à expliquer quelle est l'utilité d'un comportement ou d'un outil qu'ils ont choisi d'adopter afin de protéger leur vie privée. Plusieurs « savent » qu'ils doivent agir ainsi en ligne, mais ne savent pas réellement pourquoi.

> « I'm not technically savvy. I go with these things, because I believe they are gonna protect my online privacy »
> *Participante - 60 à 70 ans*

> « I don't know the details of how it works. I just know I use it to protect my computer. (…) I don't know a lot about the cyberworld. I just know I use all these tools to protect myself. »
> *Participante - 70 ans et +*

Et plusieurs participants plus âgés affirment s'en remettre grandement à leurs proches afin d'assurer la protection de leurs appareils électroniques. Les « personnes-ressources » identifiées par les participants sont plus à l'aise avec les technologies (la fille, le mari, le petit-fils) ou ont des connaissances particulières en la matière (un collègue de travail qui œuvre dans le domaine de l'informatique par exemple).

> « Vous savez on n'est pas tous des cracks de l'informatique. Mon petit-fils de 16 ans nous en montre des fois et on dit « oh je ne savais pas ça ! ». Ils sont venus au monde avec un ordinateur dans les mains, eux ! »
> *Participant - 60 à 70 ans*

3.2.2.6 Leurs points de vue sur…

Les mots de passe

Nous constatons que la difficulté à retenir de nombreux mots de passe est un problème qui fait presque l'unanimité chez les participants aux entrevues. La plupart admettent – pour cette raison – ne pas changer régulièrement (et sans y être obligés) leurs mots de passe en ligne. Plusieurs signalent, comme s'ils souhaitaient se justifier auprès de l'intervieweur, qu'ils tentent tout de même de varier les mots de passe qu'ils créent. Nous notons que l'utilisation d'une variété de mots de passe complexes pour la majorité des comptes en ligne est beaucoup moins affirmée lors des entrevues que dans le cadre du sondage.

> « C'est peut-être mon seul défaut. J'ai souvent les mêmes mots de passe. J'ai 3-4 mots de passe pour tous les sites et je réussis quand même à les oublier ! »
> *Participante - 30 à 40 ans*

> « Ça fait quelques années que j'ai les mêmes mots de passe sur Internet. Tu es bien dans tes pantoufles. Tu ne veux rien changer. Tout va bien. Mais je sais quand même que ça peut être dangereux… »
> *Participante - 30 à 40 ans*

Les témoins et historiques de navigation

Beaucoup admettent ne pas supprimer assez souvent, selon eux, les témoins et les historiques de navigation sur leurs appareils. Et plusieurs le font sans être en mesure d'expliquer en quoi cela contribue à protéger leur vie privée en ligne.

> « I don't really know what the purpose, the benefit of deleting your browsing history is. Maybe there is one, I'm not sure. »
> *Participante - 30 à 40 ans*

Leur niveau de préoccupation en lien avec la publicité ciblée est plutôt modeste ; de même, les répondants associent peu la suppression des témoins et des historiques de navigation au profilage en ligne. En fait, nous constatons que plusieurs voient en ce comportement une manière de protéger leurs renseignements personnels (surtout leurs mots de passe) en cas de vol ou d'accès physique non autorisé à leurs appareils et semblent peu intéressés/préoccupés par l'utilisation qui peut être faite des témoins et de leur historique de navigation directement en ligne. À titre d'exemple, pas moins de trois répondants insistent qu'il n'est pas nécessaire pour eux de les supprimer puisqu'ils sont les seuls à utiliser leur appareil de connexion.

> « The two computers that I use most of the time, I'm the only one that uses them, so I'm not worried about anyone looking at my browsing history. »
> *Participant - 40 à 50 ans*

Et quelques participants suppriment les témoins et historiques de navigation pour de tout autres raisons que la protection de leur vie privée en ligne. Deux répondants ont déjà supprimé leur historique de navigation afin que leurs employeurs ou les autres membres de leur ménage ne sachent pas ce qu'ils avaient consulté. Un autre répondant supprime régulièrement les témoins de navigation afin de ne pas ralentir son ordinateur inutilement. Il ne voit pas en quoi cette pratique contribuerait à protéger sa vie privée en ligne.

Les transactions en ligne

Quelques répondants ne font pas ou que très peu d'achats ou de transactions en ligne, et ce, par manque d'intérêt, d'aisance et de confiance envers le commerce électronique ou par crainte de fournir leurs renseignements financiers à des entreprises malhonnêtes. En fait, les préoccupations relatives à la protection de la vie privée semblent être généralement subordonnées au caractère incertain des achats en ligne (vont-ils réellement recevoir le produit ?, sera-t-il en bon état ?, etc.).

Chez les autres répondants, les transactions bancaires et achats sont intégrés à leur quotidien en ligne, mais le mot d'ordre est la prudence. Et toutes les méthodes sont bonnes : la consultation de sites de grandes entreprises seulement, de sites HTTPS ou de sites référés par des proches ou qui font l'objet de commentaires positifs en ligne, l'utilisation du service *PayPal*, la fourniture des renseignements obligatoires seulement,

etc. Plusieurs répondants identifient Amazon comme un site de confiance sur lequel ils sont à l'aise de faire des achats sans craindre pour leurs renseignements personnels. À première vue, cela a de quoi surprendre vu les allégations passées contre l'entreprise[421]…

3.2.2.7 Les technologies d'amélioration de la confidentialité : intérêt modéré et méfiance

En fonction des préoccupations rapportées par les participants et des comportements de protection qu'ils avaient préalablement mentionnés, nous leur avons présenté quelques (autres, le cas échéant) outils d'amélioration de la confidentialité afin de mieux saisir leur intérêt potentiel à les utiliser et les craintes qu'ils pourraient avoir à leur sujet. Les questions sur ces outils étaient précédées d'une brève description de leur fonctionnement et de leurs avantages potentiels en termes de protection de la vie privée.

Soulignons que plusieurs participants d'âges variés ont semblé peu à l'aise avec le fait de discuter d'outils « plus techniques », affirmant ne pas les connaitre et ne pas les avoir déjà utilisés et doutant d'être en mesure de les utiliser.

> « C'est plus pour les personnes qui travaillent dans l'informatique, qui sont douées (…) Moi, je ne sais pas le faire »
> *Participant - 30 à 40 ans*

> « I'm just not really familiar with them. It's not that I would never use them, but I don't know enough about it to download one and use it »
> *Participante - 30 à 40 ans*

De manière générale, nous avons été surpris du faible intérêt des participants pour les outils qui leur ont été présentés, à l'exception du bloqueur de publicités. Nous constatons un haut niveau de méfiance envers le fonctionnement des autres outils présentés et leur capacité à protéger les renseignements personnels des usagers. Nous aborderons plus en détail les différents reproches des participants envers quelques outils présentés. Mentionnons simplement que l'expression « si c'est gratuit, vous êtes le produit » semble avoir marqué les esprits. Plusieurs se questionnent sur le financement des fournisseurs de ces outils gratuits. D'autres ne comprennent pas le choix de ces entreprises et semblent presque leur reprocher de ne pas exploiter pleinement leurs renseignements personnels comme le font toutes les autres, révélant involontairement à quel point ils ont pleinement internalisé les pratiques de l'industrie.

---

[421] Voir par exemple : MANANCOURT, V. « 'Millions of people's data is at risk' — Amazon insiders sound alarm over security », Politico, 24 février 2021, en ligne: https://www.politico.eu/article/data-at-risk-amazon-security-threat/ ; LYNKSEY, D. « 'Alexa, are you invading my privacy?' – the dark side of our voice assistants », The Guardian, 9 octobre 2019, en ligne: https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants ; HAY NEWMAN, L. « Amazon's Latest Gimmicks Are Pushing the Limits of Privacy », Wired, 11 octobre 2020, en ligne: https://www.wired.com/story/amazon-drone-camera-go-palm-data-privacy/

L'exemple des moteurs de recherches privés

Quelques participants seulement connaissent les moteurs de recherche privés. Plusieurs les confondent avec les navigateurs privés ou encore avec le mode de navigation privée sur les navigateurs.

Deux participants affirment initialement n'en avoir jamais utilisé avant de se raviser et de pointer leur utilisation passée des moteurs *DuckDuckGo* et *Ecosia*. Il faut dire que ces moteurs n'avaient pas été choisis (et utilisés) pour des raisons liées à la protection de ses renseignements personnels. Dans un cas, la participante s'était tournée vers DuckDuckGo, que son navigateur lui proposait parmi d'autres, un jour où elle trouvait Google trop lent. Dans l'autre cas, la participante a fait appel aux services d'*Ecosia* pour des raisons environnementales (l'entreprise contribue à la plantation d'arbres dans le monde). Si cette dernière ignorait qu'il s'agissait d'un moteur de recherche privé, elle était en mesure de fournir énormément de détails sur les démarches environnementales de l'entreprise allemande.

Une brève description des moteurs de recherche privés est fournie aux participants qui font aussitôt le parallèle avec Google. Une participante demande d'ailleurs si ces moteurs sont disponibles… sur Google !

De manière générale, les participants se montrent assez peu intéressés à utiliser des moteurs de recherche privés. Certains les ayant déjà utilisés affirment que ces moteurs de recherche sont moins efficaces, qu'ils offrent de moins bons résultats de recherche que Google.

> « I feel it brings up a lot of irrelevant search results. So, it's a little bit of extra work »
> *Participante - 30 à 40 ans*

Ceux qui n'ont jamais utilisé de moteurs de recherche privés se posent eux aussi des questions sur leur efficacité - un facteur qui semble donc déterminant dans l'adoption ou non de ce type d'outil.

> « I might be interested in using those, as long as they're effective. I mean it would depend on if they can give me the proper results. »
> *Participante - 60 à 70 ans*

> « I don't think I would use the private search engines, mostly because I find that even Yahoo or Bing aren't as efficient as Google"
> *Participante - 30 à 40 ans*

Au-delà de l'efficacité des moteurs de recherche privés, certains remettent en doute la description qui leur est faite des pratiques des moteurs de recherche privés en matière de traitements des renseignements personnels des usagers.

> « Est-ce que vraiment ça va me protéger ou on nous dit que ça va nous protéger, mais en arrière-plan, non ? »
> *Participant - 30 à 40 ans*

> « They have to make money somehow ! I'm just wondering how they are doing it."
> *Participant - 40 à 50 ans*

Enfin, certains participants concluent la discussion en reconnaissant qu'ils sont trop habitués à leur moteur de recherche actuel (surtout Google) et qu'ils ne peuvent s'imaginer le changer, même si la protection de leur vie privée en ligne s'en voyait améliorée.

L'exemple des gestionnaires de mots de passe

La plupart des participants à qui l'outil est présenté ne semblent pas particulièrement intéressés à utiliser un gestionnaire de mots de passe. Cette réaction est quelque peu surprenante considérant le sentiment généralisé qu'il est difficile de retenir tous les mots de passe aujourd'hui requis en ligne.

Quelques-uns souhaiteraient les utiliser, mais craignent d'oublier le (nouveau) mot de passe. D'autres sont vivement opposés à utiliser l'outil en raison d'une autre crainte : Qu'arrivera-t-il si le mot de passe du gestionnaire est piraté sur l'appareil de l'usager ou auprès de la compagnie ? Cette inquiétude est partagée par des consommateurs de tous les groupes d'âge consultés.

> « I would be wary about that. Passwords are the biggest things. To have a system that keeps them all in one place. I'm very wary of that. »
> *Participante - 30 à 40 ans*

> « Si tu mets ces mots de passe là dans le gestionnaire, il y a un tiers qui va le connaitre. C'est mieux de les garder pour soi. Il y a une personne quelque part qui pourrait y accéder sinon. »
> *Participant - 40 à 50 ans*

> « Je ne suis pas certain de vouloir utiliser ça parce que si eux autres me donnent un mot de passe, ils vont connaitre le mot passe eux aussi. Qu'est-ce qui me dit que ce mot de passe là, il n'est pas revendu à d'autres après ? Je ne sais pas. »
> *Participant - 60 à 70 ans*

Un participant propose la solution suivante afin d'utiliser l'outil dont il voit l'utilité malgré cette crainte : y mettre tous ses mots de passe, sauf ceux de ses comptes les plus importants (ex. : comptes bancaires).

Chez les quelques participants qui avaient déjà utilisé ou qui utilisent régulièrement un gestionnaire de mots de passe, les avis sont positifs, mais on reproche certaines limites aux outils comme leur coût et leur incompatibilité avec certains sites et plateformes.

L'exemple des adresses électroniques jetables

De manière, les adresses électroniques jetables ne soulèvent ni intérêt, ni inquiétude chez les consommateurs interviewés. Très peu de participants en connaissent l'existence. Aucun ne les utilise. Et quelques-uns à peine y voient une quelconque utilité potentielle.

En fait, plusieurs participants sont d'avis qu'ils agissent déjà similairement à ce que ferait l'outil, c'est-à-dire qu'ils ont plusieurs adresses électroniques dont certaines sont destinées

aux sites Web et concours susceptibles de les inonder de courriers électroniques indésirables par la suite.

> « I wouldn't say it's disposable, but I have one email that I use for those things, as opposed to my primary email »
> *Participante - 50 à 60 ans*

> « Moi, j'ai créé une adresse courriel justement pour quand il me demande une adresse, et que je n'ai pas le choix, pour visiter le site. (…) Et quand je reçois trop de courriels indésirables sur celle-là, je la ferme et j'en fais une autre (…) le moindrement qu'on me demande une adresse courriel pour rentrer sur un site, je donne une adresse que je sais qu'à un moment je vais fermer. »
> *Participant - 60 à 70 ans*

Un participant souligne aussi que ces adresses électroniques temporaires sont parfois identifiées et bloquées par les sites Web lorsqu'il tente de les utiliser.

L'exemple d'un bloqueur de publicités

Les bloqueurs de publicités se distinguent des autres outils présentés aux consommateurs interviewés en ce qu'ils sont plus connus et utilisés régulièrement par ces derniers. Par contre, nous notons que la plupart des utilisateurs ne considèrent pas que ces outils contribuent à protéger leur vie privée en ligne, ce qui souligne à nouveau les avis partagés sur l'intrusion ou non de la publicité ciblée dans la vie privée des internautes. Les répondants voient surtout les bloqueurs de publicités comme une manière de gérer le désagrément que représente ladite publicité.

> « Ça protège ta vie privée, oui et non. C'est juste des publicités. C'est juste fatigant. C'est juste agaçant. Dans mon cas, c'est surtout pour ça que je l'utilise… Comme ça il n'y a pas de *pop-up* ou de publicités qui apparaissent. »
> *Participante - 30 à 40 ans*

> « Je ne pense pas du tout que ça protège ma vie privée. Je pense juste que ça empêche les publicités d'apparaitre. »
> *Participant - 40 à 50 ans*

3.2.2.8 Un niveau de confiance surprenant

La forte majorité des répondants se disent confiants et satisfaits de la manière dont ils protègent actuellement leur vie privée en ligne

À peine six participants sur 30 se disent clairement insatisfaits et cinq autres hésitent à se dire pleinement satisfaits (« somewhat satisfied », « quand même assez satisfait »), conscients qu'ils pourraient théoriquement faire plus.

> « I'm doing as much as I could. I'm sure there are more ways I could be safer, but with the time commitment and financial situation, I feel I'm doing as much as I could. »

Participante - 40 à 50 ans

Ce résultat est surprenant considérant que plus de la moitié des répondants au sondage étaient d'avis qu'ils n'en faisaient pas suffisamment pour protéger leur vie privée en ligne.

Nous ne notons pas de corrélation entre la satisfaction des participants et leur niveau général de préoccupation pour la protection de leur vie privée en ligne. En fait, plusieurs répondants qui se disent satisfaits de la protection actuelle de leur vie privée en ligne ont fait des commentaires étonnamment cyniques sur l'état de leur vie privée en ligne au cours de l'entretien.

Il n'est pas possible pour nous de déterminer si les participants sont satisfaits parce qu'ils croient protéger adéquatement/suffisamment leurs renseignements en ligne ou parce qu'ils n'ont pas pour l'instant été victimes d'un incident touchant leurs renseignements personnels en ligne.

Peut-être sont-ils aussi satisfaits parce qu'ils croient faire tout ce qu'ils sont en mesure de faire en pratique. C'est d'ailleurs ce qui ressort des explications des consommateurs insatisfaits : ils souhaiteraient en faire davantage, mais ne pensent pas être capables. Et cette incapacité découle d'une multitude de facteurs :

> « I haven't implemented more, better protection measures, because I don't know what is available to me and I'm not that computer-savy. I'm not as knowledgeable as I wish I would be. I know that the basics are not enough. »
> *Participante - 30 à 40 ans*

> « There are always more expensive antivirus, anti phishing, softwares, upgrades to get by. I don't want to spent hundreds of dollars every year to do that. »
> *Participante - 40 à 50 ans*

> « I only have a limited data plan. So, if I keep downloading new apps, that wipes out all my monthly data. »
> *Participante - 40 à 50 ans*

> « My whole day would be spent reading privacy policies. »
> *Participante - 30 à 40 ans*

> « Dans la vie, être protégé à 100 %, c'est impossible. C'est sûr que quelqu'un qui est malveillant et qui est un pro va pouvoir me retracer quand même. Ces outils-là, c'est juste une parure. Vaut mieux le faire que ne pas le faire, mais… »
> *Participante - 30 à 40 ans*

3.2.2.9. Des pistes de solution très variées

Tous les répondants ont été questionnés sur la meilleure manière d'aider les consommateurs à protéger davantage leur vie privée en ligne. Leurs suggestions concernent trois types d'intervenants.

Pour les consommateurs

Les répondants semblent faire reposer la responsabilité de la protection de la vie privée en ligne avant tout sur les internautes eux-mêmes. Il reviendrait ainsi aux internautes de s'informer davantage sur les risques et d'adopter, après les recherches nécessaires, davantage de comportements de protection en ligne. S'ils faisaient preuve de clémence envers les limites de leur propre comportement (justifications basées sur le manque de temps ou de connaissances, par exemple), les répondants semblent plus sévères avec celles des autres.

> « An attitude shift is needed. Understanding what really needs to be private and what doesn't. [...] Basically, people are lazy. They don't think about this stuff. »
> *Participant - 40 à 50 ans*

Pour les gouvernements

La conscientisation et l'éducation des internautes sont soulevées par la majorité des répondants. Certains y voient une tâche qui revient exclusivement aux internautes, mais d'autres sont d'avis que le gouvernement et ses organismes devraient contribuer à l'exercice, notamment au moyen de formations offertes en classe et de vidéos ou de documents explicatifs largement diffusés.

L'amélioration des lois en matière de protection des renseignements personnels est, étonnamment, peu invoquée par les répondants, peut-être parce qu'ils en ignorent le contenu ou parce qu'ils doutent ultimement de son efficacité.

> « Legislations have loopholes and most corporations are very savvy to finding those loopholes. Even if there are no loopholes, we, as citizens, don't know if the rules are being followed. So I don't think legislation really helps. »
> *Participante - 30 à 40 ans*

Pour les entreprises

Nous notons que les répondants ont fait peu de suggestions d'amélioration de la protection de la vie privée en ligne relatives aux entreprises privées. Les grandes entreprises du Web, telles qu'Apple ou Google, ont pourtant une large influence sur l'évolution des pratiques de traitement des renseignements personnels en ligne, par leur capacité à influencer les législateurs et à diriger les pratiques d'entreprises qui dépendent largement d'elles pour l'accès aux données et leur exploitation. Le magazine américain Politico les a d'ailleurs récemment décrites comme les deux plus importants régulateurs en matière de vie privée en ligne au monde (« world's biggest privacy regulators »)[422].

[422] SCOTT, M et MANANCOURT, V. « Google and Apple are the world's biggest privacy regulators », Politico, 27 avril 2021, en ligne : https://www.politico.eu/article/google-apple-privacy-regulators-gdpr-floc/

Les répondants ne semblent pas forcément partager cet avis (ou en être conscients) ! Ils soulèvent tout de même quelques améliorations qu'ils souhaiteraient voir chez les entreprises, telles que l'utilisation plus répandue de la double authentification. D'autres voudraient voir, sur les sites Web qu'ils consultent, des avertissements plus clairs relativement aux politiques sur les renseignements personnels.

> « Not like in a tiny font in the terms and conditions that you don't read! Something kind of in your face: ok, this is what we're using. This why we're using it. We won't sell it to any other company, if something happens we will… »
> *Participante - 30 à 40 ans*

Enfin, d'autres se disent en faveur du développement d'outils d'amélioration de la confidentialité additionnels, mais admettent du même coup qu'il en existe déjà une bonne variété. L'utilité spécifique des outils additionnels demandés demeure floue. De manière générale, l'outil manquant protégerait contre tout, et ce, sans la moindre intervention de l'internaute…

> « A third party neutral type that would more or less kind of manage the privacy issues and not use it to their advantage »
> *Participant - 40 à 50 ans*

> « Some type of app or something that you can search that has everything bundled into one. »
> *Participant - 20 à 30 ans*

3.3 Quelques conclusions sur le sondage et les entrevues

3.3.1 Un niveau de préoccupation en hausse

Le niveau de préoccupation des internautes canadiens semble indéniablement en hausse par rapport aux années précédentes. Les internautes interrogés en 2020 dans le cadre de cette étude l'affirment presque unanimement. Et d'autres enquêtes réalisées auprès de Canadiens semblent confirmer la tendance observée.

Des sondages menés par le Commissariat à la protection de la vie privée du Canada dans les dernières années révèlent que le niveau de préoccupation pour la vie privée (en général, mais non spécifiquement en ligne) augmente de manière constante depuis 2012. 25 % des répondants se disaient énormément préoccupés par la question en 2012 contre 37 % en 2018[423]. Et le plus récent sondage du Center for International Governance Innovation évalue que le niveau de préoccupation pour la protection de la vie privée en ligne a augmenté entre 2018 et 2019 chez près d'un répondant canadien sur deux[424]. Il sera intéressant d'analyser les prochains sondages de ces organismes, menés pendant ou éventuellement après la pandémie de la COVID-19 qui a contribué à une utilisation accrue d'Internet. Certains experts se sont montrés particulièrement inquiets du fait que la

[423]COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉ DU CANADA. Sondage 2018-2019, *supra* note 158, figure 3.
[424] Sondage réalisé du 21 décembre 2018 au 10 février 2019 auprès de 25,229 d'internautes de 25 pays. Nous limiterons notre analyse aux résultats obtenus des 1000 répondants canadiens âgés de 18 à 64 ans : CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION. « Global Survey », supra note 99.

protection de la vie privée des internautes soit peu considérée par les dirigeants et les entreprises dans la gestion de la crise[425]. Les consommateurs partagent-ils cette crainte ?

Considérant les fuites de données survenues au Canada depuis la réalisation du sondage du Center for International Governance – dont celles de Desjardins et Capital One qui ont affecté bon nombre de Canadiens ou leurs proches - il apparait plausible que ce ne soit plus la moitié, mais bien la grande majorité des participants à nos entrevues qui évaluent leur niveau de préoccupation à la hausse par rapport à l'année précédente.

Notons par ailleurs que les sondages passés du Commissariat exposent eux aussi un clivage entre les résidents de certaines provinces canadiennes en matière de protection de la vie privée, notamment entre Québécois et les Britanno-colombiens[426]. Étant donné que ces sondages datent d'avant la fuite de Desjardins qui a particulièrement affecté le Québec, il faut conclure que le niveau de préoccupation particulièrement élevé des Québécois ne peut s'expliquer par ce seul fait.

3.3.2. L'ambivalence entourant les préoccupations non financières

Alors que les résultats du sondage font état d'un niveau de préoccupation élevé pour la réception de courriers électroniques indésirables et pour l'exposition à la publicité ciblée et à des comportements antisociaux en ligne, les résultats des entrevues sont moins convaincants. Très peu de répondants les évoquent spontanément et les réponses sont plutôt nonchalantes lorsque ces risques leur sont directement présentés. De manière générale, les consommateurs sont agacés, mais paraissent assez peu inquiets. Les seuls risques pour lesquels les réponses sont constantes dans le sondage et les entrevues sont ceux qui ont trait à la sécurité informatique ainsi qu'à l'accès et l'utilisation non autorisés des renseignements financiers des internautes. Le vol d'identité et ses conséquences sont sans contredit la préoccupation numéro un des Canadiens en matière de protection de la vie privée en ligne.

Comment concilier les résultats du sondage et des entrevues en ce qui concerne les autres risques possibles ? Nous avançons l'hypothèse que le terme « préoccupation » utilisé lors du sondage est associé autant à la peur qu'à l'agacement pour bon nombre de répondants. Le choix du terme y est possiblement pour quelque chose, mais le mode d'enquête peut l'être également. Une étude de Singleton et Harper sur les enquêtes guidées relatives à la

---

[425] MORISSON, S. « The year we gave up on privacy », Vox, 23 décembre 2020, en ligne : https://www.vox.com/recode/22189727/2020-pandemic-ruined-digital-privacy ; HO, S. « COVID-19 eroding global internet freedom, Canada among the most free, report says », CTV News, 14 octobre 2020, en ligne : https://www.ctvnews.ca/sci-tech/covid-19-eroding-global-internet-freedom-canada-among-the-most-free-report-says-1.5145180 ; SINGER, N. et SANG-HUN, C. « As Coronavirus Surveillance Escalates, Personal Privacy Plummets », New York Times, 23 mars 2020, en ligne : https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html ; VILLENEUVE, S. et ELIAS, D. « Surveillance Creep: Data collection and privacy in Canada during COVID-19 », Brookfield Institute, 2 septembre 2020, en ligne: https://brookfieldinstitute.ca/surveillance-creep-data-collection-and-privacy-in-canada-during-covid-19/

[426] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉ DU CANADA. Sondage 2018-2019, *supra* note 158 : « Comparativement aux répondants de la Colombie-Britannique, ceux de la région de l'Atlantique, du Québec et des Prairies sont plus susceptibles d'être préoccupés par la protection de leur vie privée ».

vie privée en ligne confirme qu'elles ont tendance à présenter des résultats plus alarmistes que celles auxquelles les personnes interviewées sont appelées à donner des réponses spontanées[427]. Il est plus aisé pour le répondant de dramatiser ses réponses lorsqu'on lui présente des questions fermées et des choix de réponse. Les auteurs réfèrent au phénomène du « talk is cheap ».

3.3.3 Une grande méconnaissance et un certain aveuglement volontaire

Les consommateurs interrogés sont nombreux à se dire impuissants à protéger leur vie privée en ligne en raison d'un manque de connaissances quant aux risques et aux mesures de protection adéquates. Et même lorsqu'ils affirment « connaître » un risque ou un outil offert, la confusion règne régulièrement en pratique.

Plus d'un cinquième des consommateurs sondés étaient incapables de répondre correctement à des questions très simples sur les pratiques de collecte et d'utilisation des renseignements personnels par les entreprises. L'étude spécifique au niveau de littératie des Canadiens en matière de vie privée réalisée par Rice et Bogdanov en 2019 arrive à des résultats plus alarmants encore :

> Many Canadians lack a basic awareness and understanding of how companies collect and use their personal data. Specifically, on 10 of the 16 statements, more than 60% of the respondents could not correctly identify how their data were being collected and used[428].

Les entrevues réalisées auprès de consommateurs montrent également des lacunes importantes en ce qui concerne les différents outils d'amélioration de la confidentialité disponibles gratuitement en ligne. À quoi servent-ils ? Quels sont les risques qu'ils peuvent aider à réduire ou éliminer ? Comment fonctionnent-ils ? Rares sont ceux qui sont en mesure de répondre à ces questions, ce qui peut expliquer, en partie, du moins, la faible utilisation de ces outils, malgré les recommandations d'experts.

Mais la méconnaissance laisse parfois place à l'aveuglement volontaire. Tout en admettant en savoir trop peu sur les risques pour leur vie privée en ligne, une proportion étonnamment élevée des participants aux entrevues se dit satisfaite de la manière dont ils se protègent contre lesdits risques et ils ont tendance à juger que les risques sont plus grands pour les autres que pour eux-mêmes. Des répondants plus jeunes s'inquiètent pour les internautes plus âgés qui seraient moins à l'aise avec les technologies. Des répondants plus âgés se disent inquiets pour les internautes plus jeunes qui divulgueraient trop de renseignements personnels en ligne. Conscients des risques pour les autres, plusieurs se croient à l'abri, alors qu'ils ne semblent prendre aucune mesure qui justifierait cette confiance.

---

[427] SINGLETON, S. M. et HARPER, J. « With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us », 11 février 2002, en ligne : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=299930
[428] RICE, M. D. et BOGDANOV, E. « Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices », Canadian Journal of Administrative Sciences, vol. 36, no. 2, 2019, p.166.

3.3.4 Des comportements difficiles à changer

Les répondants ont identifié différents comportements de protection adoptés au fil des ans pour protéger leur vie privée en ligne, dont le recours à un antivirus, qui semble bien intégré au mode de vie des internautes canadiens. Or, les résultats du sondage dressent un portrait plus positif de l'adoption des comportements par les internautes canadiens que les entrevues. Il est difficile de déterminer ce qui explique cet écart, mais il est permis de craindre que certains répondants au sondage aient embelli leur situation, surtout immédiatement après avoir répondu à une série de questions sur l'ampleur des risques pour leurs renseignements personnels en ligne.

De manière générale, nous constatons que les internautes adoptent un nombre assez restreint de comportements de protection en ligne. Et ils semblent relativement peu intéressés à modifier cette situation, même si plusieurs sont d'avis qu'ils « devraient » en faire plus. Au-delà du manque de connaissance relatif auxdits comportements, le sondage et les entrevues exposent un certain manque de volonté, un sentiment d'impuissance et un certain cynisme chez plusieurs répondants, qui a pour effet de les conforter dans leur comportement actuel.

3.3.5 Qu'en est-il du paradoxe de la vie privée ?

Nous avons abordé précédemment le débat entourant l'existence même d'un paradoxe de la vie privée en ligne (section 2.3). Rappelons que ce paradoxe peut être décrit comme une discordance entre les préoccupations des internautes et leur comportement, relativement aux questions de vie privée en ligne.

Or, comment établir si ce phénomène se manifeste chez les internautes canadiens sondés ? Il ne semble exister aucune méthodologie commune aux différentes études réalisées sur le sujet, dont les conclusions sont parfois contradictoires. Certains résultats de notre sondage, bien qu'ils soient à eux seuls non concluants, peuvent malgré tout nous indiquer certaines pistes. Ils seront brièvement présentés dans les pages qui suivent.

3.3.5.1 Le niveau de préoccupation générale et l'adoption de comportements de protection

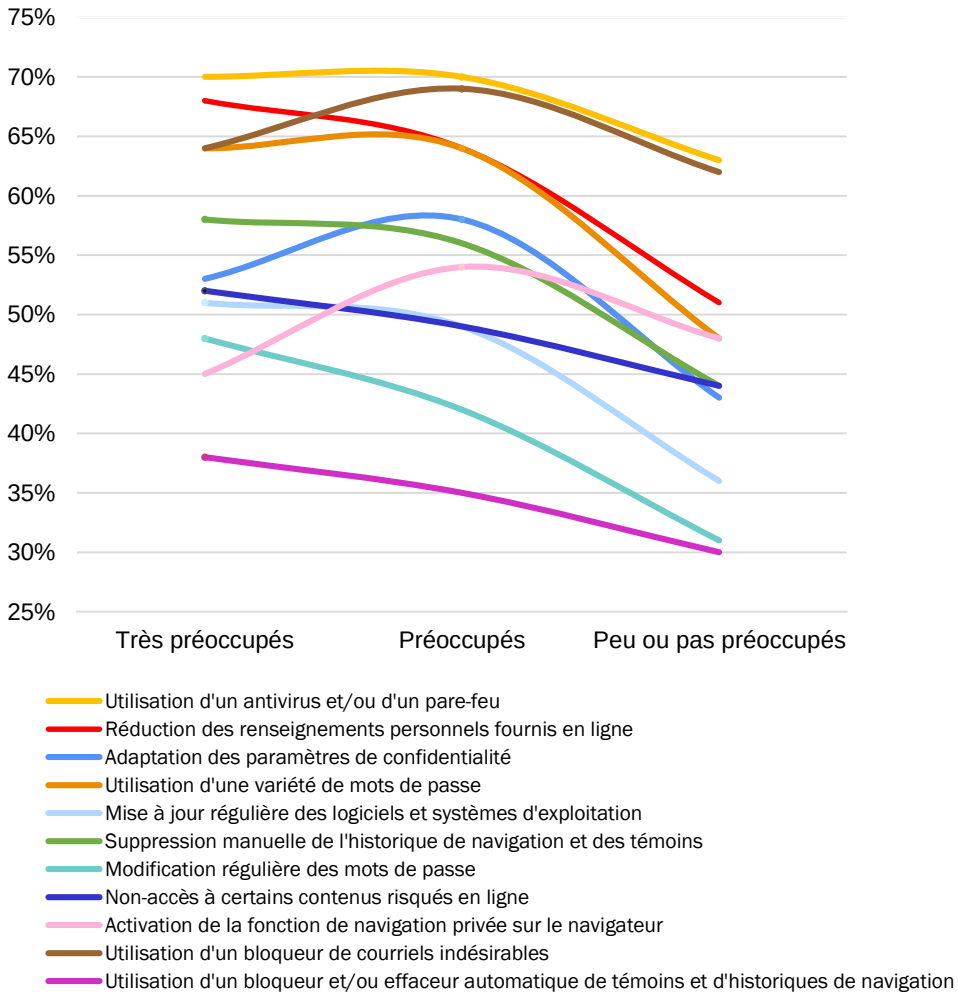
Nous constatons que le niveau de préoccupation pour la protection de la vie privée en ligne influence assez peu l'adoption de comportements destinés à réduire les risques d'atteintes à la vie privée en ligne. De manière générale, les répondants qui se déclarent très préoccupés par la protection de leur vie privée en ligne n'adoptent pas davantage de comportements de protection que ceux qui se disent moyennement préoccupés et à peine plus que ceux qui se disent pourtant peu ou pas préoccupés par le sujet (moins de 10 % d'écart en moyenne).

