L'INDUSTRIE DE L'OMNISCIENCE : LE PROFILAGE COMPORTEMENTAL ET LE DROIT À LA VIE PRIVÉE AU CANADA

Par :
Eric Cormier

Thèse soumise à la Faculté de droit de l'Université d'Ottawa
en vue de l'obtention de la maîtrise en droit

Faculté de droit
Université d'Ottawa

L'INDUSTRIE DE L'OMNISCIENCE : LE PROFILAGE COMPORTEMENTAL ET LE DROIT À LA VIE PRIVÉE AU CANADA

Eric Cormier

RÉSUMÉ

La collecte et l'agrégation des renseignements personnels par des organisations du secteur privé représentent une menace grandissante pour la vie privée des citoyens canadiens. Bien que les pratiques de profilage à des fins commerciales soient en pleine émergence depuis l'arrivée d'Internet, le Canada dispose tout de même de mesures législatives servant à limiter leur impact sur la vie privée des individus. Cependant, certaines organisations parviennent néanmoins à contourner ces mesures législatives par l'entremise d'ententes contractuelles auxquelles adhèrent les utilisateurs d'Internet. Il est donc indispensable que les lois en matière de protection des renseignements personnels soient modernisées afin de minimiser les impacts du profilage en ligne. À cet effet, certaines leçons peuvent être tirées de l'approche européenne en matière de protection des renseignements personnels collectés à partir d'Internet et d'autres technologies d'information et de communication.

TABLE DES MATIÈRES

L'INDUSTRIE DE L'OMNISCIENCE : LE PROFILAGE COMPORTEMENTAL ET LE DROIT À LA VIE PRIVÉE AU CANADA

INTRODUCTION

En cette ère de l'information numérique, un montant croissant de détails sur nos vies et nos habitudes est désormais capté et enregistré. En réalité, très peu d'individus possèdent une notion précise de la quantité de renseignements qui sont collectés, analysés et communiqués à leur sujet sur une base quotidienne[1]. De façon individuelle, ces fragments d'information, généralement constitués de données accessoires ou techniques, peuvent nous paraître insignifiants et sans conséquence sur nos vies privées. Or, il suffit pour une organisation de rassembler toutes ces pièces du puzzle pour obtenir une image qui en dévoile très long sur nos vies et nos comportements[2]. Ce principe, certaines organisations l'ont bien compris. En effet, au-delà des avantages que confèrent les technologies numériques, les traces d'information que nous laissons derrière nous lors de leur usage constituent également un bien commercial inestimable qui se situe au centre d'une véritable industrie de l'analyse et du commerce des renseignements personnels[3].

Poussées par l'accélération du développement des technologies de stockage et d'analyse de données à des prix toujours plus abordables, les organisations qui collectent et qui conservent des renseignements personnels n'ont pas cessé de se multiplier au cours des

---

[1] Voir É.-U., Federal Trade Commission, Preliminary FTC Staff Report, « Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers » (1er décembre 2010), à la p. 23, en ligne: <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> [FTC, « Protecting Consumer Privacy »]. Voir aussi Julia Angwin et Tom McGinty, « Sites Feed Personal Details to New Tracking Industry » *Wall Street Journal* (30 juillet 2010), en ligne : wsj.com <http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html>, où les auteurs citent une étude qui dévoile que les 50 sites Web les plus visités aux États-Unis installent sans avertissement en moyenne 64 dispositifs de traçage sur l'ordinateur des visiteurs.

[2] Voir Commissariat à la protection de la vie privée du Canada, « Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique » (mai 2011), en ligne : <http://www.priv.gc.ca/resource/consultations/report_201105_f.pdf>, à la p. 18 [CPVP, Rapport « Profilage »]. Voir aussi Daniel J. Solove, *Understanding Privacy,* Cambridge, Harvard University Press, 2008, à la p. 118 [Solove, *Understanding*].

[3] CPVP, Rapport « Profilage », *ibid*. à la p. 11 : « Les données sont très lucratives, et il est possible de faire de l'argent au moyen des renseignements personnels fournis sur Internet ».

dernières décennies[4]. De façon générale, les organisations accumulent des renseignements personnels au sujet de leurs consommateurs dans le but d'améliorer l'efficacité de la mise en marché de leurs produits ou pour fournir des services plus personnalisés à leur clientèle[5]. Toutefois, l'accessibilité croissante des technologies performantes permet à ces organisations de créer des dossiers numériques de consommateurs à partir desquels il est possible d'identifier et cibler des individus particuliers.

Or, la puissance et l'accessibilité des nouvelles technologies permettent aux organisations de faire bien plus que de la simple collecte de renseignements personnels. À l'aide de techniques hautement perfectionnées d'analyse de renseignements personnels, des spécialistes en marketing ont développé des méthodes permettant de formuler des prédictions sur les comportements futurs de consommateurs particuliers à partir de données collectées et agréées à leur sujet[6]. Ces « profils psychologiques » offrent un accès sans précédent aux détails les plus subtils de nos vies privées, transformant ces organisations en des êtres virtuellement omniscients. Mais, dans le contexte canadien, quelles sont les protections juridiques qui s'offrent à nous contre les impacts de ses pratiques? L'encadrement juridique et législatif en matière de protection de la vie privée et des renseignements personnels est-il suffisant, voir efficace, pour garantir une protection adéquate aux individus devant la profusion des nouvelles technologies capables de porter atteinte à la vie privée de manière plus importante que jamais?

Le présent travail se concentrera sur l'étude du droit pertinent en matière de protection de la vie privée dans le but d'évaluer si les mesures juridiques actuellement en place au Canada répondent adéquatement aux menaces que représentent les pratiques de profilage comportemental de consommateur effectuées par des associations et des entreprises du secteur privé. Bien que nous acquiescions que la collecte de renseignements personnels puisse s'effectuer à partir d'une très grande variété de technologies, nous nous concentrerons

---

[4] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, Stanford Univeristy Press, 2010, à la p. 38 et 45 [Nissenbaum, *Privacy in Context*].
[5] Corey Ciocchetti, « Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information » (2007-2008)10 Vand. J. Ent. & Tech. L. 553, à la p. 565 [Ciocchetti, « Just Click Submit »].
[6] Daniel J. Solove, *The Digital Person. Technology and Privacy in the Information Age*, New York-Londres, New York University Press, 2004, p. 18 [Solove, *Digital Person*].

principalement à l'étude des pratiques de profilage comportemental effectuées à partir de la collecte de renseignements personnels sur Internet.

D'abord, le premier chapitre de ce travail servira à définir de façon détaillée le concept de profilage comportemental, ainsi qu'à rendre compte de certaines des conséquences indésirables engendrées par celui-ci. Nous ouvrirons cette discussion avec un exposé détaillé de l'histoire du secteur de l'analyse et du partage de données personnelles tel qu'il s'est développé au cours du dernier siècle. Nous verrons notamment comment ce secteur émane du monde de la recherche en marketing, ainsi que la façon dont l'émergence des nouvelles technologies d'information et de communication, particulièrement Internet, a permis à ce secteur de jouir d'une croissance exponentielle depuis les deux dernières décennies. Dans la seconde section de ce chapitre, nous aborderons certaines notions portant sur la théorisation du concept de surveillance dans le but d'exposer les similarités et les risques que partage cette notion avec le profilage comportemental. Dans la troisième section, nous discuterons du risque de la perpétuation de certaines formes de discrimination pouvant être associées aux pratiques de profilages, plus particulièrement à partir de la pensée de l'expert en communication et en étude des médias, Oscar H. Gandy.

Ensuite, dans le deuxième chapitre, nous traiterons en profondeur du développement de la notion de la protection de la vie privée sur le plan juridique. Nous traiterons dans la première section du développement du droit à la vie privée à partir de l'élaboration au cours du 20^{e} siècle de la protection constitutionnelle contre les intrusions de l'État dans les affaires privées des individus en vertu de la *Charte canadienne des droits et libertés*[7]. La seconde section de ce chapitre portera sur l'étude du modèle d'encadrement législatif et juridique qui existe actuellement au Canada afin de nous permettre d'évaluer, lors du troisième chapitre, si ce modèle répond adéquatement aux menaces que représente le profilage comportemental. Nous ferons un résumé des dispositions pertinentes qui figurent dans les lois fédérales et provinciales portant sur la protection des renseignements personnels, plus particulièrement

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

de la *Loi sur la protection des renseignements personnels et les documents électroniques*[8] (LPRPDÉ) et des lois provinciales similaires en matière de protection des renseignements personnels dans le secteur privé, en plus de discuter du rôle et des pouvoirs du Commissariat à la protection de la vie privée du Canada (CPVP) ainsi que de ses homologues provinciaux, le tout combiné à la jurisprudence pertinente issue des tribunaux canadiens et des décisions du CPVP à ce sujet.