Le tableau ci-dessous illustre le pourcentage des répondants qui adoptent un comportement selon leur niveau général de préoccupation. On retiendra qu'il ne s'agit pas ici d'une analyse de l'efficacité des comportements de protection adoptés, mais seulement du nombre de comportements adoptés en fonction du niveau de préoccupation général exprimé.

Curieusement, on constate que certaines mesures de protection sont utilisées plus souvent par des répondants qui ne sont pas parmi les plus préoccupés par la protection de leur vie privée en ligne.

Tableau 13

L'adoption de comportements de protection de la vie privée en ligne, selon le niveau général de préoccupation



Un répondant est jugé « très préoccupé » par la protection de sa vie privée en ligne s'il a exprimé un niveau de préoccupation de 9 ou 10 sur 10. Un répondant est jugé « préoccupé » s'il a exprimé un niveau de préoccupation de 6 à 8 sur 10. Un répondant est jugé « peu ou pas préoccupé » s'il a exprimé un niveau de préoccupation de 5 et moins sur 10.

3.3.5.2 Le niveau de préoccupation spécifique à certains risques et l'adoption de comportements de protection spécifiques

Antivirus, mots de passe variés, bloqueur de pourriel et de publicité, etc. : on constatera que les mesures adoptées en plus grand nombre par les internautes sondés répondent à une variété de risques. Or, correspondent-elles aux risques spécifiquement identifiés par les répondants qui les emploient ?

Nous avons comparé l'adoption de certains comportements chez les répondants selon leur niveau de préoccupation pour certains risques spécifiques pour leur vie privée en ligne. Parmi la liste proposée aux répondants, les comportements analysés ci-dessous sont ceux qui sont le plus susceptibles de réduire les risques identifiés.

Nous constatons que les répondants qui sont plus préoccupés par certains risques prennent généralement davantage de mesures appropriées pour répondre à ces préoccupations, mais que, encore une fois, l'écart est relativement faible selon le niveau de préoccupation. Les plus grands écarts s'observent lorsqu'il est question des préoccupations relatives au piratage de renseignements personnels.

Tableau 14
L'adoption des comportements et outils de protection
selon le niveau de préoccupation spécifique à certains risques

Comportements	% des répondants qui adoptent le comportement selon leur niveau de préoccupation pour des risques spécifiques à leur vie privée en ligne*		
Risque de piratage des renseignements personnels			
	Très préoccupé	Préoccupé	Pas ou peu préoccupé
Utilisation d'un antivirus et/ou d'un pare-feu	73 %	64 %	53 %
Mise à jour régulière des logiciels et systèmes d'exploitation	51 %	43 %	37 %
Éviter certains contenus en ligne (courriels, hyperliens, sites Web, etc.)	52 %	53 %	42 %
Emploi de mots de passe différents pour la majorité des comptes en ligne	65 %	57 %	47 %
Modification régulière des mots de passe	43 %	40 %	35 %
Utilisation d'un gestionnaire de mots de passe	37 %	32 %	28 %

Utilisation de la double authentification	51 %	45 %	36 %
Risque de profilage à des fins d'exposition à de la publicité ciblée			
	Très préoccupé	Préoccupé	Pas ou peu préoccupé
Utilisation d'un bloqueur de publicités	58 %	62 %	60 %
Suppression manuelle de l'historique de navigation et des témoins	59 %	53 %	49 %
Utilisation d'un bloqueur ou effaceur automatique de témoins et d'historiques	40 %	34 %	29 %
Activation de la fonction de navigation privée sur le navigateur	48 %	52 %	51 %
Risque de réception de courriels indésirables			
	Très préoccupé[429]	Préoccupé	Pas ou peu préoccupé
Utilisation d'un bloqueur de pourriel	67 %	68 %	65 %
Utilisation d'adresses courriel temporaires	19 %	21 %	20 %

Les pourcentages sont arrondis à l'unité.

Nous constatons donc que le niveau général de préoccupation des répondants n'est pas forcément déterminant dans l'adoption de comportements de protection en ligne, sauf pour les internautes qui ne sont nullement préoccupés par la question. Ces derniers prennent systématiquement moins de mesures, bien que les écarts demeurent étonnamment faibles. Par contre, lorsqu'ils choisissent effectivement d'adopter certains comportements de protection pour leur vie privée en ligne, ces choix répondent à des craintes spécifiques et sont donc influencés par leurs préoccupations. Ce faisant, nous doutons qu'il existe une discordance complète entre les préoccupations des internautes pour leur vie privée en ligne et leur comportement réel en ligne, comme le veut la théorie du paradoxe de la vie privée.

[429] Un répondant est jugé « très préoccupé » s'il a exprimé un niveau de préoccupation de 9 ou 10 sur 10 à ce risque. Un répondant est jugé « préoccupé » s'il a exprimé un niveau de préoccupation de 6 à 8 sur 10. Un répondant est jugé « pas ou peu préoccupé » par un risque s'il a exprimé un niveau de préoccupation de 5 et moins sur 10.

L'ACCESSIBILITÉ DES TECHNOLOGIES D'AMÉLIORATION DE LA CONFIDENTIALITÉ

L'un des résultats les plus décevants du sondage et des entrevues réalisés en 2020 concerne la très faible connaissance et la rare utilisation des outils d'amélioration de la confidentialité par les internautes canadiens, et ce, alors même qu'ils sont fortement recommandés par les experts. Moins du tiers des répondants ont déjà utilisé un réseau virtuel privé, un moteur de recherche privé ou un navigateur privé par exemple. À l'exception des bloqueurs de pourriels et de publicités, les différents outils disponibles demeurent méconnus d'une part considérable de la population. Et lorsqu'ils sont discutés dans le cadre des entrevues, l'intérêt est plus que modeste. Plusieurs doutent être en mesure de pouvoir les utiliser, parce qu'ils manquent d'aisance avec les technologies ou parce qu'ils sont méfiants quant à l'utilité et à l'efficacité de ces outils.

À la lumière de ces résultats, il apparait pertinent d'analyser la manière dont les fournisseurs de ces outils présentent leurs produits et dans quelle mesure ils sont susceptibles de répondre, sur la seule base de la présentation qui en est faite, aux préoccupations des internautes canadiens. Précisons qu'il ne s'agit pas ici d'une étude du fonctionnement spécifique des outils ou de leur utilité réelle eu égard à la protection de la vie privée de leurs utilisateurs.

Nous nous attarderons aux présentations de sept types d'outils et à trois fournisseurs populaires pour chaque outil, afin de dresser un portrait des types de présentations existants et des possibles lacunes, le cas échéant, compte tenu des craintes face à ces outils identifiées chez les consommateurs.

Notons qu'un consommateur qui recherche les différents outils sur un moteur de recherche se verra également proposer quelques sites spécialisés et blogues (ex. : *PCMag*[430], *TechRadar*[431], *CNET*[432], etc.) qui offrent des explications sur les outils ou des comparaisons des différents produits offerts. Toutefois, aucune ressource ne se démarque particulièrement et il est fort probable qu'un consommateur clique éventuellement sur le site d'un fournisseur de l'outil recherché, en raison notamment des efforts d'optimisation du référencement par lesdits fournisseurs. Nous concentrons donc notre analyse sur la présentation des outils par ceux-ci.

[430] PCMAG. En ligne: https://www.pcmag.com/
[431] TECHRADAR. En ligne: https://www.techradar.com/
[432] CNET. En ligne : https://www.cnet.com/

4.1 Sommaire méthodologique

L'analyse de la présentation de la finalité et de l'usage des outils par les fournisseurs a été réalisée à l'aide d'une grille d'analyse qui s'inspire notamment des critères retenus par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) dans le cadre de son évaluation du marché des technologies d'amélioration de la confidentialité en ligne[433].

Nous avons accordé une importance particulière à la présentation et aux explications offertes par les fournisseurs en ce qui concerne les risques pour la vie privée en ligne, considérant les constats du consortium *PrimeLife* :

> Users often do not have a correct understanding of where (at what site) their personal data is stored and processed and to what entities their data is transferred. When designing and testing privacy-enhancing identity management systems, investigations are thus needed on how to evoke the correct mental models in users with regard to where what data are transmitted and under whose control the data are stored and processed. Having a comprehensive mental model will be essential for them to estimate privacy risks correctly, to understand better how far PETs can protect their online privacy[434].

En ce qui concerne la simplicité et la clarté du langage employé par les fournisseurs, nous nous sommes basés sur les travaux du gouvernement canadien en matière de « communications réussies » entre l'État et ses citoyens, dont plusieurs sont faiblement alphabétisés[435]. S'agissant d'outils informatiques qui, en plus, concernent la protection de la vie privée en ligne, nous sommes d'avis qu'il faut supposer un niveau de littératie relativement faible chez l'internaute moyen.

Les données ont été collectées sur les sites des fournisseurs sélectionnés et analysées au courant de l'hiver 2020-2021.

4.1.1 Commentaires généraux sur l'accessibilité de l'information

4.1.1.1 Un accès au français très inégal

Notre survol des sites Web à la recherche d'outils et d'information sur ces outils nous amène à un premier constat : l'offre est bien inférieure pour les internautes unilingues francophones. Plusieurs outils sont présentés exclusivement en anglais – le navigateur

---

[433] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. « PETs controls matrix - A systematic approach for assessing online and mobile privacy tools », 20 décembre 2016, pp.17 et 23-24, en ligne : https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools ; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. « PETs control matrix », annexe 1, en ligne : https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-control-matrix-annex-1-assessment-questionnaires (consulté le 15 janvier 2020).

[434] GRAF, C. *et al.*, dir, « Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project », PrimeLife HCI, 17 juin 2011, section 2.1.1.1.1, en ligne : http://primelife.ercim.eu/images/stories/deliverables/d4.1.6-towards_usable_pets-public.pdf

[435] GOUVERNEMENT DU CANADA. « Pour des communications réussies. L'alphabétisme et vous, trousse d'outils », mai 2003, sections 1 et 5, en ligne : http://publications.gc.ca/collections/Collection/PF4-16-2003F.pdf

privé Epic et le bloqueur de suivi Privacy Badger, notamment – et d'autres ont bien souvent un site Web partiellement bilingue seulement. Ce sont malheureusement les sections d'aide sur les pages secondaires desdits sites Web (pages qui contiennent par exemple des tutoriels, foires aux questions, etc.) qui échappent généralement à la traduction. Il s'agit pourtant de renseignements dont le consommateur aurait bien eu besoin. C'est dans ces pages qu'on trouve le plus souvent les explications qui complètent les phrases accrocheuses, mais vagues qui figurent sur la page d'accueil de certains fournisseurs. Plusieurs blogues offerts sur les sites des outils sont eux aussi unilingues. Ces blogues ne concernent généralement pas directement l'outil offert, mais permettent aux internautes de prendre connaissance d'enjeux qui affectent leur vie privée en ligne (risques, développement législatif, etc.).

Rappelons qu'un peu moins du quart de la population canadienne a le français comme première langue parlée[436]. Et un nombre significatif d'entre eux ne maitrise pas l'anglais. C'est le cas notamment de près de 60 % des Québécois. Il est regrettable d'observer cette barrière linguistique dans l'introduction aux technologies d'amélioration de la confidentialité en ligne, d'autant que les résultats de notre sondage tendent à démontrer une connaissance généralement inférieure des outils chez les répondants francophones.

À l'exception des bloqueurs ou effaceurs de témoins et d'historique de navigation, tous les autres outils présentés dans le cadre du sondage sont moins connus des répondants francophones qu'anglophones. L'écart est de 10 % en moyenne.

4.1.1.2 Un langage parfois complexe, malgré des efforts indéniables

Au-delà des langues dans lesquelles l'information est diffusée, la complexité des termes employés varie grandement selon les fournisseurs et les outils étudiés.

Quelques fournisseurs d'outils portent clairement une attention particulière à la clarté de l'information véhiculée. Ils la présentent au moyen de tableaux explicatifs ou accompagnée de supports visuels ou d'exemples. Ils tentent de définir les termes plus techniques employés dans la documentation en ligne, en incluant, par exemple, un hyperlien vers une autre page du site Web ou une ressource externe (ex. : article de média) ou au moyen d'une fenêtre modale sur laquelle le consommateur peut cliquer pour une définition ou des explications du terme en gras ou souligné.

La quantité de termes définis varie considérablement d'un fournisseur à l'autre ; les moteurs de recherche privés et les antivirus se démarquent toutefois par la simplicité du langage employé. Chez les autres, le choix des termes définis, le cas échéant, laisse parfois perplexe. Yopmail, un fournisseur d'adresses courriel jetables, définit par exemple ce qu'est le « spam », mais pas ce que sont les « plugins de recherche » ou « widgets » que l'internaute pourrait télécharger. Nous serions portés à croire que l'inverse aurait été plus

[436] GOUVERNEMENT DU CANADA. « Statistiques sur les langues officielles au Canada », en ligne : https://www.canada.ca/fr/patrimoine-canadien/services/langues-officielles-bilinguisme/publications/statistique.html (consulté le 14 mars 2021).

utile au consommateur moyen, vraisemblablement aux faits du phénomène des pourriels, mais moins à l'aise avec les éléments plus techniques de son navigateur.

4.1.1.3 Des ressources d'aide variées

Les efforts de certains fournisseurs en vue d'informer clairement et simplement les internautes au sujet des outils et de la protection de la vie privée en ligne se reflètent aussi dans la variété des services d'aide et d'information offerts aux usagers. Services de clavardage automatisés, infolettres, forums de discussion, balados ou émissions[437], etc. : les fournisseurs font preuve de créativité dans la diffusion de l'information. C'est tout particulièrement le cas pour les fournisseurs de services pour lesquelles le consommateur devra généralement payer (antivirus, VPN et gestionnaires de mots de passe).

Tableau 15
Les types de ressources d'aide disponibles par les fournisseurs
selon le type d'outils d'amélioration de la confidentialité en ligne offerts

Types d'outils d'amélioration de la confidentialité en ligne	Types de ressources d'aide et d'information offertes sur les sites Web étudiés				
	Foire aux questions	Assistant virtuel ou service d'aide individuel	Forum ou communauté	Blogue	Infolettre
Antivirus	✓✓✓	✓✓	✓✓✓	✓✓✓	✓✓✓
Réseaux privés virtuels (VPN)	✓✓✓	✓✓✓	✓	✓✓✓	✓
Gestionnaires de mots de passe	✓	✓✓	✓✓	✓✓✓	✓✓
Navigateurs privés	✓✓✓		✓✓	✓✓✓	✓
Moteurs de recherche privés	✓✓		✓	✓✓✓	✓✓
Bloqueur de publicités et de suivi	✓✓✓		✓	✓✓	
Adresses électroniques jetables	✓			✓	

* Les sites Web de 21 fournisseurs ont été étudiés au total, soit trois pour chaque type d'outils d'amélioration de la confidentialité en ligne retenus.

Précisons néanmoins que dans certains cas, ces services étaient difficiles à trouver sur les sites Web. De même, ce tableau ne distingue pas la qualité et la quantité de l'information disponible sur les blogues et foires aux questions. Certains blogues, par exemple, contiennent plus d'une centaine de publications, alors que d'autres ne contiennent que quelques liens utiles. Même constat pour les foires aux questions des sites étudiés ;

[437] Voir par exemple : MCAFEE. « Hackable? Podcast », en ligne : https://hackablepodcast.com/episodes ; AVAST. « Garry on lockdown », en ligne : https://blog.avast.com/garry-on-lockdown-episode-1-avast

certaines ne couvrent que très peu d'éléments (installation ou politique de confidentialité par exemple).

4.1.1.4 Une certaine incohérence

Sur une note moins positive, nous constatons avec déception que la collecte et l'utilisation des renseignements personnels des internautes qui consultent les sites Web des outils sont répandues. Plusieurs affichent par exemple des avis relatifs aux témoins de navigation dont les témoins non essentiels sont précochés pour approbation. Ironiquement, c'est notamment le cas d'Adblock Plus, un outil de blocage du suivi en ligne ! Si cette pratique n'est pas nécessairement interdite au Canada (contrairement à l'Union européenne[438]), elle parait tout de même difficilement conciliable avec la mission de ces outils, soit l'amélioration de la protection de la vie privée en ligne de leurs usagers. La lecture des politiques de confidentialité de certains sites Web fait également sourciller.

4.2 Les moteurs de recherche privés

Pour l'étude de la présentation des moteurs de recherche privés, nous avons retenu les trois grands fournisseurs DuckDuckGo, StartPage et Qwant[439]. Notons que DuckDuckGo est sans contredit le moteur de recherche privé le plus populaire. En 2019, il réalisait 50 millions de recherches chaque jour[440]. Il fait maintenant partie des moteurs de recherche disponibles par défaut sur le navigateur Chrome[441]. Qwant a, quant à lui, reçu un sérieux coup de pouce de la part du gouvernement français ; il est depuis 2019, le moteur de recherche par défaut sur tous les appareils des employés de l'État[442].

4.2.1 Présentation de la finalité

Deux des trois moteurs de recherche étudiés offraient directement sur leur page Web d'accueil, sous l'encadré de recherche, des renseignements sur les avantages pour la protection de la vie privée que procure l'outil.

---

[438] LOMAS, N. « Europe's top court says active consent is needed for tracking cookies », Techcrunch, 1er octobre 2019, en ligne : https://techcrunch.com/2019/10/01/europes-top-court-says-active-consent-is-needed-for-tracking-cookies/

[439] STEWART, C. « The Best Private Search Engines — Alternatives to Google », Hackernoon, 8 février 2018, en ligne : https://hackernoon.com/untraceable-search-engines-alternatives-to-google-811b09d5a873

[440] DUCKDUCKGO. Publication sur Twitter, 6 novembre 2019, en ligne : https://twitter.com/DuckDuckGo/status/1192079712379494406

[441] ZHOU, M. « DuckDuckGo is now a default search engine option in Chrome », CNET, 14 mars 2019, en ligne : https://www.cnet.com/news/duckduckgo-is-now-a-default-search-engine-option-in-chrome/ ; LOMAS, N. « Google has quietly added DuckDuckGo as a search engine option for Chrome users in ~60 markets », Techcrunch, 13 mars 2019, en ligne : https://techcrunch.com/2019/03/13/google-has-quietly-added-duckduckgo-as-a-search-engine-option-for-chrome-users-in-60-markets/

[442] « France is bidding adieu to Google in favor of a more private search engine », ExpressVPN, 7 août 2019, en ligne : https://www.expressvpn.com/blog/google-france-qwant-privacy/

Prenons l'exemple de la page d'accueil du site Web de DuckDuckGo, qui indique ceci :

> Vos données ne devraient pas être vendues.
> [...] Pas de pistage, pas de ciblage publicitaire, juste de la recherche.

On y mentionne clairement et simplement les risques évités, soit la vente de renseignements à des tiers, le profilage et l'exposition à de la publicité comportementale. On réfère également à plusieurs reprises à l'historique de recherche, soit les renseignements personnels que protège l'outil. En consultant – même sommairement – le site Web du fournisseur, un internaute trouverait donc facilement réponse aux questions *qui*, *quoi* et *pourquoi*.

Qwant fait bande à part en n'offrant sur sa page d'accueil aucun détail sur l'utilité de son service. Seul le *slogan* « Le moteur de recherche qui respecte votre vie privée » figure sous le logo du moteur de recherche. Afin de se renseigner sur ce qu'apporte concrètement l'outil à la protection de sa vie privée, un internaute devra cliquer sur le titre « à propos », relativement peu visible dans le coin droit de la page au côté des services de recherche musicale et géographique. Même sur sa page « à propos », on trouve relativement peu d'information sur l'utilité de Qwant ou de manière plus générale, d'un moteur de recherche privé.

Il est malheureux qu'un internaute doive cliquer sur deux autres liens[443] afin d'accéder à une réelle explication des risques des moteurs de recherche « commerciaux » pour sa vie privée en ligne. L'excellente explication de Qwant, dont il risque peu de prendre connaissance, aurait mérité une bien plus grande visibilité :

> Vous dites tout de vous à votre moteur de recherche, lorsque vous lui posez des questions tous les jours : là où vous souhaitez aller, ce que vous voulez cuisiner, les symptômes ou traitements de votre éventuelle maladie, votre sexualité, votre religion, vos projets d'investissements, votre niveau de revenus, votre profession, vos sports préférés, les films que vous allez voir... la liste des questions intimes et commercialement exploitables est infinie, et souvent ces recherches sont stockées, analysées, et revendues directement ou indirectement.
>
> [...] vous pouvez utiliser Qwant en toute confiance, nous ne tenterons jamais d'établir votre profil psychologique ou commercial pour le revendre à des annonceurs, ici ou ailleurs.

Nous notons aussi avec intérêt la mise en garde présente sur le site Web de StartPage quant aux limites d'un moteur de recherche privé pour la protection de la vie privée en ligne. Sur la page d'accueil du site Web du fournisseur, on trouve l'avertissement suivant :

> En cliquant sur les résultats d'une recherche, vous quittez la protection de Startpage.com, ce qui entraîne l'installation d'un barrage de cookies sur votre appareil.

Si cet avertissement vise avant tout à diriger les consommateurs vers l'autre service de Startpage, son « mode anonyme » de navigation, il demeure positif de voir cette clarification importante mise bien en évidence par le fournisseur. Les consommateurs doivent être informés des limites de l'outil et ne pas croire à tort qu'il n'existe plus de risques de suivi

[443] Après avoir accéder à la page « à propos » du site Web de Qwant, l'internaute devra cliquer sur le titre « Centre d'aide » et ultimement sur le titre au bas de cette page « Notre philosophie ».

et de profilage ou d'exposition à de la publicité comportementale lors de leur navigation en ligne. En l'absence d'explications sur le sujet, les phrases accrocheuses des fournisseurs étudiés pourraient en induire certains en erreur : « pas de pistage, pas de ciblage publicitaire », « un moteur de recherche [...] qui veille au respect des droits et libertés des utilisateurs », etc.

4.2.2 Présentation de l'usage

Rares sont les internautes canadiens qui n'ont jamais eu recours à Google, Yahoo ou un autre moteur de recherche. Des explications sur les fonctions de base de ce type d'outil sont donc moins nécessaires.

La seule référence évidente au fonctionnement du moteur de recherche se trouve sur la page d'accueil du site Web de StartPage qui mentionne utiliser les résultats de recherche de Google, moyennant rémunération, et supprimer tous les « trackers » des résultats de recherche avant de les transmettre à ses propres utilisateurs.

4.3 Les réseaux privés virtuels

Afin d'étudier la présentation que font les réseaux virtuels privés, nous avons retenu les trois fournisseurs suivants : NordVPN, ExpressVPN et Hide.me. Couramment nommés parmi les fournisseurs les plus populaires[444], NordVPN et ExpressVPN offrent un service payant, allant de 8 à 13 $US par mois selon les forfaits alors que Hide.me offre une version gratuite du service (limite de 2 Go de téléchargement) en plus de sa version payante.

4.3.1 Présentation de la finalité

De manière générale, nous constatons que deux finalités sont mises de l'avant par les fournisseurs sur la page d'accueil de leur site Web respectif : la protection des renseignements personnels en ligne et le contournement du géoblocage (soit les restrictions régionales à l'accès à certains contenus).

ExpressVPN insiste davantage que ses concurrents sur le contournement de la censure et des restrictions de contenu. En fait, le fournisseur ne fait même pas expressément mention de la protection des données dans la description des fonctionnalités de base de l'outil qui apparait sur la page Web dédiée à ce sujet. On y mentionne la navigation anonyme et le

[444] GROM, E. « The Popularity Of VPNs Is On The Rise », VPNBase, 9 avril 2019, en ligne : https://vpnbase.com/blog/popularity-of-vpns-is-on-rise/ ; SIMMONS, J. H. « Most Downloaded VPN Apps for Android (Big List Inside!) », VPNCrew, données en date du 15 janvier 2019, en ligne : https://www.vpncrew.com/most-downloaded-vpn-apps-for-android/ ; RIVINGTON, J. « The Best VPN Service 2019 », Tom's Guide, 2 octobre 2019, en ligne : https://www.tomsguide.com/best-picks/best-vpn ; LAUKKONEN, J. « The 8 Best Free VPN Services of 2019 », Lifewire, 23 octobre 2019, en ligne : https://www.lifewire.com/best-free-vpn-services-818192

masquage d'adresse IP, mais sans jamais expliquer en quoi ces procédés aident à la protection de la vie privée en ligne. Le consommateur trouvera réponse à cette question sur une autre page entièrement dédiée aux enjeux de confidentialité. Il est dommage que l'information ait été ainsi scindée.

Plus facilement compréhensible pour l'internaute moyen, Hide.me aborde l'anonymisation de l'adresse IP en exposant directement au lecteur la vulnérabilité que vise à corriger l'outil. On y présente en effet à l'usager son adresse IP, suivie des énoncés suivants :

> Si nous pouvons voir votre vraie identité et localisation, tout le monde peut aussi les voir.
>
> Vous êtes surveillés. Sans VPN, les sites que vous visitez ont accès à votre vraie IP et localisation. Votre FAI [Fournisseur d'accès Internet] sait quels sites vous visitez, à qui vous envoyez des courriels, et aussi ce que vous téléchargez. Non seulement votre activité en ligne est conservée, mais elle l'est sous votre nom.

Contrairement aux autres outils étudiés, les fournisseurs de réseaux privés virtuels accordent une grande place aux risques pour la vie privée des leurs abonnés que présentent les fournisseurs d'accès Internet eux-mêmes. En plus des renseignements relatifs aux activités de navigation qui sont conservés et parfois vendus par les fournisseurs d'accès Internet, on y souligne leur manque de transparence et leurs obligations en matière de droits auteurs. Hide.me accompagne par exemple la présentation de son outil d'un tableau énumérant les lois de quelques pays, dont le Canada, relativement à la conservation de registres d'activité par les fournisseurs d'accès Internet.

4.3.2 Présentation de l'usage

Le fonctionnement des réseaux privés virtuels est techniquement plus complexe que celui de bien d'autres outils étudiés. La clarté des explications fournies est donc d'autant plus importante.

Une section du site Web de chaque fournisseur est dédiée à expliquer ce qu'est un réseau privé virtuel et à vulgariser des concepts complexes comme le chiffrement et le protocole VPN. Tous utilisent l'image du tunnel et ont recours à des illustrations qui s'appuient sur cette analogie.

Mais malgré des efforts indéniables pour simplifier les explications, les présentations du fonctionnement de ce type d'outil demeurent un peu techniques et le contenu complexe. Et il est peu probable qu'un internaute moyen en comprenne toutes les subtilités. L'explication de NordVPN est la plus complète, mais également la moins facilement compréhensible :

> Lorsque vous vous connectez à un service VPN, il crée un « tunnel » chiffré sur Internet. Cela permet de sécuriser les données qui circulent entre vous et votre destination, qu'il s'agisse d'un moteur de recherche ou d'un compte bancaire en ligne.
>
> Ce tunnel est créé en authentifiant d'abord votre client auprès d'un serveur VPN. Le serveur applique ensuite un protocole de cryptage à toutes les données que vous envoyez et recevez.

Pour garantir la sécurité de chaque paquet de données, un VPN l'enveloppe dans un paquet externe, qui est ensuite crypté par encapsulation. Il protège les données pendant le transfert et constitue l'élément central du tunnel VPN. Lorsque les données arrivent sur le serveur, le paquet externe est supprimé via un processus de décryptage.

Illustration 1

Illustration schématique d'ExpressVPN du fonctionnement d'un réseau privé virtuel

Source : https://www.expressvpn.com/fr/what-is-vpn#comment-%c3%a7a-marche

Deux fournisseurs présentent aussi des vidéos qui font à la fois la promotion de leurs produits et la vulgarisation de leur fonctionnement[445]. Les sites Web étudiés présentent également des schémas d'utilisation en trois étapes, qui consistent grossièrement à installer l'application, activer la protection et choisir un serveur particulier, si désiré. Les explications relatives à l'utilisation de l'outil par l'internaute, plus simples certes, sont particulièrement bien réussies.

Un internaute qui consulte le site Web d'un fournisseur de réseaux privés virtuels devrait donc ressortir de cette expérience avec une compréhension générale modeste du fonctionnement de l'outil, mais une bonne idée de la manière dont l'outil peut être utilisé et de qui et de quoi il protège.

[445] ExpressVPN a également une chaine YouTube qui contient plusieurs vidéos de vulgarisation : https://www.youtube.com/channel/UCFzUH6rnGYqJD6EexQSdVhw (visitée le 2 mars 2021).

4.4 Les navigateurs privés

Nous avons retenu l'étude des trois navigateurs privés gratuits Tor, Brave et Epic en raison de leur popularité et de leur approche distincte en matière d'anonymisation.

4.4.1 Présentation de la finalité

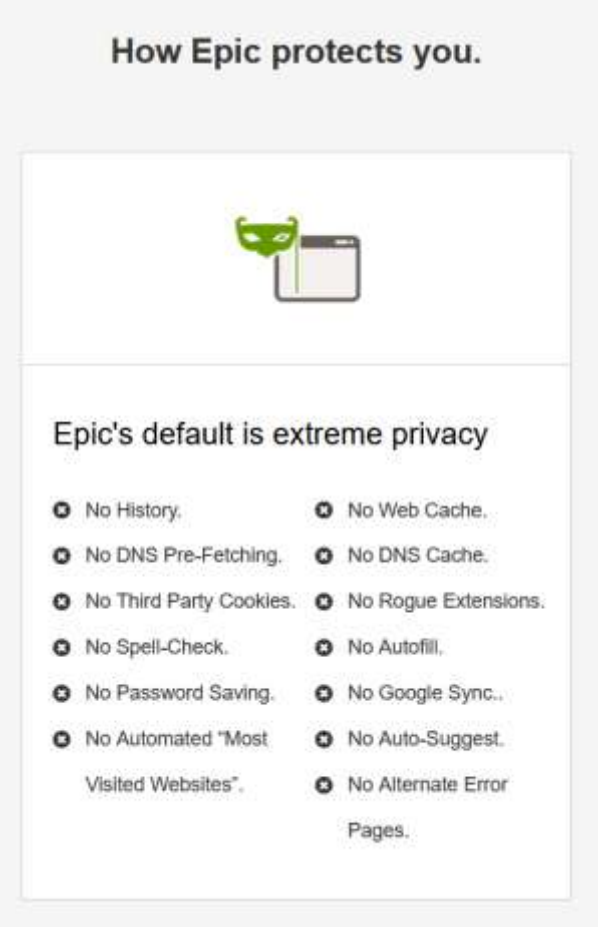
Dans cette catégorie d'outils, l'expérience du consommateur varie grandement d'un site Web à l'autre. La présentation de Tor et d'Epic, par exemple, est axée sur la protection de la vie privée en ligne tandis que celle Brave tempère cet objectif avec d'autres considérations comme la vitesse de la navigation.