Le troisième chapitre sera consacré à l'étude de l'application pratique des dispositions des lois en matière de protection des renseignements personnels dans le secteur privé dans le but d'évaluer leur efficacité pour contrer les menaces engendrées par les pratiques liées au profilage comportemental. Dans la première section, nous discuterons de la façon dont les tribunaux et le CPVP définissent la notion de « renseignement personnel » afin de déterminer quelles catégories de renseignements bénéficient des protections garanties par le droit canadien en la matière, pour ensuite nous permettre d'évaluer comment les renseignements obtenus par des pratiques de profilage s'insèrent dans ces catégories selon leur nature ou leur degré de sensibilité. Dans la section suivante, nous ferons état de la nécessité selon la LPRPDÉ que les organisations ne collectent et n'utilisent des renseignements personnels qu'à des fins jugées acceptables selon une personne raisonnable objective. Dans la troisième section, nous aborderons plus en profondeur de la question de l'obtention du consentement à la collecte et à l'utilisation des renseignements personnels. Nous verrons notamment comment la notion de contrôle des renseignements est centrale aux dispositions portant sur le consentement, pour ensuite aborder les enjeux liés à la validité du consentement. Aussi, nous aborderons la question de la forme appropriée de consentement que doivent chercher à obtenir les organisations en fonction des différents contextes.

Le quatrième chapitre sera principalement consacré à l'étude comparative de l'approche canadienne en matière de protection des renseignements personnels dans le contexte des nouvelles technologies avec l'approche développée par les pays membres de l'Union européenne dans le but d'étaler certaines pistes de solution pertinentes pour

[8] *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5 [LPRPDÉ].

l'amélioration des protections offertes par l'encadrement actuellement en place au Canada. À cet effet, nous étudierons certaines des notions du droit européen qui se démarquent du droit canadien, particulièrement en ce qui concerne la question de la catégorisation des renseignements personnels, ainsi que l'approche en matière d'obtention du consentement pour la collecte et l'utilisation des données dans le contexte des nouvelles technologies d'information et de communication. Finalement, nous ferons un retour au contexte canadien afin d'aborder les propositions de modification de la LPRPDÉ à la lumière des pistes de solutions établies à partir de l'analyse de l'approche européenne en ce qui a trait à la protection des renseignements personnels dans le contexte du profilage comportemental.

CHAPITRE 1 – LE PROFILAGE COMPORTEMENTAL ET SES IMPACTS SUR LA VIE PRIVÉE

Comme nous l'avons mentionné en introduction, la plupart des renseignements qui sont recueillis par des organisations du secteur privé le sont à des fins essentiellement pratiques, ou servent à accomplir des tâches techniques précises. Or, les renseignements dont la fonction principale est de nature purement technique ou pratique peuvent également servir à l'analyse comportementale de consommateurs. Aussi, certaines organisations du secteur privé collectent et analysent des renseignements personnels dans le but spécifique de faire du profilage comportemental. Comment pouvons-nous, alors, faire la distinction entre les pratiques qui constituent une forme d'atteinte à la vie privée et celles qui sont nécessaires au fonctionnement efficace des technologies d'information et de communication? Afin de mieux nous éclairer sur la nature du profilage comportemental et de son impact sur la vie privée des individus, le présent chapitre sera d'abord consacré à l'exploration des différentes pratiques de collecte et d'analyse de renseignements personnels effectuées par des organisations du secteur privé, pour enchainer avec une discussion sur la signification et les impacts de cette pratique sur la société.

1.1. L'émergence, l'omniprésence et l'ampleur du profilage comportemental

1.1.1. Avant Internet

La pratique de récolter des renseignements personnels à des fins commerciales n'est pas née d'hier. Dès les années 1920, le constructeur automobile General Motors développa des techniques de marketing ciblé (de l'expression anglaise *targeted marketing*) reposant sur la cueillette et l'analyse de données concernant les acheteurs potentiels[9]. Ayant découvert que plusieurs propriétaires de voiture du fabricant Ford ne retournaient pas chez ce dernier lors de l'achat de leur voiture subséquente, GM entama une campagne promotionnelle ciblant les propriétaires possédant une voiture Ford âgée de deux ans[10]. Devant le succès

[9] Solove, *Digital Person*, *supra* note 6 à la p. 16; Craig D. Tindall, « Argus Rules: The Commercialization of Personal Information » [2003] J.L Tech. & Pol'y 181, à la p. 183 [Tindall, « Argus Rules »].
[10] Solove, *Digital Person*, *ibid*.

d'une telle campagne, bon nombre d'entreprises ont suivi le chemin tracé par GM et ont commencé à rassembler des données sur les habitudes de consommation de leur clientèle et de la population en générale[11].

Tout au cours de la deuxième moitié du 20e siècle, les nouvelles avancées dans le domaine de l'informatique ont constamment augmenté la capacité des grandes entreprises et des autres organisations du secteur privé de récolter et de stocker des renseignements personnels[12]. De toute évidence, le gage de qualité d'une analyse de marché est directement proportionnel à la quantité d'information qu'une organisation est en mesure de stocker et de traiter. En organisant des quantités massives de renseignements personnels en différentes catégories, les analystes en marketing de ces entreprises pouvaient désormais isoler et cibler les groupes de consommateurs profitables selon des critères très spécifiques, rendant ainsi leurs campagnes publicitaires plus efficaces et plus économes[13].

On voit aussi à cette époque apparaître un nouveau secteur dans le domaine de l'analyse de données commerciales : les courtiers en données (*data brokers* en anglais). Contrairement aux entreprises qui récoltent des renseignements personnels au sujet de leur clientèle dans le but d'améliorer la mise en marché de leurs produits, les courtiers en données ont comme seule mission de récolter, d'analyser et de vendre des renseignements personnels[14]. En faisant la collecte, l'agrégation et l'analyse de renseignements personnels de plusieurs individus, ces organisations sont en mesure d'offrir des gammes diversifiées de produits spécialisés, tels des dossiers détaillés sur les habitudes générales des consommateurs, des données sur les habitudes de consommation dans les supermarchés, de l'information sur les acheteurs d'automobiles, ou même des renseignements de nature médicale[15].

---

[11] Tindall, « Argus Rules », *supra* note 9 aux pp. 183.
[12] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 36-38.
[13] Solove, *Digital Person*, *supra* note 6 à la p. 18.
[14] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 45.
[15] Tindall, « Argus Rules », *supra* note 9 aux pp. 183-84.

À partir des années 1970, les courtiers en données aux États-Unis se sont tournés vers l'analyse des données démographiques à la suite d'une décision du gouvernement fédéral des États-Unis de vendre des bandes magnétiques comportant les données recueillies lors de recensements nationaux[16]. En faisant l'achat de ces bandes magnétiques, les courtiers en données avaient accès à des renseignements portant notamment sur l'âge, la race, le sexe, le revenu annuel familial, l'ethnicité et l'emplacement géographique d'une grande partie de la population américaine[17]. Pour assurer la protection de la vie privée des citoyens, le Bureau du recensement des États-Unis limitait la vente des renseignements en groupements de 1500 foyers, en plus de ne fournir que l'adresse des résidents de ces foyers, et non leurs noms[18]. Toutefois, certaines agences de marketing, dont Donnelly Marketing (faisant aujourd'hui partie de la société Infogroup) et MetroMail (aujourd'hui Experian), ont rapidement commencé à coupler les données obtenues à partir des recensements avec les renseignements disponibles à partir des annuaires téléphoniques et des listes d'enregistrement électorales[19]. En ayant recours à ce type de manœuvre, ces organisations pouvaient désormais créer des bases de données personnalisées comportant des renseignements personnels sur plusieurs millions de consommateurs.