Ainsi, la page d'accueil de Brave ne met pas particulièrement l'accent sur la protection de la vie privée. On y trouve des expressions accrocheuses telles que « un meilleur Internet » et une « réimagination » [sic] du navigateur Web. En cherchant à présenter son produit comme une version améliorée des navigateurs traditionnels, Brave relègue la protection de la vie privée au second plan, au côté de la vitesse et la sécurité, sans plus.

Afin d'obtenir des explications sur la plus-value de l'outil en regard de la protection des renseignements personnels en ligne, le consommateur doit parcourir une page secondaire qui détaille les fonctionnalités de l'outil. Mais là encore, ces explications se retrouvent sous celles relatives à la vitesse de téléchargement et au programme de fidélisation *Brave Rewards*. On trouve ainsi une liste très complète, quoiqu'un peu technique, des fonctionnalités de l'outil, qui mentionne entre autres les éléments suivants : *prévention de la prise d'empreintes digitales, contrôle des témoins, mise à niveau HTTPS, effacer les données de navigation, fenêtres privées*, etc. Notons que les fonctionnalités mentionnées ne sont pas accompagnées d'explications ou de définitions, ce qui en rend la compréhension passablement difficile. Il est irréaliste de penser qu'un consommateur moyen sait ce que sont le blocage d'un script ou encore la configuration d'un bouclier global !

Le site Web d'Epic présente un problème similaire, bien qu'il mette davantage l'accent sur la protection de la vie privée en ligne sur sa page d'accueil. Les exemples présentés sur la page d'accueil ne sont pas définis (ex. : *fingerprinting, ultrasound signaling,* etc.). Et la page Web qui traite spécifiquement des fonctionnalités de l'outil offre plus de détails, mais malheureusement pas plus d'explications, tel qu'il appert de l'extrait suivant :

Illustration 2
Extrait d'une page du site Web d'Epic relative aux fonctionnalités de l'outil



Source : https://www.epicbrowser.com/our-key-features.html

La page Web du navigateur privé Tor se démarque de celles des deux autres outils étudiés, en ce que le lecteur a accès à des explications relativement simples sur l'utilité de l'outil en regard de la protection de ses renseignements personnels, et ce, directement sur la page d'accueil. Sous la phrase accrocheuse « Défendez-vous contre le suivi à la trace et la surveillance », on trouve de courts paragraphes qui abordent différents éléments clés de la protection qu'offre l'outil, le tout accompagné d'images ludiques.

Illustration 3
Extrait de la page d'accueil du site Web de Tor

BLOQUER LES TRAQUEURS

Le Navigateur Tor isole chaque site Web que vous visitez afin que les traqueurs tiers et les publicités ne puissent pas vous suivre. Tous les témoins sont automatiquement effacés une fois la navigation terminée. Il en sera de même pour votre historique de navigation.

DÉFENDRE CONTRE LA SURVEILLANCE

Le Navigateur Tor empêche quiconque surveille votre connexion de savoir quels sites Web vous visitez. Tout ce que quelqu'un qui surveille vos habitudes de navigation peut voir est que vous utilisez Tor.

RÉSISTER AU PISTAGE PAR EMPREINTE NUMÉRIQUE UNIQUE

Le Navigateur Tor vise à rendre tous les utilisateurs semblables en apparence, afin qu'il soit plus difficile de vous suivre d'après l'empreinte numérique unique de votre navigateur et les renseignements de votre appareil.

Source : https://www.torproject.org/fr/

Un consommateur technophile qui serait déçu par l'absence de détails à première vue pourra se tourner vers d'autres sections du site Web de Tor, qui offre une quantité impressionnante d'explications, d'hyperliens et d'autres ressources utiles.

Mentionnons aussi que la page d'accueil d'Epic souligne les risques de suivi en ligne qui demeurent présents lors de l'emploi d'un réseau privé virtuel ou de l'activation du mode de navigation incognito sur les navigateurs traditionnels. Même si cette mise en garde vise avant tout à convertir des utilisateurs à l'utilisation de son outil, il est intéressant de voir ce type d'avertissement aussi visiblement relayé aux consommateurs, qui bien souvent ne distinguent pas pleinement l'utilité (et les limites) des différentes technologies d'amélioration de la confidentialité.

4.4.2 Présentation de l'usage

Les sites Web des navigateurs observés sont peu descriptifs quant aux fonctionnalités de base de leurs produits, ce qui se justifie par la familiarité qu'ont les internautes avec l'usage d'un navigateur, un élément essentiel à toute navigation en ligne…

4.5 Les bloqueurs de publicités et de suivi en ligne

Nous avons choisi trois bloqueurs de publicités parmi les plus populaires, soit Adblock Plus, Privacy Badger et Ghostery. Tous prennent la forme d'une extension de navigateur et sont au moins disponibles pour les navigateurs Firefox, Chrome et Opera.

4.5.1 Présentation de la finalité

D'emblée, nous constatons qu'Adblock Plus met très peu l'accent, sur son site Web, sur la protection de la vie privée en ligne. Il faut dire qu'il s'agit avant tout d'un outil de blocage de publicités, dont les fonctions de blocage du suivi en ligne paraissent secondaires. Nous supposons que, comme beaucoup des Canadiens sondés dans notre étude, les créateurs de l'outil considèrent que la publicité personnalisée en ligne est davantage un désagrément qu'une atteinte à la vie privée.

Adblock Plus insiste ainsi expressément sur le caractère agaçant des publicités et sur leur effet sur la vitesse de navigation des internautes (à qui on promet une expérience Web plus épurée et plus rapide). Les références au blocage de suivi, qui ne se trouvent qu'à la page « à propos », auraient mérité un peu plus de visibilité, notamment cette remarque sur la pertinence de bloquer les publicités en ligne à des fins de protection des renseignements personnels :

> De nombreuses publicités comportent des dispositifs de suivi intégrés et certaines peuvent même contenir des malwares.

La protection de la vie privée en ligne est davantage au centre de la présentation chez les deux autres fournisseurs. On trouve une mention relative au blocage des dispositifs de suivi des internautes sur la page d'accueil des deux outils.

L'explication plus complète du fonctionnement de Privacy Badger est particulièrement facile à saisir pour un internaute moins à l'aise avec le numérique :

> When you view a webpage, that page will often be made up of content from many different sources. (For example, a news webpage might load the actual article from the news company, ads from an ad company, and the comments section from a different company that's been contracted out to provide that service.) Privacy Badger keeps track of all of this. If as you browse the web, the same source seems to be tracking your browser across different websites, then Privacy Badger springs into action, telling your browser not to load any more content from that source. And when your browser stops loading content from a source, that source can no longer track you. Voilà !

Nous notons que, contrairement aux deux autres outils étudiés, Privacy Badger ne fait aucune mention d'autres considérations, comme la vitesse de navigation ou le visuel des pages Web remplies de publicités. La seule finalité mentionnée concerne la protection de la vie privée en ligne. On y distingue d'ailleurs l'outil d'un simple bloqueur de publicités :

> Because Privacy Badger is primarily a privacy tool, not an ad blocker. Our aim is not to block ads, but to prevent non-consensual invasions of people's privacy because we believe they are inherently objectionable. We also want to create incentives for advertising companies to do the right thing.

L'absence de ces « arguments de vente » s'explique possiblement par le caractère non lucratif de son développeur, l'Electronic Frontier Foundation. La mission de l'organisme explique aussi le côté très pédagogique du site Web de Privacy Badger qui présente, sur sa page d'accueil, une longue série de questions et réponses relatives au fonctionnement de l'outil et à sa manière de protéger les renseignements personnels en ligne : « Does Privacy Badger prevent fingerprinting? », « Does Privacy Badger still work when blocking third-party cookies in the browser? », « Why does Privacy Badger block ads? », etc. Les explications fournies sont simples et facilement compréhensibles pour un internaute peu technophile, notamment parce que les éléments plus techniques sont tous définis et même souvent accompagnés d'hyperliens pour des explications additionnelles.

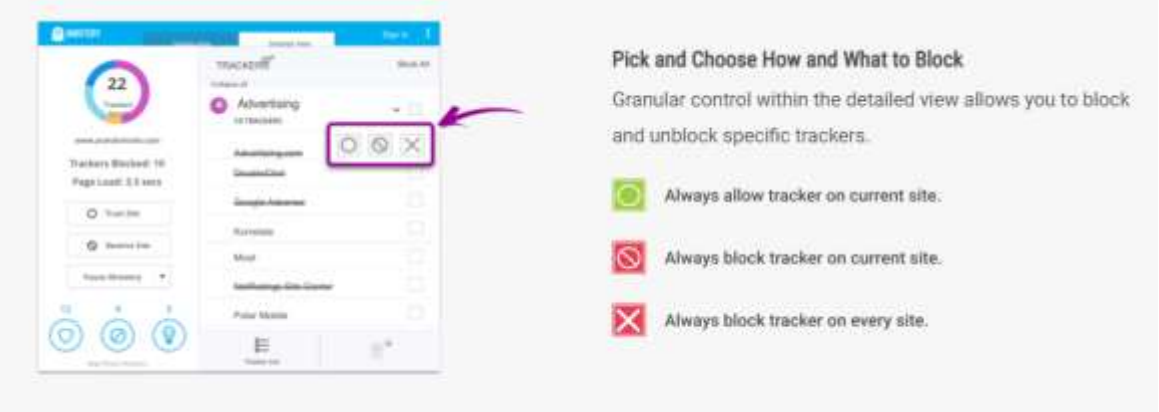
4.5.2 Présentation de l'usage

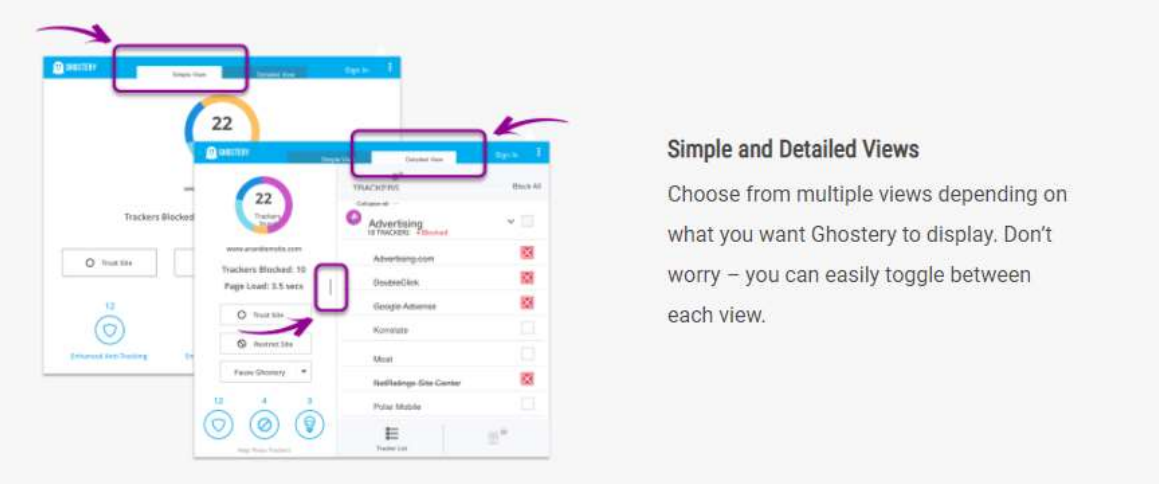
À l'exception de Privacy Badger, les sites Web des outils étudiés exposent de façon simple la manière d'utiliser l'outil, et ce au moyen de supports visuels utiles. La section d'aide du site Web d'Adblock Plus contient par exemple plusieurs tutoriels illustrés qui s'adaptent au navigateur qu'ils utilisent (en reconnaissant le navigateur utilisé)[446]. La présentation du fonctionnement est plus minimale, mais tout de même claire, du côté de Ghostery, dont une page secondaire du site Web comprend un carrousel d'images représentant l'utilisation de cinq fonctionnalités de l'outil[447].

[446] ADBLOCK PLUS. En ligne : https://help.eyeo.com/fr/adblockplus/ (consulté le 12 mars 2021).
[447] GHOSTERY. En ligne : https://www.ghostery.com/ghostery-browser-extension/ (consulté le 15 mars 2021).

Illustration 4

Extraits d'une page du site Web de Ghostery relative aux fonctionnalités de l'outil





Source : https://www.ghostery.com/ghostery-browser-extension/

La présentation de l'usage de Adblock Plus et Ghostery accorde une grande place au contrôle que pourront exercer les utilisateurs en soulignant par exemple la multiplicité des réglages possibles. Or, on offre peu d'explications aux internautes quant aux éléments à prendre en compte dans ce choix. Un consommateur à la recherche d'un bloqueur de publicité risque probablement de se demander pourquoi filtrer un traceur plutôt qu'un autre. Et il pourrait ultimement faire des choix qui ne favorisent pas une protection optimale de sa vie privée en ligne, par manque de connaissance et de soutien.

Malheureusement, Privacy Badger qui se démarquait quant à la présentation de l'utilité de l'outil est plutôt décevant en ce qui concerne la présentation de son utilisation. Toute l'information est disponible, mais la présentation est étonnamment peu attrayante pour un fournisseur qui fait pourtant un effort indéniable pour favoriser la compréhension du lecteur. Et l'internaute devra parcourir la longue liste de Questions et réponses afin de comprendre le fonctionnement de l'outil puisqu'aucune section du site n'est spécifiquement dédiée à sa présentation.

Enfin, soulignons la situation particulière dans laquelle se trouve Adblock Plus : l'outil prévoit une liste de « publicités acceptables » qu'il ne bloque pas d'emblée. Cette pratique a fait l'objet de plusieurs critiques et controverses, notamment parce que les publicitaires paient parfois pour voir leurs publicités ajoutées à cette « liste blanche » de pubs qui continueront à être présentées à l'utilisateur malgré l'activation du bloqueur[448].

Dans la mesure où plusieurs des internautes canadiens sondés avaient des doutes quant au modèle d'affaires des outils gratuits offerts et, incidemment, quant à l'ampleur de la protection réellement offerte par les TAQs, il est intéressant de s'attarder à la manière dont Adblock Plus explique le fonctionnement de son programme de publicités acceptables, un programme qui pourrait fort vraisemblablement nourrir ce scepticisme. Des mentions à l'effet que « les publicités ne sont pas toutes mauvaises » et que « les sites web ont besoin d'argent pour rester gratuits » sont présentes sur la page d'accueil du site Web, sans précisions additionnelles sinon un hyperlien vers une page qui explique comment refuser la publicité acceptée par l'outil. Depuis cette dernière page seulement, l'internaute pourra éventuellement accéder à des explications sur les critères d'analyse des publicités et sur le financement de l'outil au moyen du programme de publicité acceptable.

4.6 Les antivirus

Parmi les fournisseurs d'antivirus les plus populaires[449], nous avons choisi d'étudier la présentation faite par Avast, McAfee et Eset sur leur site Web respectif.

Les sites Web visités sont généralement de plus grande envergure que ceux d'autres catégories d'outils (généralement gratuits), possiblement parce que le prix des services offerts peut atteindre 240 $/année. Tous offrent une gamme de produits présentant différentes fonctionnalités et différents niveaux de fonctionnalités. Nous avons donc concentré nos observations sur le produit phare de chaque compagnie pour la clientèle individuelle canadienne, soit « Avast Antivirus Gratuit », « McAfee Total Protection » et « Eset Internet Security ».

4.6.1 Présentation de la finalité

Les sites Web des antivirus étudiés vont droit au but en ce qui concerne leur fonction principale. Le consommateur a rapidement une bonne idée des menaces contre lesquelles on veut le protéger. Protection contre les pirates, détection de menaces telles que des virus, logiciels malveillants ou espions, analyse de fichiers inconnus, etc. : ces fonctions sont bien visibles sur la page d'accueil des sites des différents fournisseurs étudiés.

---

[448] MAHESHWARIA, S. « Adblock Plus, Created to Protect Users From Ads, Instead Opens the Door », New York Times, 18 septembre 2016, en ligne : https://www.nytimes.com/2016/09/19/business/media/adblock-plus-created-to-protect-users-from-ads-opens-the-door.html

[449] OPSWAT. « Windows Anti-malware Market Share Report », en ligne : https://metadefender.opswat.com/reports/anti-malware-market-share# (consulté le 10 mars 2021).

D'autres pages des sites détaillent la couverture offerte (et les menaces contrées) par chacun de leurs services, généralement sous forme de tableau. Leurs présentations sont très complètes et intelligibles ; il est indéniable que les fournisseurs ont prêté une attention particulière au langage utilisé. C'est tout particulièrement le cas de McAfee qui offre par exemple la description suivante d'un virus informatique :

> Un virus informatique est un code qui, une fois exécuté, est conçu pour pénétrer dans un ordinateur et se reproduire. Les virus conçus pour endommager un ordinateur sont classés comme un type de « logiciel malveillant ». Les objectifs néfastes des différents types de logiciels malveillants sont très variés. Ils peuvent par exemple prendre les formes suivantes :
>
> 1 Des ransomwares, qui chiffrent vos fichiers, photos et documents sensibles ainsi que votre ordinateur, et qui vous obligent à effectuer un paiement (souvent par le biais de bitcoins) en échange d'un mot de passe vous permettant de déchiffrer et de déverrouiller ces fichiers
> 2 Des chevaux de Troie, qui permettent à un pirate informatique de prendre complètement le contrôle de votre ordinateur et d'exécuter des programmes comme s'il utilisait réellement votre clavier et votre souris
> 3 Des logiciels espions, qui « extraient » les informations personnelles de votre ordinateur et les revendent au plus offrant
> 4 Des logiciels publicitaires, qui génèrent des fenêtres contextuelles indésirables provenant d'annonceurs douteux

Notons aussi le choix de ce fournisseur de présenter sur sa page d'accueil des statistiques quant aux menaces découvertes et traitées chaque jour (« 480 menaces découvertes chaque minute »). Même si ce type de présentation vise avant tout à vendre un produit, il nous semble malgré tout efficace afin d'aider les internautes moins avertis à prendre conscience du risque en ligne pour la sécurité et la confidentialité de leurs renseignements personnels.

4.6.2 Présentation de l'usage

Chaque fournisseur étudié offre un portail d'aide contenant une documentation abondante et des sections dédiées à l'installation et l'activation des produits. Peu d'information sur l'utilisation des produits se trouve intégrée aux sites Web principaux.

Peut-être en raison de la complexité et de la variété des fonctions possibles, on ne trouve pas sur les sites, contrairement à ce que l'on a vu pour d'autres types d'outils, d'illustrations des interfaces, qui permettraient au consommateur d'obtenir des explications sur leur fonctionnement. On trouve tout de même, dans les différentes rubriques des sites des fournisseurs, des instructions claires, et occasionnellement accompagnées de support visuel, sur le téléchargement, l'installation ou l'activation des outils.

Illustration 5
Extraits de la page du site Web d'Eset relative à l'installation de l'antivirus

Source : https://support.eset.com/en/kb3640-install-and-activate-eset-file-security-for-microsoft-windows-server-6x

4.7 Les adresses électroniques jetables

D'après nos recherches, il n'existe pas de données publiques sur la popularité des différents fournisseurs d'adresses électroniques jetables ou temporaires. Ce faisant, nous avons retenu aux fins de cette étude trois fournisseurs qui sont régulièrement mentionnés dans les palmarès disponibles en ligne sur ce type d'outils de protection de la vie privée[450]. Il s'agit des fournisseurs Tempmail, Mohmal et YOPmail.

4.7.1 Présentation de la finalité

De manière générale, les sites Web de ce genre d'outils sont assez avares d'information. Tempmail se démarque par son site qui comprend un blogue et une section questions et réponses.

Un internaute qui se rend sur le site Web de Mohmal, par exemple, devra déjà savoir ce que sont les adresses électroniques jetables, puisque la page d'accueil ne contient qu'une mention – assez peu visible – relative aux messages électroniques.

À l'opposé, le site Web de Tempmail offre une présentation assez complète des finalités de l'outil :

[450] « 10 Free Temporary Disposable Email Services To Fight Spam », GeckoandFly, 9 juin 2019, en ligne : https://www.geckoandfly.com/7782/how-to-create-temporary-email-and-gmail-forwarding-service/ ; « 10 Best Disposable Email Services for a Temporary Email Address », MashTips, 15 avril 2018, en ligne : https://mashtips.com/disposable-email-services/ ; « Best Free Disposable Email Address Services », Technogadge, 4 avril 2016, en ligne : http://www.technogadge.com/best-free-temporary-email-providers/

> Oubliez le pourriel, la publicité, le piratage et les attaques des robots[451], l'e-mail temporaire et anonyme c'est l'absence d'engagement et de risque. Temp Courriel fournit une adresse courriel anonyme, gratuite et temporaire[452].

Un peu plus bas, une rubrique intitulée « Qu'est-ce qu'un courriel temporaire jetable ? » mentionne le cas d'usage le plus commun, soit la nécessité de fournir une adresse courriel afin de s'inscrire sur un site Web pour accéder au contenu, envoyer des commentaires ou effectuer un téléchargement. Une autre page Web du fournisseur indique que les bases de données des magasins en ligne sont parfois victimes de piratage, en conséquence de quoi les adresses courriel de leurs utilisateurs se retrouvent sur des listes d'envoi de pourriels[453].

Le fournisseur tente aussi de défaire certains mythes, notamment quant au caractère « immoral » de l'utilisation des technologies d'amélioration de la confidentialité en ligne – ce qui n'est pas sans rappeler les propos de certains répondants aux entrevues de type « je n'ai rien à cacher » :

> Techniquement, l'idée d'utiliser une adresse courriel temporaire évoque les pirates informatiques (Black Hat) ou des zones d'Internet peu recommandables (Deep Web), mais il existe des raisons convaincantes pour utiliser des services de faux courriels[454].

Alors que plusieurs Canadiens sondés ont soulevé cette préoccupation, nous constatons malheureusement qu'aucun des sites visités n'aborde la question du blocage potentiel des adresses courriel jetables par différents services Web.

4.7.2 Présentation de l'usage

Contrairement à d'autres outils étudiés, les adresses courriel jetables sont utilisables directement depuis le site Web du fournisseur. Nul besoin donc d'expliquer la procédure d'installation ou d'aborder la compatibilité avec les différents navigateurs ou systèmes d'exploitation.

Le fonctionnement de YOPmail est clairement expliqué sur la page d'accueil et sur la courte page de foire aux questions.

> Dois-je créer un compte pour utiliser YopMail ?
> Non ! Rien à faire ! Tous les comptes existent déjà, mais aucun compte ne vous appartient vraiment. Il suffit d'envoyer un courriel à n'importe quelle adresse sur YopMail et de consulter la boîte correspondante.
>
> Comment accéder à une boîte de réception ?

[451] Aucune information supplémentaire n'est disponible quant aux « attaques des robots ».
[452] TEMPMAIL. En ligne : https://temp-mail.org/fr/
[453] TEMPMAIL. « La technique derrière les adresses email jetables », 7 juin 2021, en ligne : https://temp-mail.org/blog/fr/la-technique-derriere-les-adresses-email-jetables/
[454] *Ibid.*

> Sur la page d'accueil, vous entrez n'importe quel nom de compte dans la zone de saisie prévue à cet effet. Par exemple pour accéder au compte « nimportekoi@yopmail.com » vous saisissez « nimportekoi ».

Les deux autres fournisseurs sont moins descriptifs sur la manière d'utiliser l'outil, mais ils ont l'avantage d'une interface relativement intuitive et d'une utilisation plus simple (par exemple : octroi aléatoire d'une adresse courriel).

4.8 Les gestionnaires de mots de passe

Selon les données de la firme ISE, les fournisseurs 1Password, Dashlane et LastPass représentent, respectivement, les 1er, 2e et 4e gestionnaires de mots de passe les plus populaires[455]. À noter que le troisième en liste, Keepass, n'a pas été retenu pour cette étude parce que son site Web est exclusivement en anglais. Les trois fournisseurs retenus offrent des forfaits à des prix allant de 36 à 60 $US par année. Dashlane offre également une option gratuite qui comprend le stockage d'un maximum de 50 comptes.

4.8.1 Présentation de la finalité

De manière générale, la présentation des gestionnaires de mots de passe est axée sur la facilité d'utilisation et la simplification de l'expérience en ligne par la prise en charge de la mémorisation et de la saisie automatique des mots de passe.

> Go ahead, forget your passwords – 1Password remembers them all for you. [1Password]

Les explications relatives à la protection de la vie privée sont bien présentes (surtout sous l'angle de la sécurité informatique), mais cèdent le pas aux aspects pratiques. Nous les trouvons plutôt sur des pages secondaires.

Les fuites et vols de données, notamment en raison de mots de passe peu sécuritaires, constituent les principales menaces auxquelles font référence les fournisseurs de gestionnaires de mots de passe sur leur site Web ; elles sont mises de l'avant sur tous les sites consultés. En s'appuyant sur un rapport de Verizon[456], LastPass énonce par exemple ce qui suit :

> Les mots de passe constituent un vrai problème de sécurité. D'après un rapport récent, plus de 80 % des fuites de sécurité liées au piratage sont dues à des mots de passe faibles ou volés.

On trouve également plusieurs références aux fuites de données survenues chez certaines grandes entreprises, qui ont eu pour conséquence de compromettre les identifiants et mots

---

[455] ISE. « Password Managers: Under the Hood of Secrets Management », 19 février 2019, en ligne : https://www.ise.io/casestudies/password-manager-hacking/ ; FOWLER, G. A. « Password managers have a security flaw. But you should still use one », Washington Post, 19 février 2019, en ligne : https://www.washingtonpost.com/technology/2019/02/19/password-managers-have-security-flaw-you-should-still-use-one/

[456] VERIZON. « 2021 Data Breach Investigations Report », en ligne: https://enterprise.verizon.com/resources/reports/dbir/

de passe de millions de personnes. Une page du site Web de 1Password intitulée « sécurité » présente différents types de failles de sécurité impliquant par exemple l'hameçonnage et les enregistreurs de frappe non autorisés.

Par rapport à ses concurrents, Dashlane accorde davantage d'espace à la sécurité sur sa page d'accueil, dont le titre est « Plus votre mot de passe est aléatoire, plus vous renforcez votre sécurité ». Le site adopte une approche interactive pour la présentation de sa finalité : une section intitulée « Pourquoi avez-vous choisi Dashlane ? » propose à l'utilisateur de répondre à quelques questions afin de lui démontrer la valeur de l'outil. Peu importe les réponses, le consommateur est bien entendu amené vers une page qui recommande le téléchargement de l'outil ; ce questionnaire force tout de même le consommateur à se questionner sur ses craintes et ses besoins relativement à la protection de sa vie privée en ligne, ce qui est souhaitable.

Enfin, les fournisseurs abordent tous une crainte répandue chez les consommateurs, soit le risque que le service lui-même soit piraté. Ils expliquent tous clairement ne pas avoir accès aux données de leurs clients, celles-ci étant cryptées avec un mot de passe maitre propre à chaque utilisateur.

4.8.2 Présentation de l'usage

Les sites Web des trois fournisseurs étudiés expliquent clairement l'utilisation des gestionnaires de mots de passe offerts. La simplicité d'utilisation constitue d'ailleurs un des principaux arguments de vente. Tous présentent des captures d'écran de l'outil pour en expliquer le fonctionnement ou les avantages. Par exemple, la page « Fonctionnement » du site de LastPass, à laquelle on accède directement par le menu de navigation principal, représente la marche à suivre suivante :

Illustration 6
Extrait d'une page du site Web de LastPass relative à l'installation de l'outil

Source : https://www.lastpass.com/fr/how-lastpass-works

Les trois fournisseurs traitent des processus de chiffrement employés, vraisemblablement pour renforcer leur argument de vente quant à la sécurité des outils offerts. Or, les éléments qui sont avancés sont si techniques qu'ils risquent peu d'aider l'internaute

moyen. LastPass souligne par exemple qu'il met en œuvre « le chiffrement AES 256 bits avec SHA-256 PBKDF2 et hachage salt pour garantir une sécurité complète dans le nuage[457] ». Nous voilà rassurés.

Dashlane précise au moins que le chiffrement AES 256 bits est « la méthode la plus sûre à l'heure actuelle[458] ». En l'absence de cette information, le consommateur se trouve malheureusement devant une série de symboles et chiffres sans signification particulière !

D'autres sections des sites Web des fournisseurs de gestionnaires de mots de passe sont également clairement dédiées à un public plus technophile. Il est par exemple possible de consulter un document de plus de 80 pages qui décrit la conception qu'a 1Password de la sécurité informatique[459].

[457] LASTPASS. En ligne : https://www.lastpass.com/fr/how-lastpass-works (consulté le 15 avril 2021).
[458] DASHLANE. En ligne : https://www.dashlane.com/fr/business (consulté le 15 avril 2021).
[459] 1PASSWORD. En ligne : https://1password.com/fr/security/ (consulté le 15 avril 2021).

LA LÉGISLATION CANADIENNE EN PHASE AVEC LE POINT DE VUE DES CONSOMMATEURS ?

5.1. Survol du cadre canadien fédéral et provincial applicable

Le cadre juridique canadien en matière de protection de la vie privée comprend des lois adoptées par le Parlement fédéral et par certaines juridictions provinciales. Les pouvoirs du législateur fédéral en la matière découlent de sa compétence sur le trafic et le commerce[460], alors que ceux des législations provinciales s'expliquent par leur compétence sur la propriété et les droits civils et sur les matières de nature purement locale ou privée[461].

Relativement à la protection de la vie privée dans le secteur privé, le législateur fédéral a exercé son pouvoir par l'adoption de la *LPRPDE*[462] en avril 2000. Trois provinces ont choisi de faire de même : le Québec par l'adoption de la *LPRPSP*[463] en juin 1993 (et l'inclusion de certaines dispositions relatives à la vie privée au *Code civil*[464] et à la *Charte des droits et libertés de la personne*[465]), l'Alberta par l'adoption du *APIPA*[466] en 2003 et la Colombie-Britannique par l'adoption du *BCPIPA*[467] en 2003. Le Manitoba a également adopté une loi en la matière, le *Personal Information Protection and Identity Theft Prevention Act* (*PIPITPA*)[468] en 2014, mais ne l'a jamais mise en vigueur. L'Ontario a procédé à une consultation à l'automne 2020 en vue d'élaborer sa propre loi provinciale sur le sujet[469], mais aucun projet de loi n'a encore été déposé à l'Assemblée législative de l'Ontario. Plusieurs provinces ont des lois qui concernent spécifiquement le traitement des renseignements personnels dans le secteur des soins de santé. Nous ne traiterons pas de ces lois particulières dans le cadre du présent rapport.

460 CANADA. Loi constitutionnelle de 1867, 30 & 31 Victoria, c 3, art 91(2).
461 *Ibid.*, arts 92(13) et (16).
462 LPRPDE, *supra* note 77.
463 LPRPSP, *supra* note 78.
464 QUÉBEC. Code civil du Québec, RLRQ c CCQ-1991.
465 QUÉBEC. Charte des droits et libertés de la personne, *supra* note 79.
466 APIPA, *supra* note 78.
467 BCPIPA, *supra* note 78.
468 MANITOBA. The Personal Information Protection and Identity Theft Prevention Act, CCSM c P33.7.
469 GOUVERNEMENT DE L'ONTARIO. « Ontario's Regulatory Registry, Public Consultation - Modernizing Privacy in Ontario », 2021, en ligne : https://www.ontariocanada.com/registry/view.do?language=en&postingId=37468 (consulté le 10 juin 2021).

5.1.1. La loi fédérale : un document aux origines complexes

La *LPRPDE*, est largement calquée sur une initiative d'autoréglementation développée par l'industrie au milieu des années 1990[470]. La loi qui en a découlé présente une structure étonnante : une grande partie des obligations des entreprises se trouve à l'annexe 1 de la loi, sous forme de principes au lieu d'avoir été intégrés aux articles qui constituent le corps de la Loi.