Au cours des années 1980, les spécialistes en marketing ont franchi une nouvelle étape dans le perfectionnement de leur méthode d'analyse en améliorant leurs bases de données avec des renseignements sur les caractéristiques psychologiques des consommateurs[20]. En partant de l'hypothèse que les choix de consommation d'un individu procurent des indices appréciables sur son style de vie, les analystes ont développé une gamme de méthodes visant à mesurer les différentes variables « psychographiques » des consommateurs, tels leurs opinions, leurs intérêts et leurs styles de vie[21]. Parallèlement, la période entre la fin des années 1980 et le début des années 1990 marquera nettement l'entrée des sociétés modernes dans l'ère des technologies d'information et de la transition des

[16] *Ibid.*
[17] Solove, *Digital Person*, *supra* note 6 à la p. 18.
[18] *Ibid.*
[19] *Ibid.*; Tindall, « Argus Rules », *supra* note 9 à la p. 183.
[20] Solove, *Digital Person*, *supra* note 6 aux pp. 18 et 19.
[21] Paul Pellemans, *Le marketing qualitatif : perspective psychoscopique*, Paris-Bruxelles, De Boeck & Larcier, 1998, à la p. 61.

modes de communication analogues vers le support numérique. Le mariage entre le développement de méthodes d'analyses comportementales sophistiquées et l'accès à des technologies performantes à des coûts abordables propulsera l'industrie de l'analyse et du partage de renseignements personnels vers l'âge d'or dans lequel elle se trouve encore aujourd'hui.

1.1.2. Avec Internet

Depuis l'arrivée des nouvelles technologies d'information et de communication en format numérique, dont particulièrement Internet, on assiste à une véritable explosion du volume de données numériques en circulation[22]. D'une part, le faible coût associé à la collecte d'information à partir des nouvelles technologies d'information et de communication représente un motif important pour ces entreprises à se tourner vers le commerce des données numériques[23]. D'autre part, Internet permet l'accès à un montant sans précédent de renseignements personnels, qu'ils soient publiés de façon volontaire ou non. Comme l'indique le professeur Lawrence Lessig, l'architecture d'Internet est constituée de façon à ce qu'elle nécessite que toutes les activités d'un utilisateur soient enregistrées à une étape ou une autre du réseau, permettant ainsi la création d'un montant pratiquement infini de données personnelles pouvant être stocké et agrégé[24]. Bien entendu, cela constitue une véritable mine d'or pour les organisations. C'est ainsi qu'en éliminant les contraintes physiques et économiques autrefois associées à la collecte et au partage de données, Internet est rapidement devenu le noyau du commerce des renseignements personnels[25].

---

[22] Voir Martin Hilbert et Priscila López, « The World's Technological Capacity to Store, Communicate, and Compute Information », (2011) 332:6025 Science 60, où les auteurs démontrent qu'entre 1986 et 2007, la capacité de traitement des ordinateurs a augmenté annuellement de 58 %, la capacité de transmettre de l'information bi-directionnellement a augmenté annuellement de 28 %, et la capacité totale de stockage de données a augmenté annuellement de 23 %. D'ailleurs, en 2007, la capacité totale de l'humanité à stocker de l'information se chiffrait à $2,9 \times 10^{20}$ octets, la capacité totale de communication bi-directionnellement était de 2×10^{21} octets, alors que la capacité totale de commande informatique était de $6,4 \times 10^{18}$ octets par seconde. Voir aussi Andrew Murray, *Information Technology Law*, Oxford, Oxford University Press, 2010, à la p. 37.

[23] Helen Nissenbaum décrit ce phénomène comme une « démocratisation » des technologies de stockage de données, en ce sens où l'accès à ces dernières s'est étendu à une communauté plus large et plus diverse d'utilisateurs individuels et institutionnels : Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 38.

[24] Lawrence Lessig, *Code 2.0*, New York, Basic Books, 2006, à la p. 203 [Lessig, *Code 2.0*].

[25] Solove, *Digital Person*, *supra* note 6 à la p. 22.

Une grande partie de la collecte de renseignements personnels sur Internet se fait typiquement sous la forme de questionnaires remplis volontairement par l'utilisateur. Ces questionnaires permettent aux organisations de recueillir et de traiter de façon rapide, efficace et économe de l'information sur l'ensemble de leur clientèle, dont le nom, l'adresse, le numéro de téléphone et le courriel[26]. Certains services, dont les réseaux sociaux comme Facebook, requièrent de l'utilisateur la divulgation de certains renseignements personnels lors de l'inscription[27], alors que d'autres, notamment les commerçants en ligne comme Amazon et eBay, offrent ce choix dans le but d'améliorer et de personnaliser leur service[28]. Pour les utilisateurs d'Internet, la divulgation de renseignements personnels est souvent motivée par les avantages que cela procure. En effet, pour la plupart des services offerts sur le Web, la conservation en mémoire des renseignements des utilisateurs permet une personnalisation de l'expérience, ce qui se traduit par une augmentation en efficacité et d'une plus grande précision du service[29]. Pour les commerçants comme Amazon et eBay, la mise en mémoire des préférences et des achats antérieurs de leur clientèle permet de perfectionner des listes de suggestions taillées sur mesures pour chaque client[30].

La divulgation volontaire des renseignements personnels est certainement un moyen efficace et très répandu pour les entreprises en ligne d'obtenir de l'information sur les utilisateurs d'Internet. Mais les sites Web peuvent aussi recueillir des données sur les utilisateurs d'Internet de manière plus discrète[31]. Comme nous l'avons mentionné, toute activité sur le Web doit être enregistrée à une étape ou l'autre du processus afin d'assurer

---

[26] Ciocchetti, « Just Click Submit », *supra* note 5 à la p. 563.

[27] Facebook, « Déclaration des droits et responsabilités », art. 4, en ligne : Facebook.com <http://www.facebook.com/terms.php> : « Les utilisateurs de Facebook donnent leur vrai nom et de vraies informations les concernant, et nous vous demandons de nous aider à ce que cela ne change pas ».

[28] Amazon, « Déclaration de confidentialité Amazon.ca », en ligne : Amazon.ca <http://www.amazon.ca/gp/help/customer/display.html?ie=UTF8&nodeId=918814> : « Les renseignements que nous recueillons à votre sujet nous permettent de personnaliser et d'améliorer constamment nos services lors de vos visites sur le site Amazon.ca »; eBay, « Règlement sur le respect de la vie privée d'eBay », en ligne : eBay.ca <http://pages.cafr.ebay.ca/help/policies/privacy-policy.html> : « Notre collecte de renseignements personnels a pour principal objectif de vous offrir une expérience sécuritaire, satisfaisante, efficace et personnalisée ».

[29] Ciocchetti, « Just Click Submit », *supra* note 5 à la p. 565.

[30] *Ibid*., à la p. 567.

[31] Solove, *Digital Person*, *supra* note 6 à la p. 23.

que l'information se rende à bon port. On emploie parfois l'expression « *clickstream data* »[32] pour décrire l'ensemble des renseignements nécessaires pour créer un lien assurant le transfert du contenu d'Internet vers l'ordinateur d'un utilisateur. En d'autres mots, le *clickstream data* représente la traînée d'information concernant la façon dont navigue un utilisateur Web en cliquant sur des liens multiples[33]. Le *clickstream data* est aussi un archive de l'ensemble des activités d'un utilisateur d'Internet dans lequel on retrouve, entre autres, la liste de chaque page visitée sur chaque site Web, le montant de temps passé sur chacune de ces pages, ainsi que l'ordre dans lequel les pages ont été visitées[34].

Pour être en mesure d'associer correctement l'information contenue dans le *clickstream data* avec un utilisateur particulier, les sites Internet et les moteurs de recherche installent des « cookies » dans la mémoire cache du navigateur Web des utilisateurs[35]. Les cookies sont des fichiers installés par les sites Web sur le disque dur de l'utilisateur et qui comportent des séries de codes permettant aux sites d'identifier individuellement chaque utilisateur[36]. Ainsi, lorsque l'utilisateur retourne au site Web, le site cherche pour le cookie dans la mémoire cache du navigateur, identifie l'utilisateur et repère à partir d'une base de données l'information recueillie lors de la dernière visite de l'utilisateur[37]. Les cookies permettent donc à un site Web d'avoir instantanément accès aux moindres détails concernant les interactions antérieures de l'utilisateur avec le site[38].

---

[32] De manière littérale, l'expression anglaise *clickstream data* se traduit comme le flux de données résultant de la somme des clics de souris d'un internaute.
[33] Solove, *Digital Person*, *supra* note 6 à la p. 24.
[34] Daniel B. Garrie et Rebecca Wong, « The Future of Consumer Web Data: A European/US Perspective » (2006) 15:2 Int'l J.L. & I.T. 129, à la p. 130 [Garrie et Wong, « Future of Web Data »].
[35] Omer Tene, « What Google Knows: Privacy and Internet Search Engines » [2008] Utah L. Rev. 1433, à la p. 1447 [Tene, « What Google Knows »].
[36] Daniel J. Solove, Mark Rothenberg et Paul M. Schwartz, *Information Privacy Law*, 2e éd., New York, Aspen, 2006, à la p. 625 [Solove et al., *Information Privacy Law*].
[37] Solove, *Digital Person*, *supra* note 6 à la p. 24.
[38] Dustin D. Bergert, « Balancing Consumer Privacy with Behavioral Targeting » (2010-2011) 27 Santa Clara Computer & High Tech. L.J. 3, à la p. 8 [Bergert, « Balancing Consumer Privacy »].