La forme surprenante et le contenu parfois flou de la loi s'expliquent, selon le juge Décary de la Cour d'appel fédérale, par l'historique particulier des dispositions :

> The PIPED Act [acronyme anglophone de la *LPRPDE*] is also a compromise as to form, as is amply demonstrated by the recital of its historical background. Schedule 1 is an exact replica of Part 4 of the CSA Standard adopted in 1995, which Standard in turn was based on the OECD Guidelines adopted in 1980 and to which Canada had adhered in 1984. Both the CSA Standard and the OECD Guidelines are the product of intense negotiations between competing interests, which proceeded on the basis of self-regulation and which did not use nor purport to use legal drafting[471].

Ces exercices répétés de conciliation des intérêts divergents ont donné naissance à une loi dont les objectifs et les approches semblent parfois contradictoires et qui se révèle ultimement foncièrement insatisfaisante. La *LPRPDE* a fait depuis 2000 l'objet de quelques modifications, avec l'ajout en 2018, par exemple, d'une obligation d'aviser les personnes concernées à la suite d'un incident de confidentialité, mais n'a fait l'objet d'aucune réforme majeure et d'aucune réécriture de fond depuis son adoption.

Notons que la loi fédérale comprend également (comme son nom le suggère) une série de dispositions relatives à la documentation électronique, dont le lien avec la protection des renseignements personnels semble au mieux faible. De quoi mêler encore davantage les consommateurs et même les juristes qui tentent de bien comprendre le cadre juridique applicable !

5.1.2. Des lois provinciales similaires, mais distinctes

La loi fédérale s'applique en principe à l'ensemble du secteur privé sur le territoire canadien. Or, comment cohabite-t-elle avec les lois provinces existantes ?

En pratique, une organisation ne sera soumise qu'à une seule des lois à la fois, selon le lieu où elle opère et selon l'activité qu'elle exerce. Ainsi, la *LPRPDE* prévoit la possibilité d'exclure de l'application de la loi, certaines organisations, activités ou catégories d'activités lorsque celles-ci sont soumises à une loi provinciale « essentiellement similaire »[472]. Cette qualification qui est faite par le Gouverneur en Conseil au moyen d'un

---

[470] LEVIN. « Privacy Law in the United States », *supra* note 64, p.380.
[471] *Englander* v *Telus Communications Inc.*, 2004 FCA 387, para 43.
[472] LPRPDE, *supra* note 77, art 26.

décret, peut porter sur l'entièreté de la loi ou certains éléments seulement (par exemple le traitement des renseignements personnels relatifs à la santé).

Les lois provinciales de protection des renseignements personnels qui sont en vigueur sur le territoire canadien ont toutes été jugées suffisamment similaires à la loi fédérale.

Ainsi, au Québec, en Alberta et en Colombie-Britannique, les entreprises privées sont plutôt soumises à la loi provinciale, sauf s'il s'agit d'entreprises sous réglementation fédérale (services bancaires, télécommunication, aviation, etc.) ou s'il est question d'activité commerciale qui nécessite le transfert de renseignements personnels au-delà des frontières provinciales[473].

Tableau 16
L'application des lois canadiennes de protection des renseignements personnels détenus par le secteur privé, selon les provinces

<table>
<tr><td rowspan="2">Lieu</td><td colspan="2">Lois applicables selon le statut de l'entreprise qui procède au traitement des renseignements personnels</td></tr>
<tr><td>Entreprises de juridiction provinciale</td><td>Entreprises de juridiction fédérale</td></tr>
<tr><td>Alberta</td><td>Personal Information Protection Act (APIPA)</td><td rowspan="4">Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

* Réforme de la loi en cours (depuis novembre 2020)</td></tr>
<tr><td>Colombie-Britannique</td><td>Personal Information Protection Act (BCPIPA)</td></tr>
<tr><td>Québec</td><td>Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP)

* Réforme de la loi en cours (depuis juin 2020)</td></tr>
<tr><td>Autres provinces et territoires</td><td>Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)</td></tr>
</table>

Même si elles sont perçues comme similaires ici, il peut arriver que les différentes lois applicables au Canada ne soient pas perçues ainsi par des entités étrangères. Les évaluations réalisées par la Commission européenne quant à l'adéquation des cadres

[473] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Lois provinciales qui peuvent s'appliquer au lieu de la LPRPDE », mai 2020, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/

juridiques en matière de protection des renseignements personnels (décisions d'adéquation) en sont un bon exemple.

L'encadrement réglementaire applicable au sein de l'Union européenne limite le transfert de renseignements personnels vers un pays ou une organisation qui ne respecteraient pas le niveau de protection offert au sein de l'Union européenne. Pour faciliter l'analyse et éviter aux entreprises de devoir mettre en place des garanties particulières à chaque transfert, il existe un mécanisme de reconnaissance de l'adéquation d'encadrements étrangers avec l'encadrement européen[474]. Les transferts vers un pays tiers jugé « adéquat » par la Commission européenne sont alors assimilés à des transferts de données au sein de l'Union européenne. L'encadrement fédéral canadien bénéficie depuis le 20 décembre 2001[475] d'une telle décision d'adéquation (réaffirmée en 2006[476]). Or, l'analyse de l'encadrement québécois – qualifié, ici, rappelons-le, d'essentiellement similaire à celui que prévoit la loi fédérale - a plutôt mené à une recommandation de ne pas déclarer l'encadrement adéquat pour l'Union européenne[477] !

Notons qu'autant la loi fédérale que les lois provinciales devront éventuellement faire l'objet d'une nouvelle évaluation par la Commission européenne puisque l'Union européenne a modifié son cadre réglementaire en 2016 par l'adoption du *Règlement général de protection des données* (*RGPD*) (entré en vigueur en 2018).

5.1.3. Des réformes tant attendues

C'est d'ailleurs partiellement en raison des futures évaluations européennes[478] que plusieurs législateurs canadiens procèdent actuellement à des réformes importantes de leurs lois respectives en matière de protection des renseignements personnels dans le secteur privé.

Le 12 juin 2020, le projet de loi 64 a été déposé à l'Assemblée nationale du Québec[479], proposant des changements à quelque 21 lois de la province ainsi qu'une réforme importante de la *LPRPSP*.

---

474 RGPD, *supra* note 55, art 45. Anciennement UNION EUROPÉENNE. Directive 95|46|CE, *supra* note 85, art 25.
475 COMMISSION DES COMMUNAUTÉS EUROPÉENNES. Décision 2002/2/CE, *supra* note 87.
476 CANADA. « Troisième rapport d'étape sur les évolutions en matière de législation sur la protection des données au Canada », rapport à la Commission européenne, juin 2018, p.3, en ligne : https://www.ic.gc.ca/eic/site/113.nsf/fra/h_07662.html
477 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES. Avis 7/2014 sur la protection des données à caractère personnel au Québec, 1443/15/FR WP 219, 4 juin 2014, en ligne : https://www.dataprotection.ro/servlet/ViewDocument?id=1290 ; Notons que la décision de la Commission européenne a été suspendue jusqu'à ce que le Québec procède à certains changements législatifs.
478 « The Privacy Commissioner's office said it understands a review of the GDPR by the European Commission is required by May 2020 » : SOLOMON, H. « Give privacy commissioner enforcement power, says parliamentary committee », IT World Canada, 5 mars 2018, en ligne: https://www.itworldcanada.com/article/give-privacy-commissioner-enforcement-power-says-parliamentary-committee/402451
479 QUÉBEC. Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, en ligne : http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html

Quelques mois plus tard, soit le 17 novembre 2020, le projet de loi C-11 a été déposé à la Chambre des communes à Ottawa[480]. Il proposait une réécriture complète de la *LPRPDE* (dorénavant appelée *Loi sur la protection de la vie privée des consommateurs*) et la création d'un tribunal de la protection des renseignements personnels et des données. Ce projet de loi s'inscrivait dans la mise en œuvre de la *Charte canadienne du numérique*, un document dévoilé en mai 2019 qui, plutôt qu'une charte, constitue en réalité une feuille de route du gouvernement canadien pour des initiatives réglementaires à venir[481].

Ces deux projets ont eu un parcours assez différent dans les mois qui ont suivi. Dans le cas du projet de loi québécois, il a ultimement été adopté le 21 septembre 2021 à la suite d'une longue étude par la Commission des institutions du Québec, au cours de laquelle se sont multipliées les pauses. L'entrée en vigueur de la majorité des nouvelles dispositions est prévue pour septembre 2023[482]. Le projet de loi fédéral est pour sa part mort au feuilleton à l'été 2021, suite de l'annonce de la tenue d'une élection fédérale en septembre 2021. Mais même avant cette annonce, le projet n'en était qu'à l'étape de la seconde lecture à la Chambre des communes[483] et ne semblait pas faire partie de l'agenda législatif prioritaire du gouvernement de l'époque. Au moment de publier ce rapport, nous ignorons si le gouvernement réélu entend redéposer tel quel le texte du projet C-11.

5.2. Comment les lois canadiennes répondent-elles aux préoccupations des consommateurs ?

Dans le cadre de l'analyse qui suit, nous aborderons les lois fédérale et provinciales qui traitent de la protection des renseignements personnels dans le secteur privé. Nous aborderons également les changements proposés par les deux projets de loi déposés en 2020. À noter qu'en raison du très court délai entre l'adoption du projet de loi québécois et le dépôt du présent rapport, nous ne sommes pas en mesure d'étudier la Loi 25 du Québec (l'aboutissement du projet 64). Nous avons donc choisi de limiter notre étude aux versions des deux projets en date de janvier 2021. Certains commentaires relatifs au projet québécois pourraient donc ne plus être à jour en raison d'amendements apportés au projet après cette date. Dans le cas du projet fédéral, ce choix n'a aucun impact puisque le texte du projet C-11 n'a fait l'objet d'aucune modification entre son dépôt en novembre 2020 et la dissolution du Parlement en août 2021.

---

480 CANADA. Projet de loi C-11. Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois, deuxième session, quarante-troisième législature, 2020.
481 UNION DES CONSOMMATEURS. « Une charte des droits des internautes : Pour une perspective canadienne », janvier 2020, en ligne : https://uniondesconsommateurs.ca/une-charte-des-droits-des-internautes-pour-une-perspective-canadienne/ comprend une analyse de la Charte canadienne du numérique à la lumière des autres instruments de reconnaissance des droits des internautes développés à l'étranger et à l'international (section 3.2.4).
482 ASSEMBLÉE NATIONALE DU QUÉBEC. « Projet de loi n° 64», en ligne : http://assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html (consulté le 10 octobre 2021).
483 PARLEMENT DU CANADA. «C-11 - 43e législature, 2e session», LegisInfo, en ligne : https://www.parl.ca/LegisInfo/fr/projet-de-loi/43-2/C-11 (consulté le 10 octobre 2021).

Nous concentrerons notre étude sur les différentes approches législatives retenues et non sur le détail des dispositions spécifiques que contiennent les lois ou projets en question. Comment abordent-ils certains risques pour la vie privée ? Comment conçoivent-ils la responsabilité de chaque partie dans la protection des renseignements personnels ?

Dans certains cas, l'approche retenue par les législateurs canadiens a été critiquée par des experts ou des groupes de la société civile. Le cas échéant, nous soulignerons au passage ces critiques et certaines autres approches législatives ou réglementaires proposées par les auteurs ou mises en place à l'étranger, notamment au sein de l'Union européenne.

5.2.1 Préoccupations relatives au traitement des renseignements personnels

Rappelons que les trois grandes préoccupations recensées par Malhotra *et al*. ont toutes obtenu un haut niveau d'appui de la part des répondants canadiens au sondage. Ces préoccupations ont trait à l'ampleur de la collecte de renseignements personnels, au degré de contrôle qu'exercent les consommateurs sur cette collecte et sur le traitement général de leurs renseignements personnels et, finalement, à l'état de leurs connaissances en la matière.

Nous examinerons donc d'abord comment les lois canadiennes applicables abordent « l'économie fondée sur les données » (*data-driven economy*), le contrôle des consommateurs sur leurs renseignements personnels et la transparence des entreprises quant au traitement desdits renseignements.

5.2.1.1 Les lois canadiennes et la transparence des entreprises en matière de traitement des renseignements personnels

L'approche des législateurs canadiens en ce qui concerne la connaissance qu'ont les individus du traitement de leurs renseignements personnels s'articule autour d'une obligation de transparence pour les entreprises impliquées dans le traitement.

Les quatre lois canadiennes applicables au secteur privé prévoient ainsi qu'une entreprise doit fournir à un individu, avant ou au moment de la collecte de ses renseignements personnels, des explications sur les fins de cette collecte[484]. La loi québécoise et la loi fédérale prévoient plusieurs autres éléments qui doivent également être divulgués d'office ou sur demande à la personne concernée (notamment en ce qui concerne l'accès au dossier par des employés de l'entreprise ou par l'individu lui-même)[485]. La loi fédérale, qui, rappelons-le, s'articule davantage sous forme de grands principes, prévoit en sus qu'un individu doit pouvoir obtenir de l'information sur les politiques et pratiques d'une

[484] LPRPDE, *supra* note 77, annexe 1, art 4.2.3 ; LPRPSP, *supra* note 78, art 8 ; BCPIPA, *supra* note 78, art 10(1)a) ; APIPA, *supra* note 78, art 13(1)a).
[485] LPRPDE, *supra* note 77, annexe 1, art 4.8 ; LPRPSP, *supra* note 78, art 8.

organisation en matière de traitement de ses renseignements personnels « sans efforts déraisonnables »[486].

Afin de se conformer à ces obligations de transparence - plus ou moins sévères selon la loi applicable -, les entreprises canadiennes indiquent généralement les renseignements requis dans leurs conditions d'utilisation des biens ou services vendus, ou dans la politique de confidentialité de leur site Web (à laquelle renvoie généralement la fenêtre au bas d'une page Web), avec, souvent, la mention « J'accepte les conditions d'utilisation » et une case que doit cocher l'internaute pour poursuivre sa navigation ou son opération, et qui constitue l'expression de son consentement auxdites conditions. Malgré une obligation distincte de transmettre l'information de manière compréhensible et facilement accessible[487], nous avons déjà souligné à la section 2.1.1.3, plusieurs problèmes associés en pratique à ces types de documents. Ils sont longs, complexes et bien souvent remplis de termes ambigus. Difficile donc de les considérer comme facilement compréhensibles et accessibles pour le consommateur moyen…

S'ajoute aux difficultés de compréhension, un autre problème de taille : la quantité de documents de ce type auxquels un individu est exposé en ligne. À chaque site Web consulté, à chaque service utilisé en ligne : l'individu sera exposé à toujours plus d'information sur le traitement de ses renseignements personnels.

Cette réalité a mené des chercheurs à parler d'une situation de surinformation (*information overload*) dans laquelle l'individu n'est en mesure de traiter de manière adéquate qu'une fraction de l'information qu'il reçoit[488]. Rappelons que la lecture des politiques de grandes organisations telles que Facebook, Google, Snapchat, Airbnb prend au moins 20 minutes chacune[489]. Une étude réalisée en 2008 concluait qu'un individu qui lirait les politiques de confidentialité de tous les sites Web qu'il consulte devrait y consacrer environ 240 heures par année, l'équivalent de 10 jours complets ou de près de 40 minutes par jour[490]. Il est vraisemblable que le temps à y consacrer aujourd'hui serait bien supérieur[491].

Plusieurs chercheurs qui se sont penchés sur les politiques de confidentialité dans le secteur privé arrivent malheureusement au constat qu'il est impossible de renseigner adéquatement les individus sur ces politiques, dans le contexte actuel :

> If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details,

---

[486] LPRPDE, *supra* note 77, annexe 1, art 4.8.1.
[487] *Ibid.,* annexe 1, art 4.8.
[488] BEN-SHAHAR, O et SCHNEIDER, C. E. « The failure of mandated disclosure », University of Pennsylvania Law Review, vol. 159, p.687, en ligne : https://www.law.upenn.edu/journals/lawreview/articles/volume159/issue3/BenShaharSchneider159U.Pa.L.Rev.647(2011).pdf
[489] COLEMAN, J. « Here's How Long It Would Take to Read All the New Privacy Updates », 23 mai 2018, en ligne : https://jonnathancoleman.medium.com/heres-how-long-it-would-take-to-read-all-the-privacy-updates-you-ve-been-getting-cd4f215cff6d
[490] MCDONALD, A. M. et CRANOR, L. F. « The Cost of Reading Privacy Policies », A Journal of Law and Policy for the Information Society, 2008, p.18, en ligne : https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf
[491] À titre d'exemple, la politique de Google faisait un peu plus de 2000 mots en 2009 contre 4000 mots dix ans plus tard : WARZEL. « Google's 4,000-Word Privacy Policy », *supra* note 138.

> ones that are likely to make a difference: who are the business associates and what information is being shared with them; what are their commitments; what steps are taken to anonymize information; how will that information be processed and used. An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance. Thus the transparency paradox: transparency of textual meaning and transparency of practice conflict in all but rare instances[492].

5.2.1.1.1. Des obligations accrues dans les réformes législatives proposées

Dans le cadre des réformes fédérale et québécoise, l'approche législative commune qui met l'accent sur la diffusion obligatoire de renseignements par l'entreprise qui entend procéder au traitement de renseignements personnels est entièrement maintenue. Les obligations de transparence des entreprises sont d'ailleurs étendues à de nouveaux éléments. Certains de ces ajouts s'expliquent par l'évolution des technologies, dans un contexte où les lois sont notamment révisées afin d'être mieux adaptées aux réalités du Web. Par exemple, le projet de loi 64 (Qc) prévoit la divulgation obligatoire du recours par l'entreprise à une technologie de traitement des renseignements personnels qui permet d'identifier, de localiser ou d'effectuer un profilage des individus visés[493].

5.2.1.2. Les lois canadiennes et le contrôle des consommateurs sur leurs renseignements

Le contrôle qu'exercent (ou souhaiteraient exercer) les consommateurs sur le traitement de leurs renseignements personnels se présente dans les lois canadiennes principalement dans les dispositions relatives au consentement. Ces dispositions doivent bien entendu être lues avec celles relatives à la transparence des entreprises puisqu'un consentement ne sera valable que s'il est libre et éclairé.

Le traitement du consentement dans les différentes lois

Les quatre lois prévoient que la collecte ou le traitement des renseignements personnels ne peut avoir lieu, sauf exception, que si la personne concernée y a préalablement consenti à moins d'en être autrement autorisé par les lois[494].

Les différentes lois en vigueur au pays font donc du consentement du consommateur un élément central au traitement de ses renseignements personnels par le secteur privé. Elles placent le consommateur, en apparence, à tout le moins, au centre des décisions. Pourtant, il s'avère que l'exercice du consentement est beaucoup plus difficile en pratique qu'il n'y

---

[492] NISSENBAUM, H. « A Contextual Approach to Privacy Online », Journal of the American Academy of Arts & Sciences, automne 2011, p.36, en ligne : https://www.amacad.org/publication/contextual-approach-privacy-online
[493] QUÉBEC. Projet de loi n° 64, *supra* note 479, art 99 (qui ajoute l'art 8.1 de la *LPRPSP*).
[494] Notons que ces autres bases légales sont rédigées et considérées en pratique comme des exceptions au consentement. : LPRPDE, *supra* note 77, annexe 1, principe 4.3 ; LPRPSP, *supra* note 78, arts 6 ; BCPIPA, *supra* note 78, art 14 ; APIPA, *supra* note 78, art 7(1).

parait dans la loi et que le consommateur exerce ultimement assez peu de contrôle réel sur le traitement de ses renseignements en ligne. Certains qualifient dès lors le cadre législatif actuel en matière de consentement d'illusoire[495] ou de trop optimiste[496]. Voyons pourquoi.

Trois questions sont centrales afin d'analyser la qualité d'un consentement : Est-il éclairé ? Est-il donné librement ? Et est-il manifeste ? Pour chacune de ces questions, les réalités du Web affectent négativement la réponse.

En ce qui concerne le caractère éclairé du consentement, rappelons le phénomène de la surinformation et le caractère illisible et flou des politiques de protection de la vie privée de grandes entreprises étudiées par le New York Times, dont nous avons traité précédemment. S'ajoute à cela, la difficulté qu'ont les consommateurs à évaluer les risques et autres conséquences de leur éventuel consentement, particulièrement les conséquences à plus long terme. Cette réalité est parfois décrite comme une « myopie de la vie privée » (*privacy myopia*[497]), en référence au trouble de la vision qui rend plus difficile la vue des objets éloignés. Nous constatons donc que le contexte actuel du Web rend difficilement possible l'expression par le consommateur d'un consentement réellement éclairé.

La situation ne s'améliore pas lorsqu'il est question du caractère libre du consentement des consommateurs en ligne. Le consommateur exprime-t-il son choix sans contrainte ? Le consommateur a-t-il réellement le choix d'accepter ou non le traitement de ses renseignements personnels par des entreprises en ligne, lorsqu'il fait par exemple affaire à une entreprise qui exerce un monopole ou quasi-monopole sur l'offre de certains biens ou services[498] ? La réponse est simple : non. S'il refuse de consentir à la collecte et l'utilisation de ses renseignements auxquelles l'entreprise entend procéder, il doit du même coup renoncer aux biens ou services (incluant par exemple l'accès à un site Web ou à une plateforme numérique) qu'il désire, et dont il ne peut pas nécessairement se passer. Ce choix, particulièrement présent en ligne, amène certains experts à parler de dilemme de la vie privée[499]. Un dilemme d'autant plus difficile à trancher, pour le consommateur qui comprend bien ce qu'il désire, mais qui ne comprend pas nécessairement ce que l'entreprise exige en échange et le coût réel que cela représente.

Sur ce dernier point, notons qu'il existe tout de même dans les quatre lois en vigueur des dispositions qui tentent – avec plus ou moins de succès – de résoudre ce problème. Ainsi,

---

[495] WORLD ECONOMIC FORUM. « Redesigning Data Privacy: Reimagining Notice & Consent for human technology interaction, white paper », juillet 2020, p.4, en ligne : http://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf

[496] SOH, S. Y. « Privacy nudges: an alternative regulatory mechanism to 'informed consent' for online data protection behaviour », European Data Protection Law Review, vol. 5, no. 1, 2019, pp.67-68.

[497] BYGRAVE, L. et SCHARTUM, D. « Consent, Proportionality and Collective Power », dans GUTWIRTH, S. *et al.*, dir, Reinventing Data Protection ?, Springer, 2009, pp.3-4, en ligne : https://www.researchgate.net/publication/226832769_Consent_Proportionality_and_Collective_Power

[498] *Ibid.*

[499] GOULDING, A. « The identity and privacy dilemma », Newsroom, 26 août 2019, en ligne : https://www.newsroom.co.nz/@ideasroom/2019/08/26/770241/the-identity-and-privacy-dilemma# ; BURKHARDT, K. « The privacy paradox is a privacy dilemma », Mozilla Firefox, 24 août 2018, en ligne : https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/

il est interdit de rendre conditionnel à l'offre d'un bien ou service le consentement au traitement de renseignements personnels… à moins que les opérations pour lesquelles l'entreprise demande le consentement ne soit requises pour l'exécution du contrat[500] ou pour la réalisation de « fins légitimes »[501]. Ces exceptions font bien souvent l'objet d'une interprétation excessivement large par les entreprises[502].

Enfin, le sérieux d'un consentement s'évalue également par la manière par laquelle il est exprimé par le consommateur. À ce sujet, les lois en vigueur laissent beaucoup de marge de manœuvre aux entreprises en les autorisant dans certaines circonstances à s'appuyer sur un consentement implicite au traitement de renseignements personnels, c'est-à-dire un consentement qui se déduit des circonstances. La *LPRPDE* permet de procéder au traitement des renseignements personnels sur la base d'un consentement implicite dès lors que les renseignements visés ne sont pas sensibles[503]. Les lois albertaine et britanno-colombienne ne distinguent pas selon le type de renseignements, mais imposent un critère de raisonnabilité[504]. Seule la loi québécoise prévoit que le consentement doit toujours être manifeste (exprimé clairement)[505].

La reconnaissance du consentement implicite équivaut à la mise en place d'un système d'*opt-out*, ou de consentement négatif : si la personne ne pose pas de geste concret afin de signifier son refus au traitement de ses renseignements personnels, il sera permis de considérer qu'elle a accepté. Ainsi, une personne qui consulte un site Web consent implicitement à la collecte et à l'utilisation de ses renseignements par ce site s'il est indiqué quelque part sur le site qu'il s'agit de la pratique de l'entreprise[506]. En apparence, tout ça semble logique : une personne continue d'utiliser un service après avoir appris qu'il collecterait des renseignements à son sujet. Elle doit bien être d'accord, non ? En pratique, c'est loin d'être si clair, en raison de l'absence de réelle concurrence dans certains secteurs en ligne, mais aussi parce que cette connaissance par le consommateur des politiques et des pratiques des entreprises est, comme nous le mentionnions, purement théorique et ne reflète absolument pas la réalité.

La légitimité du consentement implicite se voit donc remise en question selon les circonstances.

---

500 LPRPSP, *supra* note 78, art 9(1°) ; BCPIPA, *supra* note 78, art 7(2) ; APIPA, *supra* note 78, art 7(2).
501 LPRPDE, *supra* note 77, annexe 1, art 4.3.3.
502 Soulignons à ce sujet, le dépôt en Europe de multiples plaintes contre Google, Facebook, WhatsApp et Instagram par l'organisation à but non lucratif None of your business quelques minutes à peine après l'entrée en vigueur du plus récent règlement européen (plus sévère en matière de « consentement forcé ») : GROTHAUS, M. « Google and Facebook are already accused of breaking GDPR laws », Fast Company, 25 mai 2018, en ligne : https://www.fastcompany.com/40577794/google-and-facebook-are-already-accused-of-breaking-gdpr-laws ; MOODY, G. « Google hit with first big GDPR fine over "forced consent"; eight new complaints filed over "right to access" », Privacy News Online, 2 février 2019, en ligne : https://www.privateinternetaccess.com/blog/google-hit-with-first-gdpr-fine-over-forced-consent-eight-new-complaints-filed-over-right-to-access/
503 LPRPDE, supra note 76, annexe 1, art 4.3.6.
504 BCPIPA, *supra* note 78, art 8(1) ; APIPA, *supra* note 78, art 8(2)b).
505 LPRPSP, *supra* note 78, art 14.
506 Voir à ce sujet les commentaires du Commissariat à la protection de la vie privée du Canada sur le consentement implicite en matière de publicité comportementale : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne », décembre 2011, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/gl_ba_1112/

> […] with opt-out the consent procured is less legitimate than with opt-in regimes. This disparity does not make opt-out consent illegitimate, but it is certainly ambiguous, as opt-out consent might be the product of mere inertia or lack of awareness of the option to opt out[507].

L'approche des organismes responsables de l'application des lois

Si l'encadrement du consentement est essentiel à toute discussion sur l'état du contrôle qu'exerce un consommateur sur ses renseignements personnels, il n'est pas le seul élément d'intérêt dans les lois canadiennes. Le sentiment d'avoir perdu le contrôle (ou de ne l'avoir jamais eu) sur le traitement des données en ligne que ressentent bien des consommateurs est vraisemblablement amplifié par une impression que les institutions qui gouvernent sont impuissantes, elles aussi.

L'analyse des pouvoirs d'intervention limités qui sont conférés aux organismes qui sont chargés de l'application des lois de protection des renseignements personnels au pays permet de conclure que les législateurs canadiens ont choisi de mettre en place un système qui n'a pas principalement pour but de punir les entreprises fautives, mais plutôt d'accompagner les entreprises dans l'élaboration, l'amélioration et la correction de leurs pratiques et politiques en matière de traitement des renseignements personnels. C'est particulièrement le cas au fédéral, ce qui peut s'expliquer notamment par les origines particulières de sa loi.

L'organisme chargé de veiller à l'application de la *LPRPDE* est le Commissariat à la protection de la vie privée du Canada. En vertu de la Loi, le Commissariat peut recevoir et examiner les plaintes de particuliers[508], mener des vérifications[509] et intenter des poursuites[510]. Il n'a toutefois aucun réel pouvoir coercitif : il peut formuler des recommandations à la suite d'une enquête ou encore conclure des accords (volontaires) de conformité avec une organisation, mais en l'absence de coopération, il devra se tourner vers les tribunaux et entamer des démarches (laborieuses) afin de faire respecter la loi et punir les contrevenants. Il n'a donc aucun pouvoir exécutoire direct[511].

Parmi les plus fervents critiques des faibles pouvoirs d'actions du Commissariat, on retrouve le Commissariat lui-même qui réclame des changements à la loi en ce sens depuis de nombreuses années déjà ! Dans le cadre d'un rapport sur la nécessité de réformer la *LPRPDE* publié en 2013, le Commissariat affirmait ceci :

---

[507] SOLOVE, D. J. « Privacy Self-Management and the Consent Dilemma », Harvard Law Review, vol. 126, 2013, p.1899, en ligne : https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications

[508] LPRPDE, *supra* note 77, arts 12 et ss.

[509] *Ibid.,* arts 18 et ss.

[510] *Ibid.,* art 15.

[511] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Arguments en faveur de la réforme de la Loi sur la protection des renseignements personnels et les documents électroniques », mai 2013, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/pipeda_r/pipeda_r_201305/

> Les recommandations « douces » assorties de peu de conséquences en cas de manquement à la loi ne sont plus efficaces dans un environnement qui évolue rapidement et où les risques pour la vie privée sont à la hausse.
>
> [...] Il est légitime de se demander comment une petite entité disposant de ressources limitées, comme le Commissariat, peut attirer l'attention de ces entreprises et les encourager activement à se conformer à la LPRPDE, alors qu'en réalité, le fait de contrevenir à la loi canadienne en matière de protection de la vie privée entraîne très peu de conséquences.[512]

Les organismes chargés de veiller à l'application des lois québécoise, albertaine et britanno-colombienne – la Commission d'accès à l'information et les Information and Privacy Commissioners, respectivement - ont une plus grande marge de manœuvre dans les décisions qu'elles peuvent rendre (qui ne se limitent pas à de simples recommandations) à la suite d'une enquête et/ou d'une plainte[513], mais demeurent, eux aussi, insatisfaits du manque de mordant de leurs pouvoirs d'intervention[514]. Comme le Commissaire fédéral, ils n'ont pas la possibilité d'imposer directement des sanctions pécuniaires aux entreprises fautives sans enquête et condamnation pénale[515]. Et le montant des sanctions pénales n'est pas nécessairement très dissuasif ; il est d'au plus quelques milliers de dollars pour une première offense au Québec, sauf exception[516].

5.2.1.2.1. Le contrôle des consommateurs dans les réformes législatives proposées

Les projets de loi fédérale et québécoise apportent bon nombre de changements en ce qui concerne le contrôle exercé par les consommateurs sur le traitement de leurs renseignements personnels... mais pas nécessairement à leur avantage. Les projets témoignent aussi d'un changement d'approche en ce qui concerne les organismes chargés d'assurer le respect des lois.

Entre renforcement et adoucissement du consentement

Le projet de loi québécois s'éloigne quelque peu du modèle *d'opt-in* actuellement en place en ouvrant la porte au recours au consentement implicite pour des utilisations à des fins

---

[512] *Ibid.*
[513] MINISTÈRE DE LA JUSTICE DU CANADA. « Les commissariats à l'information et à la protection de la vie privée : fusion et questions connexes », 2015, en ligne : https://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/p7.html ; LPRPSP, supra note 77, art 83 ; BCPIPA, supra note 77, art 52 ; APIPA, supra note 77, art 52.
[514] STODDART, J. *et al.*. « Modernisation des lois sur l'accès à l'information et la protection des renseignements personnels au XXIe siècle », CAI, 2013, en ligne : https://www.cai.gouv.qc.ca/modernisation-des-lois-sur-lacces-a-linformation-et-la-protection-des-renseignements-personnels-au-xxie-siecle/ ; BUCHANAN, J. et FRANKS, K. « BC Privacy Law Reform Update: Commissioner Calling for Changes to BC's Personal Information Protection Act », McCarthy, 8 juin 2020, en ligne: https://www.mccarthy.ca/en/insights/blogs/techlex/bc-privacy-law-reform-update-commissioner-calling-changes-bcs-personal-information-protection-act ; BURDEN, A. « Canada: Alberta's Legislation On Privacy And Protection Of Personal Information Needs Review: Commissioner », Mondaq, 7 janvier 2021, en ligne: https://www.mondaq.com/canada/data-protection/1022652/alberta39s-legislation-on-privacy-and-protection-of-personal-information-needs-review-commissioner
[515] LPRPSP, supra note 77, art 91 *a contrario* ; APIPA, supra note 77, art 52 et art 59 *a contrario.*
[516] LPRPSP, supra note 77, art 91 ; C BCPIPA, supra note 77, art 50 et art 52 *a contrario*.

autres que celles pour lesquelles le renseignement personnel a été recueilli, sauf si les renseignements personnels visés sont sensibles[517] ; il s'agit ainsi d'une nouvelle exception à l'exigence d'un consentement exprès, qui se limite heureusement aux usages autres dont les fins seraient compatibles avec celles pour lesquelles le renseignement a été recueilli. Par ailleurs, une obligation d'obtenir un consentement distinct pour chaque fin de la collecte s'ajoute aux obligations existantes[518].