1.1.3. Le ciblage comportemental, les moteurs de recherche et les réseaux sociaux en ligne

Initialement, le *clickstream data* servait essentiellement à rassembler de l'information technique de base sur un utilisateur du Web, tel le type d'ordinateur utilisé pour accéder à Internet, le navigateur Internet utilisé et l'identification des sites Web visités[39]. Au fur et à mesure qu'augmenta la capacité des sites Web de collecter des renseignements de nature beaucoup plus personnelle, plusieurs entreprises en ligne en sont venues à dépendre de cette information pour livrer des services à leurs consommateurs[40]. L'un des secteurs les plus performants dans ce domaine est sans aucun doute le marché de la diffusion de publicité Internet par ciblage comportemental.

En essence, le ciblage comportemental (de l'anglais *behavioral targeting*) consiste à faire l'analyse des intérêts et des activités des consommateurs afin de leur livrer plus efficacement de la publicité personnalisée[41]. Une version plus élémentaire de cette technique, surtout employée lors des débuts de l'émergence du Web, consiste à diffuser de la publicité ciblée à un utilisateur particulier sur la base de prédictions déduites à partir des interactions de cet utilisateur avec le contenu d'un site Web[42]. Les percées dans le domaine des technologies de stockage de données ont également permis de traiter l'information recueillie par les sites Web avec des modèles statistiques afin de générer des profils individuels pouvant être catégorisés selon des critères démographiques ou selon des groupes intérêts particuliers[43].

Cependant, la croissance rapide et la complexification d'Internet au cours de la dernière décennie ont fait en sorte que les données collectées à partir d'un seul site Web ne

---

[39] Garrie et Wong, « Future of Web Data », *supra* note 34 à la p. 131.
[40] *Ibid*., à la p. 132.
[41] Paul H. Rubin et Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Boston, Kluwer, 2002, à la p. 16 [Rubin et Lenard, *Commercial Use*].
[42] Robert Todd Graham-Collins, « The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat » (2009-2010) 44 Ga. L. Rev. 545, à la p. 552 [Graham-Collins, « Deep Packet »]; Andrew Hotaling, « Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting » (2008) 16 CommLaw Conspectus 529, à la p. 534.
[43] Rubin et Lenard, *Commercial Use*, *supra* note 41 à la p. 16.

suffisent plus toujours à assurer la pertinence des publicités livrées aux utilisateurs[44]. Pour faire face à cette limitation, plusieurs annonceurs et sites Web font affaire avec des régies publicitaires (de l'expression anglaise *advertising networks*). Ces régies se spécialisent dans le jumelage stratégique des annonceurs en ligne avec les sites Web qui possèdent les espaces les plus avantageux pour les publicités[45]. Ce type d'arrangement permet à une régie publicitaire de collecter des renseignements personnels à partir de centaines de milliers de sites Internet différents et d'avoir accès aux détails portant sur les activités d'un utilisateur particulier sur l'ensemble de ces sites[46]. Les régies publicitaires peuvent également coupler les renseignements recueillis avec des données obtenues chez de tierces parties, tels les courtiers en données, pour créer des profils comportementaux hautement détaillés d'utilisateurs Internet[47].

Récemment, une grande partie de l'industrie de la publicité sur Internet s'est concentrée autour des moteurs de recherche, plus particulièrement autour de Google[48]. Pour la majorité des utilisateurs d'Internet, les moteurs de recherches représentent la porte d'entrée au Web[49]. La réputation d'un moteur de recherche dépend donc directement de sa capacité à générer les résultats de recherches les plus pertinents selon les intentions de l'utilisateur[50]. C'est précisément par une maîtrise de ce principe que Google est rapidement parvenu à dominer le marché de la recherche en ligne[51].