Du côté du projet de loi fédéral, on maintient le modèle d'*opt-out* plus généralisé qui est déjà en place pour le traitement de renseignements non sensibles. On y propose quelques changements et réécritures mineurs à la loi existante qui, selon la professeure Teresa Scassa, ne justifient pas les déclarations du gouvernement à l'effet qu'il « réforme » le consentement en matière de protection des renseignements personnels dans le secteur privé[519]. Ce qui est surtout modifié par le projet de loi fédéral est l'ampleur des exceptions au principe du consentement, exceptions qui sont destinées à réduire le fardeau des entreprises. Parmi ces nouvelles exceptions, on retrouve celle relative au traitement de renseignements personnels réalisé dans le cadre d'activités d'affaires et pour lequel une personne raisonnable s'attendrait à une telle collecte, utilisation, etc. de ces renseignements personnels[520]. Le projet de loi spécifie que cette exception inclut entre autres les situations où il est « pratiquement impossible » d'obtenir le consentement étant donné l'absence de lien direct entre l'entreprise et le consommateur[521]. Autre fait inquiétant : dans sa forme réécrite, la loi fédérale associe directement les obligations de transparence des entreprises à la validité du consentement du consommateur[522]. Ce faisant, lorsque le consentement n'est pas requis, il n'est pas clair que l'entreprise ait tout de même l'obligation d'informer le consommateur de ses pratiques et politiques préalablement à la collecte ou autre traitement de ses renseignements personnels.

Un droit à la mobilité des données

Si leur révision du consentement est considérablement différente, les deux projets de loi s'entendent sur la reconnaissance d'un nouveau droit aux consommateurs : le droit à la mobilité de ses renseignements personnels[523]. Notons tout de même que le projet fédéral prévoit une application plus restreinte, en limitant l'exercice de ce droit à certains secteurs d'activités visés par un encadrement réglementaire spécifique additionnel.

De manière générale, le droit à la mobilité des données - connu en Europe sous le nom de droit à la portabilité des données[524] - permet aux individus d'obtenir une copie de leurs

---

[517] QUÉBEC. Projet de loi n° 64, *supra* note 479, art 102 (qui remplace les art 12 à 14 de la *LPRPSP*).
[518] *Ibid.*
[519] SCASSA, T. « The Gutting of Consent in Bill C-11 », 21 décembre 2020, en ligne : http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=336:the-gutting-of-consent-in-bill-c-11&Itemid=80
[520] CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 18.
[521] *Ibid.*, art 18(2)e).
[522] *Ibid.*, art 15(3).
[523] QUÉBEC. Projet de loi n° 64, *supra* note 479, art 112 (qui modifie l'art 27 de la *LPRPSP*) ; CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 72.
[524] RGPD, supra note 54, art 20.

renseignements personnels détenus par un fournisseur de service en vue de les remettre à un nouveau fournisseur de service (ex. : banque, télécom, etc.) ou d'en demander la communication directement entre les deux organisations[525]. En octroyant un droit à la mobilité des données aux particuliers, le législateur augmente ainsi leur contrôle sur des renseignements personnels déjà été collectés et utilisés par une entreprise.

Le droit à la mobilité des données est certes associé à une conception des renseignements personnels comme propriété des individus concernés[526] et à une notion de contrôle de cette propriété, mais ce droit relève-t-il réellement de la protection des renseignements personnels ? La question fait débat, mais les auteurs sont généralement d'avis qu'il s'agit avant tout d'une mesure propre au droit de la concurrence, qui vise à favoriser la concurrence au sein du marché des services numériques en facilitant les déplacements des consommateurs entre fournisseurs[527]. Un droit à la mobilité du numéro de téléphone (qui est indéniablement un renseignement personnel) existe depuis très longtemps déjà au Canada, et il n'a pas en aucun temps été associé à une mesure de protection de la vie privée…

Des organismes de surveillance plus dissuasifs

Les organismes chargés de l'application des lois visées par les deux projets de loi se voient octroyer des pouvoirs d'intervention renforcés, qui font d'eux des organismes qui devraient être plus à même de dissuader les contrevenants potentiels à la loi : pouvoir de rendre des ordonnances[528], pouvoirs d'enquête renforcés[529], pouvoir d'imposer des sanctions administratives pécuniaires[530], etc.

En mettant en place de sanctions administratives pécuniaires, réclamées depuis longtemps par les organismes intéressés, le législateur québécois répond à l'une des critiques les plus récurrentes à l'encontre des lois de protection des renseignements personnels ici et ailleurs : qu'elles ne sont que des « tigres de papier », menaçantes en apparence, mais inoffensives en pratique[531].

---

[525] Le projet de loi 64 prévoit que les renseignements doivent être transmis au particulier, alors que le projet de loi C-11 prévoit que les renseignements sont communiqués directement à l'organisation désignée par le particulier.
[526] Scassa au sujet du droit à la portabilité des données et du droit à l'oubli : « These are quasi-ownership rights » : T. SCASSA. « Data Ownership », CIGI Papers No. 187, septembre 2018, p.2, en ligne : https://www.cigionline.org/publications/data-ownership
[527] DE HERT, P. *et al.* « The right to data portability in the GDPR: Towards user-centric interoperability of digital services », Computer Law & Security Review, vol. 34, no. 2, avril 2018, p.194, en ligne : https://www.sciencedirect.com/science/article/pii/S0267364917303333 ; T. SCASSA. « Replacing Canada's 20-Year-Old Data Protection Law », CIGI, 23 décembre 2020, en ligne : https://www.cigionline.org/articles/replacing-canadas-20-year-old-data-protection-law ; VAN DER AUWERMEULEN, B. « How to attribute the right to data portability in Europe: A comparative analysis of legislations », Computer Law & Security Review, vol. 33, no. 1, février 2017, p.59, en ligne : https://www.sciencedirect.com/science/article/abs/pii/S0267364916302175
[528] CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 92(2).
[529] QUÉBEC. Projet de loi n° 64, *supra* note 479, arts 144 et ss.
[530] *Ibid.*, art 150 (qui ajoute les arts 90.1 et ss. à la LPRPSP).
[531] GOLLA, S. J. « Is Data Protection Law Growing Teeth: The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR », Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 8, no. 1, 2017, p.70.

Malheureusement, le législateur fédéral, de son côté, sape considérablement les nouveaux pouvoirs du Commissariat par la mise en place d'un palier additionnel : le tribunal de la protection des renseignements personnels et des données. En vertu du projet de loi C-11, il revient au tribunal d'imposer les sanctions que le Commissariat ne peut que recommander à ce dernier[532]. Qui plus est, ces sanctions ne sont possibles que pour une liste restreinte d'infractions à la loi[533]. Notons que les règles générales relatives à la forme et la validité du consentement ne sont pas visées[534] ! Il faut donc comprendre que, malgré certains changements, le législateur fédéral continue de favoriser une approche relativement « douce » pour son organisme chargé de veiller au respect de la loi en matière de protection de la vie privée : forcer l'entreprise à mettre fin à certaines pratiques non conformes, à en améliorer d'autres, mais rarement la punir financièrement (ou du moins ni rapidement, ni simplement).

Un nouveau droit d'action individuel et collectif

Les deux projets de loi apportent aussi des changements considérables en ce qui concerne les démarches individuelles que peuvent entreprendre les individus en réponse au traitement non conforme de leurs renseignements personnels.

Ces changements ont assurément pour but d'offrir davantage de pouvoir aux individus en cas de problème, en ce qu'ils élargissent le type de pénalités auxquelles s'expose une entreprise qui enfreint la loi et ouvrent davantage la porte au dédommagement individuel. Encore une fois, par contre, la version fédérale présente des limites et des obstacles dont les justifications sont difficiles à cerner.

Le projet de loi 64 (Qc) prévoit ainsi la possibilité pour les personnes qui auraient été victimes d'un manquement d'obtenir des dommages-intérêts compensatoires et même, dans certains cas, des dommages-intérêts punitifs[535]. Le projet de loi C-11 permet aussi l'obtention de dommages-intérêts, mais seulement si le Commissariat a préalablement conclu qu'il y a eu contravention à la loi (et que la conclusion a été confirmée par le tribunal, s'il y a eu appel)[536]. Ce faisant, de nombreuses victimes risquent d'être privées en pratique de ce droit, en raison notamment de la possibilité pour le Commissariat de conclure des accords de conformité qui mettent fin à l'examen d'une plainte[537]. Cette particularité du projet de loi fédéral est particulièrement décevante, en ce qu'elle conditionne ce droit des consommateurs à l'application de la loi par un organisme de surveillance dont le sous-financement est bien documenté[538]. Le sentiment d'impuissance du consommateur, que

---

[532] CANADA. Projet de loi C-11, *supra* note 480, partie 1, arts 94(1) et 93.
[533] *Ibid.*, art 93(1)
[534] *Ibid.*, art 93(1) c) et d). Seuls les articles 15(5) et 16 relatifs au consentement sont visés.
[535] QUÉBEC. Projet de loi n° 64, *supra* note 479, art 152 (qui prévoit l'ajout de l'art 93.1 à la *LPRPSP*).
[536] CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 106(1).
[537] *Ibid.*, art 86.
[538] Voir par exemple les propos du Commissariat en 2018 : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Le commissaire dénonce la lenteur des réformes visant les lois désuètes sur la protection des renseignements personnels », communiqué, 27 septembre 2018, en ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/nr-c_180927/

les projets de loi semblaient pourtant tenter d'atténuer, risque plutôt d'être amplifié par un système dont l'objectif et le fonctionnement semblent s'opposer !

5.2.1.3. Les lois canadiennes et l'économie fondée sur les données

Les lois canadiennes sur les renseignements personnels actuellement en vigueur ont été adoptées entre 1993 et 2003 ; les défis auxquels elles tentaient de répondre diffèrent considérablement de ceux d'aujourd'hui, notamment en termes d'échelle de grandeur. Les années qui ont suivi leur adoption ont été riches en développements. Les renseignements personnels des internautes ont gagné en importance dans le cadre d'une économie de plus en plus fondée sur les données (*data-driven economy*). Google s'est lancé dans la publicité comportementale en 2003 au moyen de sa branche publicitaire AdSense (et par l'achat de DoubleClick en 2007)[539]. Facebook a pris son envol en 2006[540]. Puis, est venu le boom des objets connectés en 2010[541]. Mayer-Schönberger et Padova résument ainsi la vision - aujourd'hui inadaptée - de l'encadrement européen (au parcours historique similaire à celui du Canada) :

> Unsurprisingly, the directive reflects a "small data" world in which data collection, storage and processing is still comparatively expensive and thus undertaken sparingly[542].

Malgré tout, les lois actuelles offrent certaines réponses aux préoccupations des consommateurs, grâce à deux principes directeurs qui s'avèrent pertinents au contexte des mégadonnées. Certains y voient une manière efficace d'en limiter la collecte et l'utilisation. Mais d'autres y voient plutôt une incompatibilité entre la loi et le terrain, dont l'effet ultime est d'entraver l'innovation sans pour autant assurer une application efficace de la loi[543].

> The big data business model is antithetical to data minimization. It incentivizes collection of more data for longer periods of time. It is aimed precisely at those unanticipated secondary uses, the "crown jewels" of big data[544].

La finalité de la collecte

Les quatre lois canadiennes prévoient toutes que l'entité qui collecte les renseignements personnels doit identifier à quelles fins elle le fait[545]. Elle doit ensuite divulguer ces fins aux

---

[539] OKO. « The History of Online Advertising, OKO Ad Management », 19 juillet 2019, en ligne : https://oko.uk/blog/the-history-of-online-advertising
[540] PHILLIPS, S. « A brief history of Facebook », The Guardian, 25 juillet 2007, en ligne : https://www.theguardian.com/technology/2007/jul/25/media.newmedia
[541] KHVOYNITSKAYA, S. The IoT history and future, ITransition, 25 novembre 2019, en ligne : https://www.itransition.com/blog/iot-history
[542] MAYER-SCHÖNBERGER. « Regime Change ? », *supra* note 546, p.321.
[543] Voir par exemple : ZARSKY. « Incompatible », *supra* note 546.
[544] TENE, O et POLONETSKY, J. « Big Data for All: Privacy and User Control in the Age of Analytics », Northwestern Journal of Technology and Intellectual Property, vol. 11, no. 5, 2013, pp.259-260, en ligne : https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip
[545] LPRPDE, *supra* note 77, annexe 1, art 4.2 ; LPRPSP, *supra* note 78, art 4 ; BCPIPA, *supra* note 78, art 10(1)a) ; APIPA, *supra* note 78, art 13(1)a).

personnes concernées. Cette obligation représente une limite considérable dans le contexte des mégadonnées puisqu'un des intérêts du phénomène concerne les données et inférences inattendues qui peuvent découler du traitement automatisé d'une telle quantité de renseignements personnels. Des chercheurs s'inquiètent que l'identification des finalités de la collecte par des entreprises désireuses de maintenir la plus-value du traitement des mégadonnées se fasse en respect du texte de la loi, mais non de son esprit/objectif, par la dénonciation, par exemple, de finalités floues[546].

En plus de l'obligation d'identifier à l'avance les fins de la collecte, la loi fédérale et les lois albertaine et britanno-colombienne imposent aussi des restrictions quant aux finalités qui sont acceptables, soit, uniquement, les « fins qu'une personne raisonnable estimerait acceptables dans les circonstances[547] ». Le Commissariat fédéral a publié des lignes directrices sur le sujet, qui pointaient par exemple du doigt les traitements discriminatoires, injustes ou contraires à l'éthique[548]. La loi québécoise prévoit pour sa part l'obligation pour une entreprise d'avoir un intérêt légitime dans le traitement des renseignements personnels auquel elle entend procéder[549]. Des chercheurs québécois sont d'avis qu'il y a ultimement une grande similarité entre les deux critères[550].

La minimisation ou limitation de la collecte et de la conservation

Un second principe des lois canadiennes vient également restreindre l'étendue de l'exploitation des mégadonnées, en limitant la collecte de renseignements qui sera permise[551] : ainsi, la loi prévoit que la collecte doit être minimale, c'est-à-dire se limiter aux renseignements qui seront nécessaires pour les fins identifiées[552]. Et cette notion de limitation se trouve également ailleurs dans les lois, notamment en ce qui concerne l'utilisation et la conservation des renseignements collectés passé certains délais ou certaines situations de fait. Historiquement, ce principe était enligné avec les pratiques des

---

546 ZARSKY, T. Z. « Incompatible: The GDPR in the Age of Big Data », Seton Hall Law Review, vol. 47, no. 4(2), 2017, en ligne : https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr ; MAYER-SCHÖNBERGER, V. et PADOVA, Y. « Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation », Columbia Science & Technology Law Review, vol. 17, 2016, p.322, en ligne : https://www.researchgate.net/publication/303665079_Regime_Change_Enabling_Big_Data_Through_Europe%27s_New_Data_Protection_Regulation

547 BCPIPA, *supra* note 78, arts 3 et 5(3) ; APIPA, *supra* note 78, art 3 (« for purposes that are reasonable »), LPRPDE, *supra* note 77, art 5(3).

548 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3) », mai 2018, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/

549 LPRPSP, *supra* note 78, art 4(1).

550 Ils sont d'avis que les lignes directrices du Commissariat à la protection de la vie privée du Canada, basées sur le critère fédéral, pourraient servir de guide d'interprétation au critère provincial également : DÉZIEL, P-L., BENYEKHLEF, K. et GAUMOND, E. « Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA », document de réponse aux questions posées par la Commission d'accès à l'information du Québec dans le cadre de la consultation sur l'intelligence artificielle, avril 2020, p.18, en ligne : http://collections.banq.qc.ca/ark:/52327/bs4067010

551 *Ibid.,* p.16.

552 LPRPDE, *supra* note 77, annexe 1, art 4.4 ; LPRPSP, *supra* note 78, art 5(1) ; BCPIPA, *supra* note 78, art 11(a) ; APIPA, *supra* note 78., art 11(2).

entreprises, dont les coûts de conservation des données excédaient leur intérêt potentiel, ce qui n'est certainement plus le cas aujourd'hui[553].

La prise en compte des besoins des entreprises dans la loi actuelle

Si les lois canadiennes de protection des renseignements personnels n'ont pas été conçues pour une économie axée sur l'exploitation des données et des renseignements personnels en ligne, il demeure que les législateurs ont historiquement porté une attention particulière (voire prioritaire) aux besoins des entreprises dans le cadre de l'élaboration de ces lois.

Rappelons que le Canada devait se doter d'un cadre législatif rapidement afin de faciliter ses relations commerciales avec l'Europe, et que c'est ce qui a mené à l'adoption de la *LPRPDE* en 2000. Le titre complet de la Loi mentionne expressément sa véritable finalité : la facilitation et la promotion du commerce électronique :

> Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions et en modifiant la Loi sur la preuve au Canada, la Loi sur les textes réglementaires et la Loi sur la révision des lois[554]

La protection des renseignements personnels apparait dès lors comme une manière d'encourager le commerce électronique en permettant aux entreprises, à certaines conditions, d'exploiter les renseignements personnels des consommateurs et en favorisant la confiance de ces derniers en cette pratique, vu l'existence de règles.

L'article 3 de la Loi mentionne que l'encadrement tient compte « du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels[555] ». Les besoins des entreprises et les droits des individus se voient donc placés sur un pied d'égalité dans ce qui se présente comme un exercice d'arbitrage. Le Commissaire fédéral a par le passé critiqué l'absence de reconnaissance officielle du droit à la protection de la vie privée dans la loi fédérale et s'est montré en faveur de l'ajout d'un préambule comme moyen d'enchâsser ce droit « dans le cadre qui lui est propre, soit celui des droits de la personne »[556].

---

[553] BENNETT, C. J. et BAYLEY, R. M. « Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments » dans VAN DER SLOOT, B., BROEDERS et SCHRIJVERS, E. Exploring the boundaries of Big Data, Amsterdam University Press, 2016, p.210, en ligne : https://www.wrr.nl/binaries/wrr/documenten/verkenningen/2016/04/28/exploring-the-boundaries-of-big-data-32/V032-Exploring-Boundaries-Big-Data.pdf

[554] LPRPDE, supra note 76.

[555] *Ibid.*, art 3.

[556] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Moderniser les lois fédérales en matière de protection de la vie privée pour mieux protéger les Canadiens », allocution, 9 mars 2020, en ligne : https://priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2020/sp-d_20200309/

Les lois albertaine et britanno-colombienne soulignent elles aussi que leur objectif est l'encadrement du traitement des renseignements personnels d'une manière qui reconnait à la fois le droit des individus à la protection de leurs renseignements et les besoins des entreprises[557]. La loi québécoise ne souligne pas aussi clairement l'importance des besoins des entreprises dans l'approche législative retenue en matière de protection des renseignements personnels, mais les dispositions qui s'y trouvent, notamment celles qui portent sur les exceptions au consentement, laissent tout de même penser que l'approche retenue est… essentiellement similaire.

5.2.1.3.1. Une plus grande place à l'anonymisation des renseignements dans les réformes législatives proposées

De manière générale, les projets de loi 64 et C-11 ne remettent pas en question l'approche des législateurs qui s'appuie sur une recherche d'équilibre entre les besoins économiques des entreprises et la protection de la vie privée des consommateurs. Le projet de loi fédéral éloigne même encore davantage la loi d'une reconnaissance d'un droit fondamental en faveur des consommateurs, malgré les demandes répétées du Commissariat fédéral.

> En réalité, le projet de loi accorde sans doute davantage de poids aux intérêts commerciaux que la loi actuelle, puisqu'il ajoute de nouveaux facteurs commerciaux à prendre en compte dans la balance sans évoquer les leçons tirées au cours des vingt dernières années quant aux effets perturbateurs de la technologie sur les droits.
>
> Selon nous, il serait normal et juste que les activités commerciales soient autorisées dans le respect des droits, plutôt que de mettre les droits et les intérêts commerciaux sur le même pied[558].

Le Commissariat, citant les travaux de la professeure Teresa Scassa, souligne d'ailleurs que le fait d'aborder la loi sous l'angle de la protection d'un droit humain offrirait davantage de flexibilité pour son interprétation et son évolution. Au-delà du péril qu'elle représente pour le droit individuel à la protection de sa vie privée, la surveillance de masse peut nuire au bien-être collectif ou encore porter atteinte à d'autres droits, tels que le droit à l'égalité et à la protection contre la discrimination[559].

Les projets de loi maintiennent également les règles relatives à la minimisation de la collecte de renseignements personnels et à l'identification préalable de ses fins, mais le projet de loi québécois prend tout de même acte des critiques de l'industrie relativement

---

[557] BCPIPA, *supra* note 78, art 2 ; APIPA, *supra* note 78, art 3.
[558] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre de la Charte du numérique », 11 mai 2021, en ligne : https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_ethi_c11_2105/#toc3-1
[559] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. Ù Réforme des lois sur la vie privée : Pour faire respecter les droits et rétablir la confiance envers le gouvernement et l'économie numérique », rapport annuel au Parlement 2018-2019 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques, 2019, en ligne : https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201819/ar_201819/#heading-0-0-3-1

à l'applicabilité difficile du deuxième principe en regard des mégadonnées. Il propose l'ajout d'une exception à l'obligation de mentionner toutes les finalités avant la collecte ou l'utilisation des renseignements personnels : l'entreprise n'aura pas à préciser les fins additionnelles de traitement des données qui sont compatibles avec celles pour lesquelles il y a préalablement eu consentement[560]. Notons que cette exception est plus restrictive que son pendant européen, qui prévoit cette possibilité à moins que les nouvelles fins soient incompatibles[561].

Les projets de loi viennent par ailleurs définir et encadrer davantage les pratiques de dépersonnalisation et d'anonymisation des données collectées, ce qui n'est pas négligeable dans le contexte des mégadonnées et du traitement des renseignements personnels au moyen de l'intelligence artificielle. À ce sujet, le législateur fédéral semble davantage conscient des risques de réidentification et met de l'avant une définition plus contraignante des renseignements dépersonnalisés, qui exclut les renseignements qui, seuls ou en combinaison avec d'autres, pourraient permettre d'identifier l'individu concerné[562]. La définition équivalente prévue au projet de loi 64 ne tient pas compte de l'identification indirecte[563]. Mais le projet de loi québécoise définit tout de même le concept d'anonymisation : un renseignement est anonymisé lorsqu'il ne permet plus d'identifier directement ou indirectement la personne concernée, et ce, de façon irréversible[564]. Les lois albertaine et britanno-colombienne, qui ne font pas l'objet de réforme pour l'instant, ne font pas mention de ces concepts.

L'inclusion de ces définitions est particulièrement intéressante puisque les renseignements dépersonnalisés ne sont plus, en principe, des renseignements personnels pour lesquels les lois de protection trouvent application (et donc pour lesquels un consentement est requis préalablement à leur traitement par des entreprises)[565]. Étant donné que le traitement des mégadonnées augmente les risques de réidentification de renseignements pourtant dépersonnalisés[566], il est prometteur de voir les législateurs traiter de dépersonnalisation et d'anonymisation avec prudence.

---

[560] QUÉBEC. Projet de loi n° 64, *supra* note 479, art 100 (qui prévoit le nouvel art 12(2)1) de la *LPRPSP*).
[561] RGPD, *supra* note 55, art 5(b) ; SEINEN, W., WALTER, A. et VAN GRONDELLE, S. « Compatibility as a Mechanism for Responsible Further Processing of Personal Data», p.3, en ligne : https://www.bakermckenzie.com/-/media/files/insight/publications/2018/10/compatibility_mechanism_responsible_further_personal_data_processing.pdf?la=en
[562] CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 2, définition de « dépersonnaliser ».
[563] QUÉBEC. Projet de loi n° 64, *supra* note 479, art 100 (qui prévoit le nouvel art 12(4)1) de la *LPRPSP*).
[564] *Ibid.*, art 111 (qui prévoit le nouvel art 23 de la LPRPSP).
[565] Notons à ce sujet que le projet de loi fédéral aborde tout de même le traitement des renseignements suivant la dépersonnalisation dans plusieurs articles du projet de loi C-11. Certains y voient une confusion du législateur fédéral, alors que d'autres y voient une reconnaissance par ce dernier des limites des processus actuels de dépersonnalisation ; voir aussi à ce sujet : SCASSA, T. « Data for Good?: An Assessment of the Proposed Exception in Canada's Private Sector Data Protection Law Reform Bill », 6 décembre 2020, en ligne : http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=335:data-for-good?-an-assessment-of-the-proposed-exception-in-canada%E2%80%99s-private-sector-data-protection-law-reform-bill&Itemid=80
[566] BENNETT, C. J. et BAYLEY, R. M. « Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments » dans VAN DER SLOOT, B., BROEDERS et SCHRIJVERS, E. Exploring the boundaries of Big Data, Amsterdam University Press, 2016, p.210, en ligne : https://www.wrr.nl/binaries/wrr/documenten/verkenningen/2016/04/28/exploring-the-boundaries-of-big-data-32/V032-Exploring-Boundaries-Big-Data.pdf ; voir à ce sujet les exemples de ré-identification « accidentelle » dans PURTOVA, N. « The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law »,

5.2.2 Préoccupations spécifiques relatives à la sécurité des renseignements personnels collectés, traités et conservés

Les lois actuelles de protection des renseignements personnels contiennent certaines dispositions pertinentes à la sécurité des systèmes de traitement et de conservation des données. Leur présence tend à démontrer que les législateurs, contrairement à certains experts, ne distinguent pas pleinement la sécurité des données et la protection de la vie privée, ou à tout le moins, qu'ils les perçoivent comme complémentaires.

De manière générale, les lois ne dictent pas aux entreprises comment elles doivent assurer la sécurité, l'intégrité et la confidentialité des renseignements personnels qu'elles collectent et détiennent. Elles prévoient des obligations plus générales en la matière[567] et certaines précisent que le degré de protection doit notamment tenir compte du type et de la sensibilité des renseignements en cause[568]. La loi fédérale est la seule qui entre davantage dans les détails, en imposant expressément la mise en place de mesures de protection administratives, techniques et matérielles[569].

La responsabilité de l'entreprise qui transfère les renseignements personnels qu'elle détient à des entreprises tierces engagées pour l'aider dans le traitement desdits renseignements fait l'objet d'un traitement inégal selon les législateurs canadiens. Seule la loi fédérale prévoit expressément que l'entreprise doit s'assurer de la suffisance de la protection offerte par l'entreprise tierce (qui doit être d'un degré comparable à celui qu'impose la loi[570]). Les lois albertaine et britanno-colombienne soulignent de manière plus générale la responsabilité des entreprises en regard des données sous leur contrôle[571]. La loi québécoise est étonnamment silencieuse sur cette question.

5.2.2.1 L'élimination des renseignements personnels détenus

La loi québécoise parait également inachevée en ce qui concerne le traitement à réserver aux renseignements personnels lorsque leur utilisation est complétée ou lorsqu'ils ne devraient plus être utilisés ; la loi indique simplement que l'utilisation n'est alors plus permise.

Law, Innovation and Technology, vol. 10, no. 1, 2018, pp.7-8, en ligne : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355 ; FASKEN. « Privacy and Cybersecurity Bulletin », 1er mars 2021, en ligne : https://www.fasken.com/en/knowledge/2021/03/1-de-identification-of-personal-information-under-the-proposed-consumer-privacy-protection-act

[567] LPRPDE, *supra* note 77 annexe 1, arts 4.7 et 4.7.1 ; BCPIPA, *supra* note 78, art 35 ; APIPA, *supra* note 78, art 34 ; LPRPSP, *supra* note 78, art 10.

[568] LPRPSP, supra note 77, art 10 ; LPRPDE, supra note 76, annexe 1, arts 4.7 et 4.7.2.

[569] LPRPDE, *supra* note 77, annexe 1, art 4.7.3.

[570] LPRPDE, supra note 76, annexe 1, art 4.1.3 et art 7.2(2).

[571] BCPIPA, *supra* note 78, art 4(2) ; APIPA, *supra* note 78, art 5(1).

À l'inverse, les lois fédérale, albertaine et britanno-colombienne prévoient que les renseignements doivent être détruits, effacés ou dépersonnalisés après usage[572]. La *LPRPDE* prévoit d'ailleurs qu'une organisation doit élaborer des lignes directrices sur cette question et prévoir des durées maximales de conservation[573].

5.2.2.2 L'envoi d'un avis en cas d'incident de confidentialité

La *LPRPDE* prévoit une obligation pour les entreprises de déclarer au Commissaire à la protection de la vie privée et à l'individu concerné une atteinte aux mesures de sécurité qui résulterait en une communication non autorisée, une perte ou un accès non autorisé aux renseignements personnels qu'elles détiennent, s'il est raisonnable de croire que l'atteinte présente un risque réel de préjudice grave pour l'individu en question[574]. Les entreprises doivent tenir un registre des atteintes pertinentes[575].

De manière générale, les règles relatives à l'envoi d'avis à la suite d'un bris de sécurité ou de confidentialité s'expliquent par la volonté du législateur d'assurer une réponse rapide des entités et des individus concernés afin d'éviter une violation de la vie privée ou d'en diminuer l'impact, le cas échéant[576].

Notons que les obligations de notification des incidents de confidentialité prévues à la *LPRPDE* sont moins onéreuses que celles qu'on retrouve dans le *RGPD* de l'Union européenne. Les entreprises soumises à la loi européenne ont en effet l'obligation de rapporter tout incident aux autorités compétentes, à moins qu'il « ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques[577] ». Ce n'est que lorsqu'il est question de l'envoi d'un avis distinct aux individus concernés que la question du préjudice susceptible d'être causé par l'atteinte aux mesures de sécurité est prise en compte[578]. Ce faisant, les autorités compétentes sont vraisemblablement plus à même de dresser un portrait de l'état des mesures de sécurité dans certains secteurs et d'intervenir rapidement en présence de problèmes récurrents. La disposition canadienne se distingue aussi de celles adoptées dans certains États américains en matière d'avis d'incident, en ce qu'elle ne prévoit pas de délais spécifiques pour aviser (ex. : 30-45 jours)[579], mais demande plutôt d'agir « le plus tôt possible [580]». Soulignons aussi l'inclusion dans certaines lois américaines d'une obligation – sans équivalent au Canada - pour les entreprises

---

572 LPRPDE, supra note 76, annexe 1, arts 4.5 à 4.5.4 ; BCPIPA, supra note 77, art 35(2) ; APIPA, supra note 77, art 35(2).
573 LPRPDE, supra note 76, annexe 1, art 4.5.2.
574 *Ibid.*, arts 10.1(1) et 10.1(3) et 2(1).
575 *Ibid.*, art 10.3(1).
576 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES. « Guidelines on Personal data breach notification under Regulation 2016/679 », 18/EN WP250rev.01, 3 octobre 2017, p.6.
577 RGPD, supra note 54, art 33(1).
578 *Ibid.*, arts 33 et 34.
579 SERRATO, J. K. *et al*. « US states pass data protection laws on the heels of the GDPR », 9 juillet 2018, Norton Rose Fullbright, en ligne : https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/
580 LPRPDE, supra note 76, art 10.1(2).

d'aviser les agences d'évaluation du crédit lors de certains incidents de confidentialité qui affectent des consommateurs[581].

La loi albertaine oblige elle aussi l'envoi obligatoire d'avis au Commissaire, mais pas aux individus directement[582]. Aucune des deux autres lois provinciales applicables au secteur privé ne prévoit de disposition à ce sujet. Ces règles figurent à la *LPRPDE* depuis 2018 seulement[583], mais à la loi albertaine depuis plus de 10 ans[584] !

5.2.2.3. Des compléments importants dans les réformes législatives proposées

Parmi les changements les plus significatifs prévus aux projets de loi C-11 (fédéral) et 64 (Qc), nous notons l'inclusion de dispositions relatives à la sécurité des systèmes de traitement et de conservation des renseignements personnels des entreprises. Les changements proposés sont inspirés de dispositions existantes dans d'autres lois canadiennes ou dans le *RGPD*.

La volonté de moderniser considérablement les obligations des entreprises en matière de sécurité des données parait être en phase avec les préoccupations accrues des consommateurs à ce sujet. Elle reflète également, indéniablement, la place importante que prend Internet dans les démarches de réformes.

L'évaluation préalable des risques

Le projet de loi 64 oblige les entreprises à procéder à une évaluation des facteurs de risque pour la protection de la vie privée (EVFP) avant la mise en place de tout système d'information ou de prestation électronique de service qui impliquerait le traitement de renseignements personnels[585]. Cette obligation va plus loin que celle prévue par exemple à la *LPRPDE* en ce qui concerne l'implantation de mesures de sécurité pour les systèmes ; en fait, l'entreprise devra choisir et implanter les mesures à la lumière des résultats de son analyse des risques[586]. L'EVFP québécois est largement inspiré de l'analyse d'impact relative à la protection des données (AIPD) développée en Europe[587].

Ce type d'analyse a pour but d'aider les entreprises à mettre en place des mesures qui répondent à leurs obligations légales. En ce sens, elles servent d'outils d'auto responsabilisation, ce qui n'est pas sans rappeler l'approche d'accompagnement favorisée

---

581 Voir par exemple les explications au sujet des dispositions adoptées en Alaska, au Colorado, au Rhode Island et au Vermont : DIGITAL GUARDIAN. « The Definitive Guide to U.S. State Data Breach Laws », 2018, en ligne : https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf
582 A APIPA, *supra* note 78, art 34.1.
583 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Un an après l'entrée en vigueur des déclarations obligatoires des atteintes à la protection des données : ce que nous avons appris et ce que les entreprises doivent savoir », 31 octobre 2019, en ligne : https://www.priv.gc.ca/fr/blogue/20191031/
584 ALBERTA. Personal Information Protection Amendment Act, 2009, SA 2009, c 50.
585 QUÉBEC. Projet de loi n° 64, *supra* note 479, art 95 (qui ajoute l'art 3.3 à la *LPRPSP*).
586 RGPD, supra note 54, préambule, para 84.
587 *Ibid.*, art 35.

par certains organismes de surveillance du respect de la loi[588]. Dans ses lignes directrices, le Groupe de travail « article 29 » sur la protection des données souligne ainsi la plus-value de ces analyses pour les entreprises afin de se conformer aux lois[589] (au-delà de leur obligation à procéder à l'analyse elle-même).

En adaptant cette création européenne dans le projet de loi 64, le législateur québécois a malheureusement soustrait un volet important de l'analyse des risques. Seuls les impacts pour la protection de la vie privée sont pris en compte ; le modèle européen traite plus largement des droits et libertés des individus affectés, ce qui comprend en outre la protection de la liberté d'expression et de mouvement et le droit de ne pas faire l'objet de discrimination, par exemple[590]. Ce choix de ne pas considérer l'impact du traitement des renseignements personnels sur d'autres droits fondamentaux est réitéré dans le projet de loi lorsqu'il est question du traitement automatisé des données à des fins décisionnelles[591].

Les avis d'incidents

Le projet de loi québécois intègre finalement des dispositions relatives à l'envoi d'avis d'incidents de confidentialité à la Commission et aux individus concernés, « [s]i l'incident présente un risque qu'un préjudice sérieux soit causé »[592]. Ces dispositions ressemblent beaucoup à celles qui sont déjà présentes à la *LPRPDE*. Après l'adoption du projet, il ne restera donc que la loi britanno-colombienne dans laquelle cette obligation sera toujours manquante.

Le traitement des fraudes qui découlent des atteintes à la vie privée en ligne

Les consommateurs canadiens interrogés dans le cadre de notre sondage se montrent particulièrement préoccupés par la fraude ou le vol de leur identité qui découleraient d'un accès non autorisé à leurs renseignements personnels détenus par une entreprise.

---

[588]Notons que le Commissariat à la protection de la vie privée du Canada offre depuis longtemps un outil et un guide d'évaluation sur son site Web : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Outil d'autoévaluation – LPRPDE », juillet 2008, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/conformite-a-la-lprpde-et-outils-de-formation/pipeda_sa_tool_200807/ ; La Commission d'accès à l'information fournit elle aussi un guide d'accompagnement en ligne : COMMISSION D'ACCÈS À L'INFORMATION. « Guide d'accompagnement, mai 2020, en ligne : https://www.cai.gouv.qc.ca/documents/Guide_EFVP_FR.pdf

[589] GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES. « Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 », 17/EN WP 248, 4 avril 2017, p.19, en ligne : https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/wp248_enpdf.pdf

[590] *Ibid.*, p.15.

[591] Voir les commentaires de la Ligue des droits et libertés : LIGUE DES DROITS ET LIBERTÉS. « Mémoire, consultations particulières et auditions publiques au sujet du projet de loi 64 : loi modernisant des dispositions législatives en matière de protection des renseignements personnels », 2020, pp.9-10, en ligne : https://liguedesdroits.ca/wp-content/fichiers/2020/09/memoire_projet_loi_64_renseignement_personnel_20200923.pdf

[592] QUÉBEC. Projet de loi n° 64, *supra* note 479, art 95 (qui ajoute l'art 3.5 à la *LPRPSP*).

Similairement aux lois actuellement en vigueur, les projets de loi n'abordent pas spécifiquement ces conséquences ou l'aide qui peut être apportée aux consommateurs qui en seraient victimes. La fraude liée à l'identité et le vol d'identité sont couverts par des infractions prévues au Code criminel canadien. Une personne qui en est victime sera dès lors dirigée vers les corps policiers et le Centre antifraude du Canada[593].

Soulignons tout de même que le législateur québécois s'est attardé plus spécifiquement à l'un des aspects de cette problématique à la suite de la fuite de données chez Desjardins. La *Loi sur les agents d'évaluation du crédit* a été adoptée en octobre 2020 et prévoit certaines protections pertinentes que doivent maintenant offrir ces entreprises avec lesquelles sont susceptibles de faire affaire les victimes d'une fuite ou d'un vol de leurs renseignements personnels pour limiter les risques ou les effets d'un vol d'identité. Les consommateurs peuvent ainsi appliquer un gel de sécurité à leur dossier afin de limiter la communication de renseignements à des tiers[594], recevoir une alerte de sécurité lors d'une communication[595] et faire ajouter une note explicative à leur dossier de crédit[596]. Précisons que les notes explicatives du projet de loi ne font aucune mention de la protection de la vie privée des Québécois, mais abordent plutôt la nécessité d'encadrer les pratiques commerciales des agences d'évaluation du crédit[597], pratiques qui avaient fait l'objet d'une couverture négative importante dans les mois précédant le dépôt du projet[598]. Les bénéfices potentiels pour les consommateurs en regard du traitement de leurs renseignements personnels sont dès lors une conséquence positive, mais non la raison d'être de cette nouvelle loi.

Nous constatons donc que, malgré une volonté indéniable du législateur d'intégrer davantage de dispositions relatives à la sécurité des systèmes informatiques et des renseignements personnels qu'ils contiennent aux lois de protection des renseignements personnels, certains sujets demeurent traités indépendamment, notamment lorsqu'il est question de certaines conséquences qui découleraient d'un non-respect des lois de protection des renseignements personnels.

---

[593] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Le vol d'identité et vous », octobre 2020, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/identites/vol-d-identite/guide_idt/
[594] QUÉBEC. Loi sur les agents d'évaluation du crédit, LQ 2020, c 21, art 9.
[595] *Ibid*., art 10.
[596] *Ibid.*, art 11.
[597] QUÉBEC. Projet de loi 53. Loi sur les agents d'évaluation du crédit, première session, quarante-deuxième législature, 2019, notes explicatives.
[598] Voir par exemple : « Des clients de Desjardins excédés par le temps d'attente chez Equifax », TVA Nouvelles, 3 juillet 2019, en ligne : https://www.journaldemontreal.com/2019/07/03/des-clients-de-desjardins-excedes-par-le-temps-dattente-chez-equifax-1 ; « Des clients de Desjardins peinent à se faire servir en français par Equifax », Radio-Canada, 4 juillet 2019, en ligne https://ici.radio-canada.ca/nouvelle/1211212/clients-desjardins-equifax-difficultes-service-francais-oqlf ; BORDELEAU, S. « « Inacceptable » : Desjardins lance des mesures pour pallier les « ratés » d'Equifax », Radio-Canada, 5 juillet 2019, en ligne : https://ici.radio-canada.ca/nouvelle/1211973/desjardins-mesures-accelerer-activation-forfaits-equifax

5.2.3 Préoccupations spécifiques relatives à l'utilisation des renseignements personnels à des fins commerciales

Les pratiques de suivi et de profilage des consommateurs en ligne ont pris de l'ampleur dans les dernières décennies. Les lois actuelles de protection des renseignements personnels, qui n'ont pas été pensées dans ce contexte, peinent à s'appliquer efficacement.

Pour que les lois trouvent application, il faut d'abord que les données collectées et utilisées constituent des renseignements personnels au sens des lois : ils sont généralement définis comme des renseignements qui concernent un individu identifiable ou qui permettent de l'identifier. À elles seules, des données comme l'adresse IP d'un individu ou le numéro de série de son appareil de connexion ne permettront pas d'identifier un individu. Leur traitement est-il visé par les lois ?

Puisque la collecte et l'utilisation de ces données sont destinées à permettre le développement de publicités personnalisées, adaptées au comportement des individus, le Commissariat à la protection de la vie privée du Canada a émis l'avis, dans des lignes directrices, que les renseignements qui servent au suivi et au ciblage en ligne sont généralement visés par la loi[599].

Cette fin spécifique du traitement des renseignements personnels ne fait pas l'objet de règles particulières. Il faut donc se référer aux règles générales des différentes lois, principalement en matière de consentement. Notons que le consentement implicite, dont les nombreux problèmes ont été abordés précédemment, est généralement jugé acceptable dans un contexte de publicité ciblée en ligne, si l'entreprise a respecté ses obligations de transparence[600].

5.2.3.1 Des réformes dont les effets demeurent incertains

Les projets de loi apportent des changements aux règles du consentement qui peuvent être pertinentes au suivi en ligne et à l'utilisation des renseignements personnels à des fins de profilage et de publicités ciblées. Par contre, leur effet exact demeure incertain, considérant certaines exceptions mises de l'avant par les législateurs.

---

[599] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Le vol d'identité », *supra* note 593 ; voir une analyse plus détaillée de l'adéquation de la définition de «renseignement personnel» au pratique de publicité comportementale : OPTION CONSOMMATEURS. « Le prix de la gratuité - Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne? », juin 2015, pp.38-40, en ligne : https://option-consommateurs.org/wp-content/uploads/2017/06/option-consommateurs-2014-2015-gratuite-rapport.pdf

[600] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Lignes directrices », *supra* note 506 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Position de principe sur la publicité comportementale en ligne », décembre 2015, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/

De manière générale, les entreprises ont l'obligation de dévoiler aux consommateurs les raisons de la collecte de renseignements personnels et l'utilisation qu'elles comptent en faire. Le projet de loi québécois précise expressément que cette divulgation doit comprendre la dénonciation du recours à une technologie dont les fonctions permettent d'identifier ou de localiser l'internaute ou d'effectuer son profilage, le cas échéant[601].

En ce qui concerne le consentement requis du consommateur, le projet C-11 prévoit une exception lorsque la collecte ou l'utilisation est faite en vue d'une activité d'affaires et qu'une personne raisonnable pourrait s'y attendre. On donne spécifiquement l'exemple des « activités dans le cadre desquelles il est pratiquement impossible pour l'organisation d'obtenir le consentement de l'individu, en raison de l'absence de lien direct avec celui-ci[602] », ce qui risque fort d'inclure plusieurs entreprises tierces qui procèdent à l'analyse de données, notamment à des fins de marketing[603]. Ce contournement du consentement n'est toutefois pas possible lorsque les renseignements personnels sont recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu[604], ce qui devrait logiquement toucher le phénomène de la publicité ciblée[605]. Mais tous les traitements de données à des fins commerciales n'ont pas directement pour but d'influencer le comportement…

Par ailleurs, rappelons que le projet de loi C-11 maintient la possibilité de se contenter d'un consentement implicite pour procéder au traitement des renseignements personnels. Similairement, le projet de loi québécois permet de considérer, selon les circonstances, l'existence d'un consentement implicite[606], même si un consentement distinct est requis pour chacune des fins pour lesquelles seront collectées les données. Il est difficile de concevoir comment ces deux règles coexisteront et quel type de consentement serait ultimement valable pour procéder au traitement de renseignements personnels à des fins d'identification, de localisation et de profilage ou lorsqu'ils sont destinés à être vendus à d'autres entités.

Le législateur québécois semble conscient du désir de plusieurs internautes de refuser en bloc les différentes formes de suivi en ligne. Sans leur donner réellement les outils pour y arriver, il prévoit tout de même certaines obligations de transparence additionnelles. Ainsi, les entreprises qui offrent des moyens pour désactiver les fonctions d'identification, de localisation et de profilage doivent en informer les consommateurs[607]. Rien par contre si les entreprises n'offrent pas volontairement ces fonctions, et aucune obligation de le faire…

Les projets de loi canadiens n'abordent pas spécifiquement l'enjeu de la vente de renseignements personnels à des entités tierces (mise à part une obligation de divulguer

---

601 QUÉBEC. Projet de loi n° 64, *supra* note 479, art 18 (qui ajoute l'art 65.0.1(1)1°) à la *LPRPSP*).
602 CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 18(2)e).
603 YOUNG, D. « New federal privacy law – a fine balance between the GDPR and PIPEDA? », 2020, en ligne : http://davidyounglaw.ca/compliance-bulletins/new-federal-privacy-law-a-fine-balance-between-the-gdpr-and-pipeda/
604 CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 18(1)b).
605 YOUNG. « New federal privacy law », *supra* note 603.
606 En l'interdisant *a contrario* pour les renseignements personnels sensibles : QUÉBEC. Projet de loi n° 64, *supra* note 479, art 19 (qui modifie l'art 65.1 de la LPRPSP).
607 *Ibid.*, art 18 (qui ajoute l'art 65.0.1(1)1°) à la LPRPSP).

le nom ou le type de parties tierces avec qui les données collectées pourraient être partagées[608]).

Il s'agit d'un sujet qui, ici comme ailleurs, fait l'objet de trop peu de discussion de la part des législateurs et régulateurs[609]. Notons tout de même quelques initiatives américaines sur le sujet. La *California Consumer Privacy Act*, par exemple, reconnait aux individus le droit de refuser la vente de renseignements personnels à des tiers. L'entreprise a ainsi l'obligation de l'aviser de la possibilité d'une vente future et de lui donner l'opportunité de s'y opposer[610]. De même, des lois californienne et vermontoise relatives aux courtiers de données favorisent une plus grande transparence, en forçant l'enregistrement auprès de l'État des entreprises de courtage de données[611].

5.2.4 Préoccupations spécifiques relatives à la réception de courriers électroniques indésirables

L'adresse courriel d'un individu constitue sans contredit un renseignement personnel. La collecte et l'utilisation de ce renseignement personnel sont donc théoriquement soumises aux règles générales prévues aux différentes lois, dont celles qui portent sur le consentement. Par contre, le législateur fédéral a choisi de traiter spécifiquement du problème des communications électroniques indésirables dans le cadre d'un régime réglementaire distinct établi par la *Loi canadienne anti-pourriel* (*LCAP*). Trois entités partagent la responsabilité de l'application de la *LCAP* : le Commissariat à la protection de la vie privée du Canada, le Conseil de la radiodiffusion et des télécommunications canadiennes et le Bureau de la concurrence du gouvernement fédéral[612]. L'implication de ces deux derniers organismes confirme que le problème n'est pas uniquement perçu comme une atteinte à la vie privée, mais aussi comme un problème commercial et technologique. En fait, la protection de la vie privée n'est pas l'élément central du cadre législatif. L'objectif de la loi est plutôt « de promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation des pratiques commerciales qui découragent l'exercice des activités commerciales par voie électronique[613] ». Cela n'est pas sans rappeler l'objectif de la *LPRPDE,* qui réfère elle aussi à des considérations davantage économiques que de droits humains.

---

608 CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 15(3)e).
609 SHERMAN, J. « Federal Privacy Rules Must Get "Data Broker" Definitions Right », LawFare, 8 avril 2021, en ligne: https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right
610 ÉTAT DE LA CALIFORNIE. California Consumer Privacy Act of 2018, arts 1798.120 et 1798.115(d).
611 California Civil Code § 1798.99.80 ; Vermont Statute 9 V.S.A. § 2430.
612 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Forme de consentement », mars 2014, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/loi-canadienne-anti-pourriel/casl_faqs_2014/
613 CANADA. Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications, L.C. 2010, ch. 23.

En voulant limiter l'envoi de pourriels et les désagréments qu'ils occasionnent à l'ensemble des parties intéressées, le législateur fédéral se trouve à renforcer les protections offertes aux consommateurs en ce qui concerne l'utilisation de leurs renseignements personnels. Ainsi, ironiquement, les règles prévues à la *LCAP* en matière de consentement sont plus sévères que celles qui sont prévues à la *LPRPDE* ; on y interdit l'envoi de messages électroniques commerciaux sans le consentement exprès ou tacite du destinataire, sauf exception (mise en place d'un système d'*opt-in* spécifique aux communications électroniques[614] alors que la *LPRDPE* permet le recours général à un modèle d'*opt-out*, sauf exception[615]).

Pourquoi une telle restriction au consentement implicite pour les communications électroniques, mais pas pour le suivi en ligne par exemple ? Le législateur fédéral considère-t-il l'un comme plus attentatoire à la vie privée des individus que l'autre ? Ou s'agit-il plutôt d'une confirmation que ce sont les considérations économiques qui sont déterminantes dans le choix du cadre réglementaire en matière de protection des renseignements personnels ? Dans un cas, la pratique est perçue comme une nuisance au bon fonctionnement de l'économie numérique, alors que dans l'autre, elle semble plutôt perçue comme une nécessité.

Soulignons par ailleurs que la *LCAP* fait l'objet de problèmes similaires à ceux que l'on trouve à la *LPRPDE* en ce qui concerne les recours individuels des consommateurs. L'entrée en vigueur des dispositions relatives aux dommages et intérêts compensatoires et statutaires qui peuvent être réclamés par les consommateurs advenant le non-respect de la Loi est suspendue depuis 2017 (année d'entrée en vigueur des dispositions relatives au consentement requis pour l'envoi des communications visées)[616]. Rien n'indique que le législateur entend procéder à leur mise en vigueur prochainement. Le consommateur est donc, encore une fois, privé d'un dédommagement utile en cas d'atteinte à sa vie privée en ligne.

La *LCAP* n'a pas fait l'objet de modifications depuis 2015.

---

[614] CRTC. « Bulletin d'information de Conformité et Enquêtes CRTC 2012-549 », 10 octobre 2012, en ligne : https://crtc.gc.ca/fra/archive/2012/2012-549.htm ; FEKETE, M. et KARDASH, A. « CASL compliance: More than spam. Understanding Canada's anti-spam law », Osler, en ligne : https://www.osler.com/en/resources/in-focus/casl-compliance-more-than-spam-understanding-canada-s-anti-spam-law (consulté le 10 juillet 2021).
[615] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. Forme de consentement, *supra* note 612.
[616] MARUSYK, R. et LANFRANCONI, D. « Canada: Update: CASL Private Right Of Action Suspended, But Be Careful, Other CASL Provisions Are Still Alive », Mondaq, 20 juillet 2017, https://www.mondaq.com/canada/class-actions/610750/update-casl-private-right-of-action-suspended-but-be-careful-other-casl-provisions-are-still-alive ; BRUINEMAN, M. « Fate of controversial CASL », Law Times, 19 mars 2018, en ligne : https://www.lawtimesnews.com/practice-areas/privacy-and-data/fate-of-controversial-casl-section-unknown/262966

5.2.5 Préoccupations spécifiques relatives aux atteintes à la réputation et à l'intégrité psychologique et physique des internautes

De manière générale, la protection de la réputation et du bien-être physique et psychologique des internautes dépasse la portée des encadrements en matière de protection des renseignements personnels au Canada.

On ne trouve ainsi aucune disposition qui traite expressément de la réputation des individus dans le cadre des lois provinciales de protection des renseignements personnels. Une seule mention figure à la loi fédérale ; l'atteinte à la réputation d'un particulier y est mentionnée comme étant un préjudice grave survenu à la suite d'une atteinte aux mesures de sécurité qui donne ouverture à l'application de l'article 10.1 (déclaration obligatoire d'un bris de sécurité au commissaire et à l'intéressé)[617].

La réputation et l'intégrité des individus en ligne sont plutôt abordées par les législateurs sous l'angle de la responsabilité des plateformes, du droit criminel ou du droit civil (en matière de diffamation). Le harcèlement en ligne et la diffusion de contenus intimes sans le consentement font, par exemple, l'objet de dispositions au *Code criminel*[618]. Et des changements législatifs sont attendus en ce qui concerne le traitement de certains contenus haineux ou illégaux sur les plateformes de partage et de communication en ligne[619].

Et le choix des législateurs d'aborder ces enjeux dans des lois et règlements distincts se fait sentir. Une victime d'une atteinte à sa réputation qui découlerait de l'utilisation de ses renseignements personnels ne sera que très peu outillée par les lois de protection des renseignements personnels, fédérale ou provinciales pour entreprendre un recours ou chercher réparation, voire même pour faire cesser une atteinte.

Certes, le droit à la correction de renseignements personnels inexacts détenus par une entité et l'obligation pour cette entité de ne plus utiliser les renseignements personnels une fois l'objet de la collecte accompli qui figurent aux lois existantes peuvent s'avérer utiles à l'occasion. Mais ces mesures offrent un redressement très imparfait et incomplet. Les lois ne s'appliquent que dans le cadre de l'exploitation d'une entreprise ou d'une activité commerciale, alors que certains sites Web ne sont destinés qu'à un usage personnel non commercial. Et les objectifs de la collecte et de l'utilisation de renseignements sont difficiles à délimiter dans le temps dans le contexte des médias sociaux, où se produisent plus souvent qu'autrement les situations susceptibles d'atteindre à la réputation ou à l'intégrité des internautes[620].

Les lois actuelles ne prévoient pas non plus de mesures spécifiques concernant les personnes mineures, dont la réputation et l'intégrité sont davantage à risque en ligne. Les

---

[617] LPRPDE, supra note 76, arts 10.1(1) et 10.1(3).
[618] Voir par exemple : CANADA. Code criminel, LRC 1985, c C-46, arts 162 et 264.
[619] PAULS, K. « New rules on removal of illegal online content could help in battle against child pornography », Radio-canada, 4 janvier 2021, en ligne : https://www.cbc.ca/news/canada/manitoba/canada-illegal-online-content-child-porn-1.5847695
[620] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Réputation en ligne », *supra* note 178.

lois provinciales actuelles ne mentionnent pas l'âge à partir duquel les individus sont (généralement) en mesure de comprendre pleinement les conséquences de leurs choix concernant la protection de leur vie privée et d'offrir un consentement valable. La loi fédérale non plus, mais le Commissariat a publiquement évalué cet âge à 13 ans[621].

5.2.5.1. Des changements au Québec seulement

Aucune disposition proposée aux projets de loi C-11 (Canada) et 64 (Québec) ne concerne les comportements antisociaux de type harcèlement, menace ou autres. Le traitement de cette problématique demeure donc distinct de l'encadrement en matière de protection des renseignements personnels.

Le projet de loi fédéral ne comprend pas non plus de mesure relative à la protection de la réputation. Mais le projet de loi québécoise, si : il propose même deux changements significatifs à ce sujet.

Il établit qu'un mineur de moins de 14 ans ne peut pas consentir au traitement de ses renseignements personnels et qu'il revient au titulaire de l'autorité parentale de le faire pour lui[622]. Une exception est prévue lorsque le traitement est « manifestement au bénéfice » du mineur.

Et surtout, le projet de loi 64 de Québec met en place un droit à l'effacement et à la désindexation[623], inspiré de celui prévu au *RGPD* européen. Le droit à l'effacement, comme son nom l'indique, consiste en un droit à la suppression du contenu en ligne, alors que la désindexation n'affecte pas le contenu comme tel, mais le rend plus difficilement accessible en ne permettant pas d'y accéder au moyen d'un moteur de recherche (en utilisant le nom de la personne concernée, par exemple)[624].

Ces droits peuvent être invoqués lorsque la diffusion du renseignement personnel en question contrevient à la loi ou à une ordonnance judiciaire ou lorsqu'elle cause un préjudice grave au droit à la vie privée ou au respect de la réputation de la personne concernée. Le préjudice occasionné par la diffusion doit être manifestement supérieur à l'intérêt du public de connaitre ce renseignement ou à la liberté d'expression de la personne qui diffuse le renseignement. Et la mesure demandée (cessation de la diffusion, désindexation ou réindexation) ne doit pas excéder ce qui est requis pour éviter la perpétuation du préjudice. Le projet de loi prévoit une série d'éléments à prendre en

---

621 *A.B.* c *Bragg Communications Inc.*, 2012 CSC 46, para 17 ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Lignes directrices pour l'obtention d'un consentement valable », mai 2018, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/

622 QUÉBEC. Projet de loi n° 64, *supra* note 479, art 96 (qui ajoute l'art 4.1 à la *LPRPSP*).

623 *Ibid.*, art 113 (qui ajoute l'art 28.1 à la *LPRPSP*).

624 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Projet de position du Commissariat sur la réputation en ligne », 2018, en ligne : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/pos_or_201801/

compte dans le cadre de l'évaluation (personne mineure, personnalité publique, types et sensibilité des renseignements visés, etc.).

En procédant ainsi, Québec adopte une approche large, similaire à celle développée en Europe. Le « droit à l'oubli » tire son nom de la nécessité pour certains individus de voir les autres oublier certains comportements passés. Autant les progrès technologiques facilitent et favorisent la diffusion de l'information et l'accès à toutes ses manifestations, autant ils complexifient ce processus visant à « l'oubli », d'où l'intérêt de la mise en place d'un système d'effacement ou de désindexation[625]. L'approche a néanmoins été critiquée par certains en raison des atteintes potentielles à la liberté d'expression et la liberté de presse[626] et de la grande marge de manœuvre qui est laissée au moteur de recherche dans l'évaluation des demandes[627].

Tout en reconnaissant l'importance d'offrir des recours en cas d'atteinte à la réputation des individus en ligne, la Californie a adopté une approche différente du « droit à l'oubli ». Ainsi, le *California Consumer Privacy Act* ne prévoit pas la possibilité de faire désindexer les contenus ; il sera par contre possible de demander, sans avoir à fournir de justification, l'effacement de renseignements personnels collectés par les entreprises auprès de la personne concernée[628].

Similairement, une autre loi californienne, la *Online Eraser Law*, permet aux mineurs de demander l'effacement de tous renseignements personnels qu'ils ont eux-mêmes diffusés sur un site Web auprès duquel ils sont enregistrés (pensons notamment aux plateformes de médias sociaux)[629]. Encore une fois, la loi ne prévoit aucune condition particulière à remplir pour exercer ce droit (sinon la minorité au moment de la diffusion).

L'absence d'une exigence de justification et d'évaluation du bien-fondé de la demande garantit la rapidité du traitement et, vraisemblablement, la facilité et l'efficacité du processus, mais l'approche californienne risque toutefois de ne pas protéger pleinement la réputation des individus en ligne, notamment en raison de la facilité et de la rapidité avec laquelle les contenus disponibles sur les médias sociaux peuvent être copiés et rediffusés par autrui[630].

---

625 NEVILLE, A. « Is it a Human Right to be Forgotten? Conceptualizing the World View », Santa Clara Journal of International Law, vol. 15, no. 2, 2017, p.170.
626 Voir sur le sujet : LEE, E. « The Right to Be Forgotten v. Free Speech », I/S: A Journal Of Law And Policy, vol. 12, no. 1, 2015, en ligne : https://kb.osu.edu/bitstream/handle/1811/80043/ISJLP_V12N1_085.pdf
627 LIGUE DES DROITS. « Mémoire », *supra* note 591, pp.13-14.
628 ÉTAT DE LA CALIFORNIE. California Consumer Privacy Act, *supra* note 610, section 1798.105(a).
629 ÉTAT DE LA CALIFORNIE. Projet de la loi SB-568 Privacy: Internet: minors (2013-2014) (adopté en septembre 2013), section 22581(1), en ligne : https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568
630 DEHGHAN, S. « How does California's Erasure Law stack up against the EU's right to be forgotten », IAPP, 17 avril 2018, en ligne : https://iapp.org/news/a/how-does-californias-erasure-law-stack-up-against-the-eus-right-to-be-forgotten/

5.2.6 Préoccupations spécifiques relatives à la prise de décision automatisée à partir des renseignements personnels

La prise de décision automatisée à partir de renseignements personnels ne fait pas l'objet de dispositions particulières dans les lois canadiennes actuellement en vigueur[631]. Cette situation est donc régie par les règles générales concernant l'utilisation de renseignements personnels avec le consentement (éclairé et libre) de la personne visée et la transparence des entreprises relativement à leur pratique de traitement des renseignements personnels. Or, les systèmes d'intelligence artificielle qui permettent ce type de traitement des données représentent un défi pour l'application des lois[632], comme nous l'avons expliqué précédemment. Qui plus est, ce type de traitement des renseignements personnels introduit des risques additionnels pour les droits de la personne (dont le droit à la non-discrimination)[633].

À l'heure actuelle, un consommateur canadien ne peut refuser le traitement automatisé de ses renseignements personnels pour fin de prise de décision à son égard sans devoir également renoncer au bien ou service proposé par l'entreprise. Et il risque malheureusement d'y consentir sans réellement comprendre de quoi il en retourne, en raison de l'absence d'obligations de transparence spécifiques à ce type de traitement complexe des données.

5.2.6.1 Davantage de transparence proposée

Considérant le développement et le déploiement de ce type de traitement des renseignements personnels depuis l'adoption des quatre lois canadiennes en matière de protection des renseignements personnels dans le secteur privé au début des années 2000, il n'est guère surprenant de voir l'incorporation de modifications importantes à ce sujet dans les projets de loi 64 et C-11 déposés en 2020.

Notons que ni l'un ni l'autre des deux projets ne retient un élément central du *RGPD :* l'interdiction générale de prendre des décisions qui produisent des effets juridiques pour les personnes concernées sur la seule base du traitement automatisé de leurs renseignements personnels[634]. Cette interdiction fait l'objet de nombreuses exceptions, certes, mais demeure centrale à l'encadrement européen.

---

631 SOOKMAN, B. B., MORGAN, C. S. et GOLDENBERG, A. « Using privacy laws to regulate automated decision making », McCarthy Tétrault, 30 avril 2021, en ligne : https://www.mccarthy.ca/en/insights/blogs/techlex/using-privacy-laws-regulate-automated-decision-making

632 INNOVATION, SCIENCES ET DÉVELOPPEMENT ÉCONOMIQUE CANADA. « Renforcer la protection de la vie privée dans l'ère numérique. Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques », 2019, en ligne : https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00107.html

633 COFONE, I. « Propositions stratégiques aux fins de la réforme de la LPRPDE élaborées en réponse au rapport sur l'intelligence artificielle », Commissariat à la protection de la vie privée, novembre 2020, en ligne : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/pol-ai_202011/

634 RGPD, supra note 54, art 22(1) ; GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES. « Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 », 17/EN WP251rev.01, p.19 : « The term "right" in the provision does not mean that Article 22(1) applies only when

Les législateurs canadiens ont plutôt choisi de se concentrer sur la transparence des entreprises qui procèdent ainsi et, ultimement, sur la reconnaissance d'un droit à des explications pour les individus visés par les décisions. Un individu qui souhaiterait éviter une décision automatisée à son égard à partir de renseignements personnels déjà collectés devrait donc se tourner vers d'autres pistes de solution :

> Under the CPPA [*Consumer Privacy Protection Act* : nom abrégé d'une des lois inscrites au projet de loi C-11], any such right would need to be exercised through the right to withdraw consent or the right to be forgotten – which would be at best an indirect and more complicated avenue to achieve such this result[635].

Notons par ailleurs que les deux projets de loi prévoient une application plus large des règles que le *RGPD*. Les dispositions fédérales s'appliquent dès qu'une organisation a utilisé un traitement automatisé de données pour faire une prédiction, formuler une recommandation ou prendre une décision concernant un individu[636]. La disposition québécoise vise les décisions fondées exclusivement sur le traitement automatisé de renseignements personnels[637]. Mais, contrairement à l'encadrement européen, ni l'une ni l'autre ne requiert que ces décisions produisent des effets juridiques ou affectent de manière significative la personne concernée[638]. Et l'encadrement fédéral s'étend aux prédictions et recommandations basées sur le traitement automatisé des renseignements personnels, en plus des décisions.

Les deux projets de loi requièrent des entreprises qu'elles fournissent des explications aux individus concernés, sur demande, quant à la décision et aux renseignements personnels utilisés pour l'obtenir[639]. Le projet de loi québécois précise que ces explications doivent aussi inclure les principaux facteurs et paramètres ayant mené à la décision[640]. Le projet C-11 prévoit par ailleurs que des explications doivent aussi être fournies avant le traitement des renseignements personnels quant à l'usage que l'entreprise entend faire de systèmes décisionnels automatisés pour faire des prédictions, formuler des recommandations ou prendre des décisions à l'égard des individus[641]. Le législateur fédéral adopte ainsi une double approche en reconnaissant un droit individuel à des explications *ex ante* et *ex post*[642].

---

actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data."

635 YOUNG. « New federal privacy law », *supra* note 603.

636 CANADA. Projet de loi C-11, *supra* note 480, partie 1, arts 2 et 63(3).

637 QUÉBEC. Projet de loi n° 64, *supra* note 479, art 102 (qui ajoute l'art 12.1 à la *DPRPSP*).

638 RGPD, supra note 54, art 22(1).

639 CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 63(3) ; QUÉBEC. Projet de loi n° 64, *supra* note 479, art 102 (qui ajoute l'art 12.1(2)1°) et (2°) à la *LPRPSP*).

640 QUÉBEC. Projet de loi n° 64, *supra* note 479, art 102 (qui ajoute l'art 12.1(2)2°) à la *LPRPSP*).

641 CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 62(2)c).

642 L'auteur Gianclaudio Malgieri associe cette approche au concept de « legibility »: MALGIERI, G. « Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations », Computer Law & Security Review, vol. 35, no. 5, 2019, p.4, en ligne : https://www.researchgate.net/publication/334359463_Automated_decision-making_in_the_EU_Member_States_The_right_to_explanation_and_other_suitable_safeguards_in_the_national_legislations ; voir aussi : MALGIERI, G. et COMANDÉ, G. « Why a Right to Legibility of Automated Decision-Making

Les obligations de transparence et d'explication visent avant tout à développer une responsabilité algorithmique dans un contexte de développement rapide des systèmes d'intelligence artificielle[643]. Mais le *RGPD* va plus loin en permettant aux individus de faire des représentations à l'entreprise en regard d'une décision prise à leur sujet et d'obtenir une intervention humaine de la part du responsable du traitement des données[644]. Nous ne retrouvons pas d'équivalent dans les projets de loi 64 et C-11, malgré une recommandation en ce sens du Commissariat à la protection de la vie privée[645]. Cette dernière mesure est pourtant associée à la reconnaissance d'un autre droit essentiel à la dignité humaine : le droit de n'être sujet qu'à des inférences raisonnables[646].

L'explication d'une décision, comme le prévoient les projets, n'équivaut pas à la justification de ladite décision ou des inférences sur laquelle elle se base. La possibilité pour les individus de faire des représentations pour contester la validité d'une décision automatisée parait donc souhaitable. Des auteurs, comme Wachter et Mittelstadt, recommandent aussi l'ajout d'obligations additionnelles pour l'entreprise d'établir en quoi les données traitées constituent une base acceptable pour tirer des inférences (exactitude et fiabilité statistique des méthodes utilisées) et en quoi ces inférences sont pertinentes et acceptables pour les types de décisions automatisées visées[647]. Il ne semble pas que l'obligation d'explication générale de la décision et des renseignements utilisés, telle qu'écrite aux deux projets de loi, s'étende à ces informations spécifiques.

Qui plus est, le droit d'obtenir des explications sur le traitement automatisé et la décision rendue s'expliquent en partie par le droit corolaire de contester la décision, selon l'organe consultatif européen (groupe de travail « article 29 » sur la protection des données) :

> The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis[648]

En n'adoptant qu'un seul des deux volets pourtant complémentaires, les législateurs canadiens laissent les internautes canadiens vulnérables face au traitement automatisé de leurs renseignements personnels à des fins de prise de décision.

Exists in the General Data Protection Regulation », International Data Privacy Law, vol. 7, no. 3, novembre 2017, en ligne : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088976

643 WACHTER, S. et MITTELSTADT, M. «A right to reasonable inferences: re-thinking data protection law in the age of Big data and AI », Columbia Business Law Review, 2019, en ligne: https://www.researchgate.net/publication/327872087_A_RIGHT_TO_REASONABLE_INFERENCES_RE-THINKING_DATA_PROTECTION_LAW_IN_THE_AGE_OF_BIG_DATA_AND_AI

644 RGPD, supra note 54, art 22(3).

645 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. « Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE », novembre 2020, en ligne : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011/

646 WACHTER. « A right to reasonable inferences », *supra* note 643.

647 *Ibid.*

648 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES. « Guidelines on Automated individual decision-making », *supra* note 648, p.16.

5.3 Les lois sont-elles compatibles avec les comportements des consommateurs ?

5.3.1 La responsabilité des consommateurs

De par leur désir de ne pas entraver l'innovation et de satisfaire les besoins des entreprises en matière de traitement des renseignements personnels, les législateurs canadiens se trouvent à faire reposer une grande part de la responsabilité de la protection de leur vie privée sur les épaules des consommateurs eux-mêmes. La loi impose aux entreprises certaines obligations dans le cadre du traitement des renseignements personnels, certes, mais il revient bien souvent en définitive aux consommateurs de déterminer s'ils consentent ou non à la collecte ou autre traitement de ces données. Et pour ce faire, il lui revient de prendre connaissance, de comprendre et d'analyser les pratiques des entreprises et les risques qu'elles représentent et d'évaluer le prix de son consentement et la valeur respective des avantages qu'il lui procure. Si plusieurs répondants canadiens au sondage se montraient conscients de l'importante responsabilité qui leur incombe actuellement, il est moins évident qu'ils l'exerçaient avec le discernement requis ; beaucoup se disaient d'avis qu'il leur faudrait « en faire plus ». Mais cette charge que leur imposent les entreprises – avec l'aval des législateurs - devrait-elle leur revenir ? Les avis des participants à nos entrevues et des auteurs semblent assez partagés.

L'approche actuelle des législateurs canadiens s'inscrit davantage dans une perspective du droit à la protection de la vie privée à titre de droit individuel que chacun exerce comme il le désire (pour autant qu'il puisse réellement l'exercer librement). De plus en plus de voix s'élèvent pour défendre une perspective plus collective de ce droit, qui aurait pour effet potentiel de transférer une plus grande partie de la responsabilité à l'État dans son contrôle des pratiques des entreprises (par la loi elle-même ou par les autorités de surveillance et d'application de la loi).

Les projets de loi C-11 et 64 apportent certains ajouts qui ont pour effet de faire reposer davantage de responsabilités sur les épaules des entreprises, notamment par l'implantation de mesures de sécurité et d'évaluation plus sévères[649], mais le consentement du consommateur demeure central. Ce faisant, le partage de la responsabilité entre les intervenants dans les lois fédérale et québécoise s'en trouve relativement peu changé.

Différentes options s'offriraient à l'État afin de réduire la charge qui incombe aux consommateurs dans la protection de leur vie privée en ligne, que ce soit en la transférant à l'État ou aux entreprises. Voici quelques exemples des approches possibles.

[649] Pensons par exemple à l'évaluation des facteurs de risques à laquelle devrait dorénavant se prêter une entreprise avant la mise en place de tout système d'information ou de prestation électronique de service qui impliquerait le traitement de renseignements personnels : QUÉBEC. Projet de loi n° 64, *supra* note 479, art 95 (qui ajoute l'art 3.3 à la *LPRPSP*).

5.3.1.1 Un rôle accru pour le secteur privé (et l'État) : Les programmes de certifications

Faire porter la presque totalité de la responsabilité de la protection de la vie privée en ligne aux consommateurs par l'exercice de son droit au consentement est difficilement justifié, vu la manière dont ce droit s'exerce malheureusement en pratique. S'en remettre entièrement aux entreprises, dont la connaissance et compréhension de l'encadrement en vigueur tend à être faible[650], ne serait guère plus sage. Reste donc l'État, dont le rôle doit atteindre le point d'équilibre entre ingérence et passivité face aux pratiques des entreprises.

> A variety of problems plague the exercise of decision-making competence in the data protection field regardless of where that competence is placed. It would seem that the solution to these problems cannot lie in providing either data subjects or data controllers with even more decisional power. At the same time, reverting to a comprehensive licensing scheme administered by DPAs [Data Protection Autorities] seems unrealistic. An important question then is whether decision-making competence can be reorganized in another way that mitigates these problems[651].

Les programmes de certification qui « pré-approuvent » les politiques et les pratiques de traitement des renseignements personnels des entreprises participantes représentent potentiellement une solution intermédiaire. Ils réduisent les risques auxquels sera exposé un consommateur qui n'aurait pas fait (ou été en mesure de faire) un choix réfléchi quant au traitement de ses renseignements personnels par une entreprise. Ils réduisent la complexité de l'analyse requise par le consommateur, étant donné que ces programmes tendent à entraîner une uniformisation des pratiques au sein de certains secteurs. Ils contribuent de plus à éduquer les entreprises quant à la légalité et la légitimité de leurs pratiques. Et ils font l'objet d'une surveillance et d'une approbation par les autorités, ce qui leur accorde ainsi un sérieux et une crédibilité additionnels.

Certains États européens, comme la Norvège, la Suède et la France, ont par le passé instauré des régimes de licences dont les entreprises devaient se prémunir pour procéder à certains types de traitements de renseignements personnels. La disparition de ces programmes s'explique surtout par les ressources considérables qui étaient requises des autorités pour soutenir le fonctionnement d'un tel modèle[652]. Les programmes de certification dont le secteur privé est responsable, mais qui font l'objet d'un encadrement législatif règlent également ce problème (bien que le sous-financement des autorités de protection demeure un problème qui dépasse largement ce seul enjeu). Ils redonnent également le dernier mot aux consommateurs (qui doit encore fournir son consentement), ce qui n'était pas le cas à l'ère des licences[653].

C'est justement ce que propose le projet de loi C-11 par l'octroi au Commissariat d'un pouvoir d'approbation d'éventuels programmes de certification développés par des entités

---

[650] BYGRAVE. « Consent », *supra* note 497, p.4.
[651] *Ibid.*, p.5.
[652] *Ibid.*, p.3.
[653] *Ibid.*, p.3.

privées[654]. Soulignons que cette nouvelle règle s'inscrit encore une fois parfaitement dans la volonté du législateur fédéral canadien d'accompagner les entreprises dans le respect de la loi plutôt que de les punir ou encore les dissuader.

5.3.1.2 Un rôle accru pour l'État : L'interdiction en amont de certains traitements dangereux des renseignements personnels

Il existe une manière plus drastique de réduire la pression exercée sur les consommateurs par le consentement, soit en interdisant directement aux entreprises d'adopter certaines pratiques de traitement des renseignements personnels qui seraient jugées inacceptables par la société (et conséquemment par les législateurs) et qu'un consentement du consommateur pourrait légitimer à tort. Certains auteurs font une analogie avec la ceinture de sécurité en voiture :

> Policy intervention is motivated to the extent that people are poor navigators. Much as seat belts in cars are justified by the fact that people's natural driving habits (as well as those of other drivers) create an unacceptable level of risk, privacy interventions can be justified by similar limitations of individuals' abilities to manage privacy-related risks[655].

Cette approche n'a pas été retenue jusqu'ici par les législateurs canadiens qui s'en remettent plutôt à la capacité de choisir des consommateurs, faisant fi des risques auxquels ils les exposent malheureusement. D'autres législateurs ont fait des choix différents. L'Union européenne a par exemple choisi d'interdire le traitement automatisé des renseignements personnels afin de prendre une décision significative au sujet de la personne concernée[656] (notons que l'interdiction fait tout de même l'objet de multiples exceptions)[657]. Selon les lignes directrices relatives au *RGPD*, cette interdiction s'explique par les risques pour les droits et libertés des individus potentiellement visés par cette pratique[658]. L'Union européenne envisage également d'interdire le traitement des renseignements personnels au moyen de l'intelligence artificielle afin d'établir une cote de crédit social (*social credit score*)[659] en raison des risques d'exclusion et de discrimination qu'il présente[660].

Une autre pratique est régulièrement pointée du doigt par les défenseurs des droits de la personne et des droits des internautes comme étant socialement répréhensible : le

---

654 CANADA. Projet de loi C-11, *supra* note 480, partie 1, arts 76-81.
655 BRANDIMARTE, L., ACQUISTI, A. et LOEWENSTEIN, G. « Misplaced Confidences: Privacy and the Control Paradox », Social Psychological and Personality Science, vol. 4, no. 3, 2012, en ligne : https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf
656 RGPD, supra note 54, art 22(1) ; GROUPE DE TRAVAIL « ARTICLE 29 ». « Guidelines on Automated individual decision-making », supra note 643, p.19.
657 RGPD, supra note 54, art 22(2).
658 GROUPE DE TRAVAIL « ARTICLE 29 ». « Guidelines on Automated individual decision-making », *supra* note 648, p.9.
659 PARLEMENT EUROPÉEN. Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, 21 avril 2021, COM/2021/206, Title II, art 5(1)c).
660 *Ibid.,* préambule, para 17.

traitement des renseignements personnels à des fins de publicité ciblée[661]. En février 2021, le Contrôleur européen de la protection des données, Wojciech Wiewiórowski, a publiquement encouragé les législateurs européens à bannir la publicité ciblée basée sur des données obtenues au moyen de suivi invasif en ligne[662]. Une coalition américaine qui comprend une quarantaine de groupes d'influence comme l'American Economic Liberties Project, le Center for Digital Democracy, le Center for Humane Technology et Public Citizen fait aussi des pressions en ce sens auprès du Congrès américain[663].

5.3.2 L'inertie des consommateurs

Les études et sondages, incluant le nôtre, tendent à démontrer une certaine inertie chez les internautes d'ici et d'ailleurs en ce qui concerne la protection de leurs renseignements personnels. Ils se sentent impuissants face au traitement actuel de leurs renseignements personnels et n'ont généralement pas l'intention, l'envie ou les capacités (perçues ou réelles) d'améliorer les choses.

Comment les législateurs canadiens peuvent-ils tenir compte de cette réalité dans l'élaboration des réformes et qu'ont-ils retenu dans l'élaboration des projets de loi C-11 et 64 ?

5.3.2.1 La protection de la vie privée par défaut et les « coups de pouce »

Les législateurs peuvent mettre en place des « coups de pouce » en matière de protection de la vie privée (*privacy nudges*) destinés aux consommateurs, qui ont pour conséquence de réduire les effets négatifs de la passivité de ces derniers sur la protection de leur vie privée en ligne. Soh propose la définition suivante du concept :

> "Privacy nudges" stem from the use of soft paternalism to nudge users towards improved decision-making in the context of privacy, that is, to make them more "privacy sensitive" or in a manner that reduces users' regret[664].

Cette manière de faire n'est pas à l'abri de critiques, notamment en raison de la manipulation qu'elle sous-entend (elle encourage activement à faire certains choix)[665],

---

[661] Voir par exemple : MAHDAWI, A. « Targeted ads are one of the world's most destructive trends. Here's why », The Guardian, 5 novembre 2019, en ligne : https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/ ; https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy

[662] WOOLLACOTT, E. « European Regulator Calls For Ad Targeting Ban », Forbes, 21 février 2021, en ligne: https://www.forbes.com/sites/emmawoollacott/2021/02/11/european-regulator-calls-for-ad-targeting-ban/?sh=6b0a4ec82523

[663] Campagne "Ban Surveillance Advertising", en ligne: https://www.bansurveillanceadvertising.com/ (consulté le 10 septembre 2021) ; LOMAS, N. « US privacy, consumer, competition and civil rights groups urge ban on 'surveillance advertising' », TechCrunch, 22 mars 2021, en ligne : https://techcrunch.com/2021/03/22/us-privacy-consumer-competition-and-civil-rights-groups-urge-ban-on-surveillance-advertising/

[664] SOH, S. Y. « Privacy nudges », *supra* note 496, pp.67-68.

[665] *Ibid.,* p.73.

mais elle a tout de même l'avantage de préserver un certain degré d'autonomie pour le consommateur[666].

Un exemple de coup de pouce est la mise en place de paramètres par défaut favorables aux consommateurs. Libre au consommateur de consentir à un degré moindre de confidentialité, mais, en cas d'inaction de sa part, c'est le niveau de confidentialité le plus élevé offert par l'entreprise devra être appliqué. On trouve une disposition de ce type dans le projet de loi 64 du législateur québécois[667]. Ce type de coup de pouce s'explique facilement : des études démontrent que l'option par défaut sera généralement celle qui sera maintenue, par choix ou par inertie. Willis identifie quelques raisons qui font des paramètres par défaut le choix le plus populaire, dont :

- Le temps requis pour modifier les paramètres[668] (*transaction barrier*)
- La confusion provoquée par les paramètres sélectionnés par défaut (ce qu'ils représentent et la marge de manœuvre qui est offerte aux consommateurs)[669] ;
- La tendance à se sentir moins responsable des conséquences en cas d'inaction qu'à la suite d'une action posée[670] (*omission biais*)
- La tendance à préférer éviter de prendre des décisions[671] (*decision avoidance*)
- La perception du paramètre par défaut comme une recommandation implicite d'une partie mieux informée[672].

En adoptant un modèle de confidentialité par défaut, le législateur québécois est conscient de ce biais des consommateurs et semble reconnaitre du même coup (et pour une fois) que le droit à la protection de ses renseignements personnels devrait primer sur les considérations économiques des entreprises (pour qui une protection maximale par défaut n'est pas à l'avantage). Mais comme pour le reste du cadre législatif en place, les besoins des entreprises ne sont pas entièrement ignorés. Et le législateur québécois leur fait une faveur dans son projet de loi 64 en n'incluant pas l'exigence connexe, mais plus sévère de la confidentialité dès la conception, tel qu'elle figure, par exemple, au *RGPD*[673]. On ne retrouve pas non plus ce principe (pas plus que celui de la confidentialité par défaut, d'ailleurs) au projet de loi fédéral C-11.

Similairement, l'adoption d'un modèle d'*opt-in* (option d'adhésion, dont nous avons parlé précédemment) en ce qui concerne le consentement requis des consommateurs dont une entreprise entend collecter et traiter les renseignements personnels pourrait adéquatement répondre à l'inertie des consommateurs en matière de protection de la vie

---

666 SOLOVE, D. J. Privacy Self-Management, *supra* note 507.
667 QUÉBEC. Projet de loi n° 64, *supra* note 479, art 100 (qui ajoute l'art 9.1 à la *LPRPSP*).
668 WILLIS, L. E. « Why Not Privacy By Default? », Berkeley Technology Law Journal, vol. 29, no. 1, 2014, p8, en ligne : http://nrs.harvard.edu/urn-3:HUL.InstRepos:11266829
669 *Ibid.*, p.9.
670 *Ibid.*, pp.11-12.
671 *Ibid.*, pp.12-13.
672 *Ibid.*, p.16.
673 RGPD, supra note 54, art 25(1) ; pour en savoir plus sur le principe de la confidentialité dès la conception : KREBS, D. « "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law? », Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 4, no. 1, 2013, en ligne : https://www.jipitec.eu/issues/jipitec-4-1-2013/jipitec4krebs/jipitec-4-1-2013-2-krebs.pdf

privée en ligne. Ces derniers ne seraient dès lors plus pénalisés lors du maintien du statu quo. Malheureusement, les deux projets de loi de 2020 ne tendent pas vers ce modèle.

5.3.2.2 Le consentement obtenu par subterfuge

Soulignons tout de même l'interdiction prévue au projet de loi C-11 d'employer un subterfuge (avoir recours à une pratique trompeuse ou mensongère ou fournir une information fausse ou trompeuse) afin d'obtenir le consentement d'un consommateur[674]. Nous ne retrouvons pas une interdiction équivalente dans les lois albertaine, britanno-colombienne et québécoise (ou dans le projet de loi québécois), bien qu'il y est prévu que le consentement fourni doit être libre et éclairé, ce qui devrait naturellement restreindre la manière dont les entreprises procèdent en vue de l'obtenir.

Par l'ajout d'une telle disposition à son projet de loi, le législateur fédéral agit sur deux fronts. Il tente de rendre plus effectif l'encadrement en place en réduisant les risques que se produise en sol canadien ce qui s'est passé en Europe, soit les tentatives répétées de l'industrie de contourner l'encadrement prévu au *RGPD* depuis son entrée en vigueur[675]. Et il répond au comportement observable des consommateurs en ligne (souvent apathique et plus facilement influençable).

Forbrukerrådet, le Conseil norvégien des consommateurs, a produit en 2018 une étude détaillée sur l'emploi de ces *dark patterns* par des entreprises en Europe. Il identifie entre autres les pratiques populaires de rendre certaines options de consentement peu visibles (en jouant sur la couleur ou l'emplacement), de décrire de manière péjorative ou culpabilisante les options de confidentialité les plus sévères (cette pratique est parfois qualifiée de *confirmshaming*) et d'imposer des étapes supplémentaires aux consommateurs qui souhaitent refuser la collecte de renseignements personnels, par exemple, comparativement à ceux qui l'acceptent[676]. Il est vraisemblable que la disposition prévue au projet de loi C-11 ne couvre malheureusement pas toutes ces pratiques.

---

[674] CANADA. Projet de loi C-11, *supra* note 480, partie 1, art 16.
[675] Voir par exemple : NOUWENS, M. *et al*. « Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence », 8 janvier 2020, CHI '20 CHI Conference on Human Factors in Computing Systems, 2020, en ligne : https://arxiv.org/abs/2001.02479
[676] FORBRUKERRÅDET. « Deceived by design », 27 juin 2018, p.12 et ss, en ligne : https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

LA PAROLE AUX EXPERTS

Au courant de l'été 2021, nous nous sommes entretenus avec deux professeurs d'universités canadiennes spécialisés en matière de protection des renseignements personnels en ligne afin d'obtenir leur point de vue sur certains enjeux soulevés dans le présent rapport[677].

Les opinions rapportées dans le présent chapitre, recueillies dans le cadre d'entrevues par téléphone ou par vidéoconférence[678], sont celles de :

- Mme Céline Castets-Renard[679], professeure titulaire à la Faculté de droit de l'Université d'Ottawa (section du droit civil) et titulaire de la Chaire de recherche de l'Université d'Ottawa sur l'intelligence artificielle responsable à l'échelle mondiale et de la Chaire Law, Accountability, and Social Trust in AI (rattachée à l'Université fédérale Toulouse Midi-Pyrénées). Elle a enseigné plusieurs cours sur la protection des données personnelles, notamment dans une perspective de droit comparé.
- M. Ignacio Cofone[680], professeur adjoint à la faculté de droit de l'Université McGill, où il enseigne des cours sur l'encadrement de l'intelligence artificielle et le traitement des renseignements personnels. Il a publié plusieurs articles sur la protection de la vie privée en ligne et travaille actuellement sur la conceptualisation et l'évaluation des atteintes à la vie privée par les tribunaux[681].

6.1 Quelle approche générale devraient adopter les législateurs canadiens ?

D'emblée, les deux chercheurs appuient la position du Commissariat à la protection de la vie privée du Canada qui prône une approche centrée davantage sur le respect des droits humains dans le cadre des lois canadiennes de protection des renseignements personnels dans le secteur privé.

Pour Mme Castets-Renard, l'ajout d'une disposition qui reconnaitrait explicitement le droit à la protection des renseignements personnels aurait l'effet d'un levier pour les tribunaux, qui leur permettrait de sanctionner plus facilement les abus. Invoquant l'image d'un

[677] Nous avons contacté plusieurs chercheurs canadiens. Deux ont ultimement accepté nos demandes d'entrevue. Nous avons aussi invité, en vain, les *offices de protection de la vie privée*. Un sommaire des faits saillants de notre recherche a été expédié aux répondants préalablement aux entrevues.
[678] En plus d'avoir discuté avec nous par téléphone, M. Cofone nous a fourni des réponses additionnelles par écrit et nous a référés à certains de ses articles et recherches pour des éléments de contexte complémentaires.
[679] UNIVERSITÉ D'OTTAWA. Biographie de Céline Castets-Renard, en ligne : https://droitcivil.uottawa.ca/en/people/castets-renard-celine
[680] COFONE, I. Site Web personnel, en ligne : http://www.ignaciocofone.com/
[681] COFONE, I. « Privacy Standing », University of Illinois Law Review, 2022, en ligne : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782887

parapluie, elle souhaite que les juges (et les consommateurs) puissent s'appuyer sur une disposition plus générale de la loi pour conclure à une violation du droit à la protection de la vie privée, lorsque les règles plus spécifiques laissent échapper une situation (notamment dans le contexte des avancées technologiques et de l'intelligence artificielle). Elle soutient d'ailleurs que l'absence d'une telle reconnaissance dans la *LPRPDE* nuit présentement aux consommateurs canadiens, surtout que l'interprétation de la loi est complexe, vu la variété d'objectifs poursuivis (dont plusieurs d'ordre économique).

Les deux chercheurs citent en exemple l'approche du *RGPD* fondée sur les droits, mais rappellent du même coup la nécessité de l'adapter au contexte juridique canadien, notamment parce que le droit européen reconnait aux consommateurs deux droits fondamentaux distincts, la protection de sa vie privée et celle de ses renseignements personnels, contrairement au droit canadien qui distingue plus difficilement les deux.

6.2 Quelle responsabilité pour chaque partie ?

S'il faut axer davantage la loi sur le respect des droits fondamentaux, il faut également repenser la responsabilité de chaque partie dans la protection des renseignements personnels en ligne, selon les experts consultés.

Celle que doivent assumer les consommateurs canadiens, par exemple, leur apparait démesurée. L'analyse et les choix attendus de ces derniers ne sont guère réalistes et rendent ultimement la mise en œuvre des droits spécifiques prévus à la loi quelque peu utopique. Pour illustrer son propos, M. Cofone réfère aux difficultés exprimées par des juges dans l'évaluation des dommages à la suite d'une atteinte à la vie privée dans le cadre de recours collectifs (des difficultés importantes au point de mener au rejet de certains dossiers). Comment alors peut-on demander au consommateur moyen, qui n'a aucune connaissance particulière dans les domaines juridique et technologique, de faire cette même évaluation, et ce, alors que l'atteinte peut être encore incertaine à ce moment-là ?

L'allègement de la responsabilité qui est laissée aux consommateurs doit passer, entre autres, par l'augmentation de celle des entreprises. Selon M. Cofone, la rédaction de la loi fédérale sous forme de principes plutôt que d'obligations claires exacerbe actuellement le manque d'obligations redditionnelles (*accountability*) des entreprises au pays en ce qui a trait au traitement qu'elles font des renseignements personnels des consommateurs. Il est d'avis qu'il faut s'inspirer du *RGPD* et imposer aux organisations la responsabilité de démontrer la conformité de leurs pratiques. Cette obligation serait bénéfique sur plusieurs fronts : elle renforcerait la conformité des pratiques des entreprises, faciliterait le travail des autorités de surveillance et opérerait un changement de culture qui aurait ultimement pour effet de renforcer la confiance du public. Le professeur réfère plus spécifiquement à la notion de traçabilité des données, soit la consignation et la documentation par les entreprises de la collecte et du traitement de renseignements personnels auxquelles elles se livrent, afin d'en faire rapport aux autorités, lorsque requis. Mme Castets-Renard met quant à elle l'accent sur la responsabilité continue des entreprises à l'égard des sous-traitants qui entrent en contact avec les renseignements personnels collectés (le choix des

contractants, la sécurité des renseignements et le respect de l'encadrement par ces derniers, etc.). Comme M. Cofone, elle pointe les avancées européennes à ce sujet.

Enfin, la responsabilité de l'État est également soulevée dans les discussions. Pour Mme Castets-Renard, le traitement de certains types de renseignements personnels (comme les renseignements sensibles) nécessite un régime beaucoup plus strict, parce qu'il présente des risques accrus pour les droits humains. L'élaboration et la mise en œuvre de cet encadrement additionnel sont la responsabilité de l'État, qui se doit d'être davantage proactif.

6.3 Dans quelle mesure faut-il s'inspirer des réformes étrangères ?

Sans surprise, les deux chercheurs sont d'avis que les législateurs canadiens doivent fortement s'inspirer des cadres réglementaires européens. Parce qu'ils sont intéressants et utiles, mais aussi à cause de ce que Mme Castets-Renard qualifie de « colonialisme juridique ». En raison du poids économique et politique de l'Europe, les principes du *RGPD* ont été repris par plusieurs autres pays. Ils sont devenus depuis des standards mondiaux que le Canada doit atteindre, notamment pour assurer la pérennité de ses échanges commerciaux avec le vieux continent.

Comment donc s'inspirer du *RGPD* ? Les deux chercheurs sont d'avis qu'on ne peut pas simplement reprendre le texte du règlement européen. Certains fondements des lois canadiennes diffèrent, notamment en ce qu'elles n'adoptent pas une approche axée sur les droits fondamentaux et ne conçoivent pas le droit à la protection de la vie privée exactement de la même manière. Qui plus est, le *RGPD* date de 2016 et, bien qu'il constitue indéniablement une réforme réussie, certaines faiblesses et difficultés d'application ont été observées depuis. Pour M. Cofone, le projet de loi 64 est une excellente adaptation du *RGPD* qui tient compte de ces faiblesses, notamment celles relatives au traitement automatisé des renseignements personnels afin de prendre des décisions au sujet des personnes concernées.

Mme Castets-Renard souligne par ailleurs l'importance de ne pas oublier les dispositions européennes qui accordent d'importants pouvoirs aux autorités nationales de contrôle de l'application du *RGPD* et des lois nationales connexes. À défaut d'une autorité forte, la transposition des principes (droits et obligations) européens en sol canadien risque de n'être malheureusement que théorique.

Les deux chercheurs ne voient pas d'un très bon œil la possibilité que les législateurs canadiens s'inspirent de l'encadrement américain en matière de protection des renseignements personnels. Le caractère davantage sectoriel et régional de l'encadrement américain doit être évité à tout prix au Canada, selon eux. Il faut plutôt privilégier l'uniformisation des règles sur l'ensemble du territoire, afin de favoriser une meilleure compréhension des règles par les consommateurs et les entreprises. Mme Castets-Renard est d'ailleurs d'avis que les écarts régionaux révélés dans notre sondage en ce qui a trait

aux niveaux de préoccupation des internautes canadiens pour la protection de leur vie privée en ligne ne justifient pas de différencier l'encadrement selon les provinces. Tous sont confrontés aux mêmes problèmes et aux mêmes risques. Il importe plutôt que les consommateurs de tous horizons en soient conscients, ce qui peut être atteint par des démarches d'information du public.

6.4 Comment tenir compte des avancées technologiques ?

Puisque la loi ne peut être continuellement modifiée pour l'adapter aux développements technologiques rapides, on propose plutôt de mettre en place ou de renforcer des principes directeurs (neutres technologiquement) comme les principes de nécessité, de finalité et de minimisation de la collecte et de l'utilisation des renseignements personnels. Selon Mme Castets-Renard, leur présence dans les lois canadiennes devrait être renforcée. Ces principes qui doivent guider l'entreprise dans toutes les étapes d'interprétation et d'application de la loi ont l'avantage de simplifier la reconnaissance et l'identification d'une violation aux droits des individus.

Les deux professeurs insistent également sur l'importance des études d'impact des risques pour la vie privée (EVFP au Canada ou AIPD en Europe) dans le contexte du déploiement de l'intelligence artificielle, tout en reconnaissant que celles-ci ne doivent pas représenter un fardeau excessif pour les entreprises, notamment les PME. M. Cofone fait par ailleurs valoir que ces obligations ne représentent pas une fin en soi, mais une manière d'aider les entreprises à mettre en œuvre leur responsabilité plus générale en matière de protection des renseignements personnels.

Enfin, les chercheurs sont d'avis que certains enjeux connexes à la protection des renseignements personnels en ligne, tels que l'utilisation de l'intelligence artificielle ou le recours aux témoins de navigation en ligne, devraient être traités dans le cadre de lois ou règlements distincts. Pour Mme Castets-Renard, la *LPRPDE* et ses équivalents provinciaux sont insuffisants pour répondre aux différents problèmes auxquels font face les internautes d'aujourd'hui. Et ultimement, le Canada fait piètre figure, si l'on considère l'ampleur de l'encadrement développé en Europe en matière de droit numérique.

6.5 Que faire du consentement ?

Les deux professeurs se montrent critiques de la place donnée au consentement dans les lois canadiennes. Il ne leur parait pas réaliste ou raisonnable de s'attendre à ce que les consommateurs fassent des choix éclairés dans le contexte actuel. L'asymétrie de pouvoir et de savoir entre les parties est trop importante et il est quasi impossible pour le consommateur d'évaluer les avantages et les risques du traitement de leurs

renseignements personnels, notamment en raison du caractère imprévisible des traitements au moyen de l'intelligence artificielle[682].

Pour M. Cofone, l'obligation actuelle d'obtenir un consentement préalablement au traitement de renseignements personnels crée un faux sentiment de contrôle chez les consommateurs. Cocher par automatisme sur la case « Oui. J'accepte » au bas d'une page Web n'est pas indicatif d'un quelconque pouvoir réel, martèle-t-il ! Mme Castets-Renard partage son point de vue et souligne en outre le caractère déresponsabilisant pour les entreprises de cette approche basée sur le consentement. Le renforcement des obligations de transparence des entreprises n'est pas du tout perçu comme une solution à ces problèmes.

Tous deux réfèrent au cadre réglementaire européen, dans lequel le consentement n'est qu'une base juridique du traitement des données personnelles parmi d'autres (et ne représente pas la base utilisée dans la majorité des cas). Devrait-on opter pour un modèle similaire au Canada ? Mme Castets-Renard est en faveur de l'abandon du caractère exclusif du consentement, dont l'application au Canada lui semble hypocrite, considérant toutes les exceptions en place (en plus de celles proposées dans les projets de loi). M. Cofone, croit lui aussi qu'il faut diminuer l'importance du consentement dans le cadre juridique canadien, et ce, afin de réduire la pression irréaliste qui pèse sur les consommateurs et de responsabiliser davantage les entreprises dans leurs pratiques de traitement des renseignements personnels. Mais les deux chercheurs soulignent l'importance d'établir en parallèle un cadre d'utilisation (au moyen de principes directeurs par exemple) et des garanties et mesures de précaution pour les traitements réalisés sans le consentement des personnes concernées.

6.6 Quel avenir pour les projets de loi de 2020 ?

Les deux professeurs ne s'entendent pas pleinement sur les prochaines étapes de la modernisation des lois canadiennes de protection des renseignements personnels dans le secteur privé.

Tous deux sont satisfaits du projet de loi québécois 64, un projet qu'ils considèrent plus proche du *RGPD* et plus à l'avantage des consommateurs que le projet du fédéral. Au moment des entrevues (à l'été 2021), ils espéraient son adoption rapide et soulignaient l'intérêt que représente l'adoption de la réforme québécoise à titre de première en son genre au pays, susceptible de presser et d'orienter la modernisation subséquente des autres lois canadiennes, puisqu'une certaine uniformisation de l'encadrement à l'échelle canadienne est indispensable. Rappelons que le projet québécois a depuis été adopté.

Mais leurs opinions divergent en ce qui concerne le projet de loi fédéral C-11. Étant donné la tenue d'élections en septembre 2021 avant son adoption, il est mort au feuilleton. Le gouvernement fédéral devrait-il le déposer de nouveau ?

---

[682] COFONE, I. « Propositions stratégiques aux fins de la réforme de la LPRPDE », *supra* note 633.

D'un côté, Mme Castets-Renard croit qu'il vaut mieux poursuivre les travaux sur la base du texte du projet C-11, et donc, de le redéposer en vue d'une adoption rapide. Elle se dit déçue du projet et serait en faveur d'une réécriture complète, dans un monde idéal, mais croit que la réalité politique milite plutôt vers l'adoption rapide et assurée d'une réforme modeste et quelque peu insatisfaisante, plutôt que l'adoption incertaine et éloignée d'une meilleure réforme de la loi fédérale. Elle craint que, si le projet de réforme est revu en profondeur, plusieurs années s'écoulent avant le dépôt et l'adoption d'un nouveau projet de loi, aggravant le retard du cadre législatif canadien par rapport à l'encadrement réglementaire européen. Mieux vaut de petits changements qu'aucun changement à court terme, bref !

M. Cofone, lui, croit plutôt qu'il vaut mieux bien faire les choses, quitte à ce que la réforme prenne encore un peu de temps à se concrétiser. Il signale que si le texte de C-11 est adopté, la prochaine réforme de cette nouvelle loi n'aura vraisemblablement lieu que dans de nombreuses années. Comme il n'est pas à l'aise avec l'idée que cette nouvelle loi pourrait s'appliquer jusqu'en 2040, voire plus tard encore, il favorise une réécriture complète du projet.

Au final, les deux chercheurs ont donc les mêmes inquiétudes : le manque de volonté prévisible du législateur fédéral de retravailler à court terme sur ces enjeux et la lenteur probable de ses démarches de réforme ou de mise à jour de la *LPRPDE*. Ils proposent toutefois une réponse bien différente.

CONCLUSION

> Les citoyens numériques vivent dans un monde qu'ils ne voient pas, qu'ils ne comprennent pas et qu'ils ne contrôlent pas. À la lumière de son expérience, le citoyen numérique sait que le contrôle et le consentement associé à ses renseignements personnels sont une fiction.
>
> Jonathan A Obar[683] [traduction libre]

Que signifie protéger sa vie privée en 2021 ? Pour certains, cela veut dire se mettre à l'abri des regards. Pour d'autres, ça signifie plutôt avoir le choix et avoir le dernier mot sur qui les regarde, qui a accès à leurs renseignements personnels et à quels renseignements spécifiquement, et sur ce qu'ils peuvent en faire. Pour d'autres encore, c'est le fait de maintenir leur capacité à prendre des décisions importantes sur leur existence, sans interférence des autres, qui est déterminant. Toutes ces conceptions sont valables ; il n'existe aucune définition universelle de ce qu'est la vie privée et chacun adopte donc sa propre définition. La protection de la vie privée est dès lors un exercice hautement subjectif.

La conception de la protection de la vie privée des individus doit également se faire en tenant compte de l'environnement dans lequel les individus qui la réclament évoluent. En 2021, la prise en compte d'Internet est essentielle à toute réflexion sur le sujet. Il simplifie la collecte, l'accès et le partage de renseignements personnels par les entreprises et les particuliers, au moyen des médias sociaux et des témoins de navigation, par exemple. Les nouvelles technologies, dont celles qui font appel à l'intelligence artificielle, permettent ensuite une variété de traitements des renseignements qui étaient encore inimaginables il y a quelques années à peine, et ce, à partir d'une quantité colossale de données. L'avènement et la démocratisation de l'utilisation d'Internet sont ainsi à l'origine d'un changement d'échelle stupéfiant. Alors qu'il était naguère coûteux et relativement peu utile pour les entreprises de collecter et de conserver les renseignements personnels de leurs clients, l'inverse est maintenant vrai. On assiste à l'apparition d'une économie axée sur l'exploitation de ce type de renseignements.

Dans ce contexte, il n'est guère surprenant que les résultats de sondages réalisés auprès de consommateurs d'ici et d'ailleurs fassent état d'un niveau de préoccupation toujours en hausse pour la protection de leur vie privée en ligne. Beaucoup se disent fortement préoccupés, mais se sentent impuissants, convaincus qu'ils ne peuvent réellement changer les choses, que leurs renseignements personnels sont destinés à se retrouver à la merci des entreprises, des États et des pirates informatiques, peu importe ce que tentera l'internaute pour l'éviter. Les résultats du sondage pancanadien et des entrevues réalisés

---

[683] « Digital citizens live in a world which they cannot see, do not understand and are unable to direct. In the cold light of experience the digital citizen knows that data privacy self-management is a fiction » : OBAR, J. A. « Big Data and The Phantom Public: Walter Lippmann and the fallacy of data privacy self-management », Big Data & Society, vol. 2, no. 2, octobre 2015, p.1, en ligne : https://www.researchgate.net/publication/283438170_Big_Data_and_The_Phantom_Public_Walter_Lippmann_and_the_fallacy_of_data_privacy_self-management

en 2020 soulèvent d'ailleurs des inquiétudes quant à la faible connaissance qu'ont les consommateurs des risques pour leur vie privée en ligne et du peu de comportements de protection qu'ils adoptent.

Le présent rapport s'attarde à deux grandes armes défensives disponibles pour les consommateurs dans leur quête de vie privée en ligne : les lois de protection des renseignements personnels dans le secteur privé et les technologies d'amélioration de la confidentialité disponibles en ligne. Les deux présentent actuellement des faiblesses de taille et ne permettent pas ultimement aux consommateurs canadiens d'avoir le dernier mot sur le traitement de leurs renseignements personnels en ligne par des entreprises.

Dans le cas des technologies d'amélioration de la confidentialité en ligne, les problèmes ont surtout a trait à leur très faible notoriété. Relativement peu de Canadiens connaissent les moteurs de recherche privés, les navigateurs privés, les gestionnaires de mots de passe ou encore les réseaux privés virtuels, dont l'utilisation permettrait pourtant de répondre à certaines de leurs préoccupations. Et beaucoup moins encore les ont déjà utilisés ! Leur apport demeure donc marginal. Et les discussions à leur sujet sont difficiles. Les consommateurs se montrent méfiants. Ils doutent de leur fonctionnement, de leur efficacité. Ils ne se sentent pas compétents pour les utiliser. Et lorsqu'ils tentent de se renseigner à leur sujet, peu de ressources sont à même de bien expliquer de quel type d'outils ils ont besoin pour répondre à leurs inquiétudes. Et lorsqu'ils tombent sur les sites Web de certains fournisseurs, ces derniers ne parviennent ni à les renseigner ni à les rassurer adéquatement, la documentation qui s'y trouve étant trop incomplète ou restant au contraire souvent trop complexe pour être accessible. Les consommateurs francophones sont fortement désavantagés, bien souvent confrontés à des sites entièrement ou partiellement unilingues anglophones. Il n'est guère surprenant donc que la méconnaissance de ces technologies soit particulièrement marquée chez eux. Le rapport identifie tout de même de belles initiatives de sensibilisation et d'éducation des consommateurs par certains fournisseurs. Les autres gagneraient à s'en inspirer. Les consommateurs y gagneraient beaucoup également.

Mais il est irréaliste de penser que tous les consommateurs ont ou auront l'envie ou les capacités – même avec des efforts d'éducation populaire accrus – de trouver puis d'employer les technologies d'amélioration de la confidentialité pour protéger davantage leur vie privée en ligne. Ultimement, ces technologies ne sont que des outils complémentaires ; les réelles protections des consommateurs sont prévues à la loi. Du moins, en théorie.

Parce que les lois, les quatre en vigueur au pays qui s'appliquent aux entreprises, présentent des limites importantes d'application qui rendent certains des droits qu'elles y prévoient quelque peu utopiques, malheureusement. L'exemple le plus flagrant est sans aucun doute ce qui constitue, encore, l'élément central de ces lois, soit le droit de regard du consommateur sur le traitement de ses renseignements personnels par une entreprise. Comment peut-il l'exercer s'il n'est pas en mesure de comprendre et d'évaluer les pratiques des entreprises qui lui demandent son consentement, s'il n'est pas en mesure de négocier avec elles ou de refuser leur demande sans devoir renoncer du même coup à l'accès aux biens, services ou contenus qu'elles offrent ? Son consentement n'est bien souvent, ni

éclairé, ni libre. La situation actuelle, soit l'acceptation généralisée, chaque jour, par automatisme, par ignorance, par dépit, mais très rarement par choix réel, des conditions de service d'une multitude de sites Web n'est certes pas une manifestation du pouvoir que l'exigence d'un consentement préalable confère à l'internaute.

Les difficultés d'application du consentement en raison du rapport de force inégal entre les parties ont toujours existé, mais semblent d'autant plus importantes dans le contexte du numérique et de l'économie des données. De manière générale en fait, les lois actuelles de protection des renseignements personnels dans le secteur privé s'appliquent plus difficilement aux pratiques des entreprises en ligne. Pourquoi ? Si ces lois sont neutres technologiquement, c'est-à-dire qu'elles s'appliquent autant hors ligne qu'en ligne, elles n'ont tout simplement pas été pensées pour Internet. Leur adoption date d'entre 1993 et 2003 et elles n'ont depuis fait l'objet d'aucune réforme significative, malgré la perte de contrôle toujours grandissante des consommateurs en ligne.

Nous voilà donc en 2021. Des défis de taille attendent les législateurs canadiens dans la modernisation des lois de protection des renseignements personnels dans le secteur privé. Certains ont déjà commencé l'exercice, comme le démontrent les projets de loi des gouvernements québécois et canadien, qui s'inspirent, quoique pas toujours suffisamment, de la grande réforme européenne de 2016. Certaines préoccupations particulières des consommateurs canadiens dans le contexte du numérique y sont abordées. D'autres restent malheureusement sans réponse…

Le projet de loi québécois a récemment été adopté (septembre 2021). Le projet de loi fédéral, lui, est mort au feuilleton. Il faudra donc que le gouvernement fédéral redépose un projet de réforme de la *LPRPDE*. Souhaitons qu'il inclue cette fois deux éléments particulièrement essentiels à la protection effective des renseignements personnels des consommateurs : l'adoption d'une approche centrée sur la reconnaissance et la protection des droits de la personne et la mise en place d'une obligation pour les entreprises d'offrir par défaut le plus haut niveau de protection des renseignements personnels. La fiction du contrôle dont parle le professeur Obar ne peut plus durer.

Des liens étonnamment faibles entre les acteurs

Le présent rapport mène à un autre constat. Il existe une déconnexion claire entre les préoccupations et les actions des consommateurs, des entreprises désireuses de leur venir en aide et de l'État. Les besoins de protection des consommateurs ne sont pas forcément comblés par les offres des fournisseurs d'outils d'amélioration de la confidentialité en ligne. Certaines préoccupations des consommateurs ne sont pas abordées par les lois actuelles ou ne sont pas traitées aussi sérieusement qu'elles le devraient, selon eux. Et certains principes fondamentaux desdites lois paraissent tout simplement incompatibles avec les comportements ou les réflexes des consommateurs.

Il est pourtant difficile d'attribuer entièrement le blâme à l'État. Les consommateurs ne lui rendent pas toujours la tâche facile. Ils se disent préoccupés, mais ont beaucoup de difficulté à offrir la moindre explication sur ce qui les inquiète concrètement. Ils se disent

inquiets par le profilage en ligne, par exemple, mais ignorent de quoi il s'agit en pratique. Ils sont curieusement d'avis que leur vie privée est adéquatement protégée en ligne, alors qu'ils admettent du même coup en savoir très peu sur les risques pour celle-ci. Ils ne souhaitent pas ou ne se sentent pas en mesure de changer leur comportement en ligne, alors même qu'ils sont pourtant d'avis que c'est ce que devraient faire leurs concitoyens. Difficiles à suivre donc, ces consommateurs !

L'État parait lui aussi un peu confus. Il prétend protéger un droit fondamental, mais accorde régulièrement le dernier mot et, apparemment, l'essentiel de ses préoccupations aux intérêts économiques des entreprises (malgré le titre accrocheur de certaines lois). Il adopte une conception de la vie privée basée sur le contrôle des renseignements personnels, mais en octroie en pratique assez peu aux personnes concernées.

Nous voilà donc face à différents acteurs, qui ont tous un rôle à jouer dans la protection de la vie privée en ligne, mais qui semblent jouer présentement dans des pièces différentes…

RECOMMANDATIONS

Recommandation 1

Attendu qu'Internet influence considérablement l'exercice du droit à la protection de la vie privée des consommateurs ;

Attendu qu'Internet met en péril le droit à la protection de la vie privée, incluant la protection des renseignements personnels des individus ;

Attendu que plusieurs importants vols et fuites de renseignements personnels ont eu lieu dans les dernières années, à la suite notamment de piratage de systèmes informatiques ;

Attendu que le niveau général de préoccupation pour la protection de la vie privée en ligne est relativement élevé chez les consommateurs canadiens ;

Attendu que les lois de protection des renseignements personnels dans le secteur privé ont été adoptées il y a plus de 20 ans et ont fait l'objet de très peu de modifications depuis ;

Attendu que les nouvelles technologies ont profondément modifié la manière dont les renseignements personnels sont collectés, utilisés et conservés par les entreprises ;

Attendu que certaines règles prévues aux lois de protection des renseignements personnels dans le secteur privé ne sont pas adaptées aux pratiques actuelles de traitement des renseignements personnels en ligne ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS :

De procéder rapidement à une réforme des lois (fédérale et provinciales) de protection des renseignements personnels dans le secteur privé afin de tenir davantage compte des besoins des consommateurs et des réalités du Web et des nouvelles technologies.

Recommandation 2

Attendu qu'Internet est un réseau mondial qui ne s'arrête et ne se limite pas aux frontières physiques des États ;

Attendu que de nombreux États étrangers ont adopté de nouvelles lois de protection des renseignements personnels dans les dernières années ;

Attendu que le *Règlement général sur la protection des données* (*RGPD*) a été adopté en Europe en 2016 et a été globalement applaudi à titre de première grande réforme de la protection des renseignements personnels, malgré des critiques à l'endroit de certaines dispositions spécifiques ;

Attendu que l'Europe représente un partenaire économique important pour le Canada et que le *RGPD* limite le transfert de renseignements personnels vers des pays dont le niveau de protection des renseignements personnels est inférieur ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS :

De s'inspirer des principes législatifs développés dans des initiatives étrangères, tout particulièrement dans le *RGPD*, pour l'élaboration d'une réforme complète et cohérente des lois fédérale et provinciales de protection des renseignements personnels dans le secteur privé.

Recommandations 3 et 4

Attendu que la protection de la vie privée est reconnue comme un droit fondamental au Canada ;

Attendu que les droits fondamentaux des individus sont interdépendants et se renforcent mutuellement ; et que le droit à la protection de la vie privée est donc intrinsèquement lié à l'exercice d'autres droits fondamentaux ;

Attendu que certaines nouvelles technologies, dont les systèmes d'intelligence artificielle, sont susceptibles d'être utilisées d'une manière qui expose les droits fondamentaux des consommateurs à des risques accrus ;

Attendu qu'en cas de conflit entre l'atteinte des objectifs commerciaux et la protection de la vie privée, il importe que le respect d'un droit fondamental l'emporte ;

Attendu que le *RGPD* se base sur la reconnaissance et le respect des libertés et droits fondamentaux, en particulier le droit des individus à la protection des données à caractère personnel ;

UNION DES CONSOMMATEURS RECOMMANDE AU LÉGISLATEUR FÉDÉRAL :

D'adopter, dans le cadre de la réforme de la *LPRPDE*, une approche globale basée sur la protection des droits de la personne ;

De reconnaitre explicitement un droit à la protection de la vie privée des consommateurs dans ladite loi.

Recommandations 5 à 7

Attendu que le contrôle des consommateurs sur leur vie privée en ligne s'exerce principalement par l'expression d'un consentement libre et éclairé au traitement de leurs renseignements personnels ;

Attendu que le contrôle qu'exercent les consommateurs sur le traitement de leurs renseignements personnels en ligne est intimement lié à la sauvegarde de leur dignité et de l'autonomie humaine ;

Attendu que le modèle d'*opt-out* prévu aux lois canadiennes de protection des renseignements personnels dans le secteur privé est inadéquat, notamment parce qu' :

- Il ne tient pas compte des difficultés actuelles auxquelles font face les consommateurs qui tentent de prendre connaissance, de comprendre et d'évaluer les pratiques de traitement des renseignements personnels des entreprises ;
- Il ne tient pas compte du dilemme auquel font régulièrement face les consommateurs en ligne (choisir entre la protection des renseignements personnels ou l'accès et l'utilisation de biens et services de base en ligne) ;

Attendu que les consommateurs canadiens ont un niveau de préoccupation modérément élevé en ce qui concerne une perte de contrôle à l'égard du traitement de leurs renseignements personnels en ligne (circulation, collecte, utilisation) ;

Attendu que les lois actuelles de protection des renseignements personnels dans le secteur privé offrent peu de recours utiles aux consommateurs victimes d'une atteinte à leur droit à la protection de leur vie privée ;

Attendu que les organismes chargés de la surveillance et du respect des lois de protection des renseignements personnels dans le secteur privé n'ont aucun pouvoir exécutoire direct et sont fortement sous-financés ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS

De maintenir et renforcer le consentement libre et éclairé à titre de base de l'encadrement législatif en vigueur en matière de protection des renseignements personnels dans le secteur privé et de limiter les exceptions susceptibles de l'affaiblir ou de le vider de son sens ;

De mettre en place un modèle de consentement de type *opt-in* (explicite et distinct) pour tout traitement non essentiel de renseignements personnels ;

De reconnaitre un droit de poursuite privée non conditionnel aux démarches d'organismes publics pour les consommateurs dont les renseignements personnels n'ont pas été traités conformément aux lois.

Recommandation 8

Attendu que le contrôle des consommateurs sur leurs renseignements personnels, qu'ils exercent principalement au moyen du consentement, est intimement lié à la sauvegarde de la dignité et de l'autonomie des individus ;

Attendu que l'expression d'un consentement adéquat est difficile en ligne, notamment parce que :

- Les consommateurs ne sont pas en mesure de connaitre et de comprendre suffisamment les pratiques de traitement de leurs renseignements personnels et d'évaluer adéquatement les risques auxquels ils s'exposent en donnant leur consentement ;
- Les consommateurs n'ont bien souvent pas le choix de consentir au traitement de leurs renseignements personnels s'ils désirent utiliser ou avoir accès à des biens et services offerts en ligne ;
- Certaines entreprises ont recours à des subterfuges afin d'obtenir le consentement (*dark patterns*) ;

Attendu que l'option par défaut sera généralement retenue par les consommateurs, en raison d'un manque de temps ou de connaissance et de certains biais psychologiques ;

Attendu que les consommateurs canadiens ont un niveau général de connaissance et de compréhension relativement modeste des risques pour la vie privée en ligne et présentent une certaine inertie face à ces risques ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS :

D'imposer aux entreprises qui collectent des renseignements personnels par l'entremise de produits ou de services technologiques l'obligation d'assurer par défaut le plus haut niveau de confidentialité.

Recommandations 9 à 9.2

Attendu que les Canadiens semblent être d'avis qu'ils n'en font pas assez pour protéger leur vie privée en ligne, et ce, par manque de temps, de capacités ou de connaissances ou en raison d'un sentiment général d'impuissance ;

Attendu que les lois actuelles de protection de renseignements personnels dans le secteur privé font reposer une grande part de la responsabilité de la protection de leur vie privée sur les épaules des consommateurs eux-mêmes ;

Attendu que les consommateurs ne sont pas en mesure d'exercer adéquatement cette responsabilité ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS :

De procéder à des modifications législatives afin d'alléger la responsabilité et de faciliter l'exercice de la protection des renseignements personnels qui revient aux consommateurs.

Attendu que le consentement des consommateurs peut être instrumentalisé par des entreprises afin de légitimer des pratiques de traitement des renseignements personnels qui vont à l'encontre des valeurs collectives et de l'intérêt public ou qui constituent des atteintes déraisonnables aux droits individuels ou collectifs ;

Attendu que les consommateurs canadiens ont un niveau de préoccupation modérément élevé en ce qui concerne la prise de décisions automatisées à partir de renseignements personnels et en ce qui concerne le suivi et le profilage à des fins publicitaires en ligne ;

Attendu que le traitement automatisé de renseignements personnels afin de prendre une décision sur la personne concernée est susceptible de porter atteinte à ses droits fondamentaux, notamment son droit à la protection de la vie privée et son droit à la non-discrimination ;

Attendu que l'Union européenne a choisi d'interdire, sauf exception, le traitement automatisé des renseignements personnels à des fins de prise de décision significative au sujet de la personne concernée dans le *RGPD* ;

Attendu que la publicité ciblée qui découle d'un suivi invasif en ligne porte fortement atteinte au droit à la vie privée des consommateurs ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS :

D'envisager l'interdiction de certaines pratiques qui vont à l'encontre de l'intérêt public ou qui présentent des risques déraisonnables pour les droits fondamentaux des individus, par exemple :

- Le traitement de renseignements personnels obtenus au moyen d'un suivi invasif en ligne à des fins de publicité ciblée ;
- Le traitement automatisé de renseignements personnels afin de prendre une décision sur la personne concernée, à moins de prévoir des obligations de transparence spécifiques et un droit de contestation utile.

Attendu que les niveaux de connaissance et de compréhension des entreprises de l'encadrement en vigueur en matière de protection des renseignements personnels tendent à être faibles ;

Attendu que les programmes de certification favorisent une meilleure connaissance par les entreprises des règles et des meilleures pratiques en matière de traitement des renseignements personnels ;

Attendu que les programmes de certification tendent à produire une uniformisation des pratiques au sein de certains secteurs et peuvent ainsi réduire le coût pour les consommateurs (en temps, en analyse, etc.) de la prise de connaissance ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS :

De favoriser et d'encadrer la mise en place de programmes de certification des pratiques de traitement des renseignements personnels dans le secteur privé.

Recommandations 10 et 11

Attendu que certains systèmes et nouvelles technologies, dont ceux relatifs à l'intelligence artificielle, exposent les renseignements personnels des consommateurs à des risques accrus ;

Attendu que les questions liées au stockage non sécurisé et au piratage de renseignements personnels en ligne soulèvent un niveau de préoccupation élevé chez les consommateurs canadiens ;

Attendu que l'encadrement, dans les lois actuelles de protection des renseignements personnels dans le secteur privé, de la sécurité et de la conservation des renseignements personnels détenus par les entreprises parait inachevé et insuffisant à la lumière du recours aux nouvelles technologies par les entreprises ;

Attendu que des cas de piratage à grande échelle de renseignements personnels détenus par des entreprises ont eu lieu dans les dernières années ;

Attendu que le *RGPD* prévoit une obligation pour les entreprises de procéder à une analyse d'impact relative à la protection des données dans certaines situations pour lesquelles le traitement des renseignements personnels à l'aide de nouvelles technologies est susceptible d'engendrer un risque pour les droits et libertés des individus ;

UNION DES CONSOMMATEURS RECOMMANDE AUX LÉGISLATEURS CANADIENS

De clarifier et de renforcer les obligations et la responsabilité légale des entreprises en ce qui concerne la sécurité des renseignements personnels qu'elles collectent, utilisent ou conservent ;

D'imposer aux entreprises l'obligation de procéder à une analyse d'impact relative à la protection des données ou à une évaluation des facteurs relatifs à la vie privée dans certaines circonstances, similairement à ce qui est prévu au *RGPD*.

Recommandations 12 et 13

Attendu que les gouvernements canadiens et québécois ont déposé en 2020 des projets de loi relatifs à la protection des renseignements personnels dans le secteur privé ;

Attendu que le projet de loi québécois a été adopté par l'Assemblée nationale du Québec le 21 septembre 2021 ;

Attendu que le projet de loi fédéral C-11 est mort au feuilleton à l'été 2021 à la suite de la dissolution du Parlement du Canada ;

Attendu que le projet de loi fédéral a fait l'objet de nombreuses critiques de la part des experts et du Commissariat à la protection de la vie privée du Canada ;

Attendu que le projet de loi fédéral n'assurait pas un niveau de protection adéquat pour la vie privée des consommateurs en ligne ;

UNION DES CONSOMMATEURS RECOMMANDE AU LÉGISLATEUR FÉDÉRAL :

De ne pas redéposer le texte du projet de loi C-11 lors de la prochaine législature ;

De repenser et réécrire entièrement le projet de loi visant à réformer la *LPRPDE*, et ce,

- En s'inspirant davantage du *RGPD* ;
- En consultant préalablement et publiquement les experts et les parties prenantes et en tenant compte des critiques formulées par ces derniers à l'endroit du projet de loi C-11 ;
- En tenant compte des recommandations prévues au présent rapport.

Recommandations 14 et 15

Attendu que les outils d'amélioration de la confidentialité en ligne peuvent améliorer considérablement la protection de la vie privée des consommateurs qui y ont recours ;

Attendu que plusieurs consommateurs canadiens présentent un niveau de littératie numérique relativement faible ;

Attendu que les consommateurs canadiens :

- Utilisent très peu les différents outils d'amélioration de la confidentialité en ligne, sauf exception ;
- Affichent une méconnaissance considérable des outils d'amélioration de la confidentialité en ligne ;
- Sont passablement confus quant à l'utilité et au fonctionnement des différents outils d'amélioration de la confidentialité en ligne ;
- Présentent un haut niveau de méfiance envers certains outils ;

Attendu que les consommateurs canadiens francophones ont une connaissance nettement inférieure des outils d'amélioration de la confidentialité en ligne par rapport à leurs pendants anglophones ;

Attendu que près du quart de la population canadienne a le français comme première langue parlée ;

Attendu qu'il importe de faciliter l'accès à de l'information claire sur les outils d'amélioration de la confidentialité en ligne disponibles pour les consommateurs canadiens afin d'en favoriser l'utilisation ;

Attendu que les sites Web des fournisseurs des outils d'amélioration de la confidentialité en ligne constituent l'une des sources principales d'information sur ces outils ;

Attendu que notre étude des sites Web des fournisseurs d'outils d'amélioration de la confidentialité en ligne révèle :

- Un manque d'information claire et complète en français sur l'utilité et le fonctionnement des outils ;
- La mise en place de ressources d'aide et d'information utiles et innovantes par certains fournisseurs (ex. : assistant virtuel, balado, infolettre, communauté d'utilisateurs) ;

UNION DES CONSOMMATEURS RECOMMANDE AUX FOURNISSEURS D'OUTILS D'AMÉLIORATION DE LA CONFIDENTIALITÉ EN LIGNE :

D'offrir davantage d'information sur leur site Web en langue française ;

De poursuivre ou accroître leurs efforts de simplification et de vulgarisation de l'information présentée sur leur site Web, notamment par l'emploi de termes simples, l'offre d'exemples ou d'explications facilement compréhensibles, l'usage de supports visuels ou le recours à des ressources d'aide innovantes.

Recommandation 16

Attendu que l'information présentée par les fournisseurs d'outils d'amélioration de la confidentialité en ligne sur l'utilité et l'utilisation des outils peut être biaisée en raison de considérations financières des fournisseurs ;

Attendu qu'il importe que les consommateurs canadiens aient accès à de l'information neutre sur la protection de leur vie privée en ligne, incluant les différents risques possibles pour celle-ci et les comportements et outils qui permettent de les réduire ou de les éviter ;

Attendu que plusieurs consommateurs canadiens présentent un niveau de littératie numérique relativement faible ;

Attendu que les consommateurs canadiens :

- Ont un niveau général de connaissance et de compréhension relativement modeste des risques pour la vie privée en ligne ;
- Ont régulièrement une compréhension erronée des pratiques de traitement des renseignements personnels par les entreprises ;
- Adoptent à peine quelques comportements de protection de la vie privée en ligne ;
- Ont une très faible utilisation des différents outils d'amélioration de la confidentialité en ligne, sauf exception ;
- Ont une méconnaissance considérable des outils d'amélioration de la confidentialité en ligne ;
- Ont une importante confusion quant à l'utilité et au fonctionnement des différents outils d'amélioration de la confidentialité en ligne ;
- Ont un haut niveau de méfiance envers certains outils ;

UNION DES CONSOMMATEURS RECOMMANDE AUX GOUVERNEMENTS FÉDÉRAL ET PROVINCIAUX :

De mettre en place des programmes et des outils d'information (en plusieurs langues) pour les internautes canadiens destinés à :

- Expliquer les risques pour la protection de la vie privée et des renseignements personnels en ligne
- Présenter les comportements de protection à adopter en ligne
- Démystifier et exposer les bienfaits de l'utilisation d'outils d'amélioration de la confidentialité en ligne.