---

[44] Graham-Collins, « Deep Packet », *supra* note 42 à la p. 552.
[45] *Ibid*. à la p. 553.
[46] Dennis D. Hirsch, « The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? » (2010-2011) 34 Seattle U. L. Rev. 439, à la p. 448.
[47] *Ibid*., à la p. 448.
[48] Bien que d'autres moteurs de recherche, dont Yahoo! et Bing, s'adonnent également au commerce de publicités sur Internet, Google reste de loin le chef de file de ce marché. Voir Tene, « What Google Knows », *supra* note 35 aux pp. 1434-35. Voir aussi Michael Zimmer, « Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search » (2008) 3 J. Bus. & Tech. L. 109, à la p. 109.
[49] Viva R. Moffat, « Regulating Search » (2008-2009) 22 Harv. J.L. & Tech. 475, à la p. 476 [Moffat, « Regulating Search »].
[50] Tene, « What Google Knows », *supra* note 35 à la p. 1450.
[51] Google détient actuellement environ 84 % du marché international de la recherche en ligne. Voir NetMarketShare, « Search Engine Market Share », en ligne : <http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4>.

La capacité d'un moteur de recherche comme Google de générer des résultats de recherche pertinents repose d'abord sur l'efficacité de son système d'analyse de données de compiler et de traiter des sommes importantes de renseignements portant sur les recherches antérieures de ses utilisateurs, pour ensuite formuler à partir de ces analyses des prédictions sur les intentions cachées de l'utilisateur derrière une recherche particulière[52]. Or, cette collecte massive de donnée est aussi la pierre d'assise sur laquelle repose la source de revenus de Google. Car, si Google est en mesure d'offrir gratuitement la majorité de ses services au grand public, c'est parce qu'il est d'abord et avant tout, sur le plan économique, une régie publicitaire[53]. Selon son plus récent rapport annuel, le commerce de publicités constituait 96 % des revenus totaux de l'entreprise en 2010[54]. Grâce à son système de traitement de données Google Analytics, Google est en mesure d'offrir aux annonceurs une gamme de renseignements statistiques sur le comportement des internautes à partir de données collectées à leur sujet, tel le chemin emprunté par un internaute pour accéder à un site particulier, les achats effectués par cet internaute, les comptes créés par celui-ci ainsi que les sites visités après avoir quitté la page[55]. Comme nous le verrons plus loin dans ce travail, bien que les renseignements que Google offre aux annonceurs avec son système Google Analytics soient généralement communiqués sous une forme anonymisée, en ce sens qu'ils ne comportent pas le nom des individus concernés, il demeure très souvent possible d'identifier par déduction des individus particuliers à partir de l'ensemble des renseignements disponibles[56].

Le commerce de publicité est également la source de revenus principale de plusieurs réseaux sociaux sur Internet. L'accès privilégié dont bénéficient les réseaux sociaux à des quantités substantielles de renseignements au sujet de leurs utilisateurs représente un bien

---

[52] Brian Stallworth, « Future Imperfect: Googling for Principles in Online Behavioral Advertising » (2010) 62 Fed. Comm. L.J. 465, à la p. 470.
[53] Tene, « What Google Knows », *supra* note 35 à la p. 1451.
[54] Google, « Form 10-K, FY 2010 », à la p. 25, en ligne : Google.com <http://investor.google.com/documents/20101231_google_10K.html>.
[55] Google, « Technologie », en ligne : Google.ca <http://www.google.ca/intl/fr/corporate/tech.html>. Voir Paul Ohm, « The Rise and Fall of Invasive ISP Surveillance » [2009] U. Ill. L. Rev. 1417, à la p. 1441.
[56] Voir en général Paul Ohm, « Broken Promises of Privacy: Responding to the Surprising Failure or Anonymization » (2009-2010) 57 UCLA L. Rev. 1701 [Ohm, « Broken Promises »].

inestimable pour les annonceurs qui veulent atteindre efficacement un public cible[57]. Avec un auditoire de plus de 600 millions de membres actifs[58], le réseau social Facebook représente incontestablement une plateforme idéale pour la diffusion de publicité. L'information que détient Facebook sur ces utilisateurs permet aux annonceurs de cibler des groupes démographiques particuliers sur la base d'attributs tels le sexe, l'âge, les opinions politiques, ou toutes autres catégories jugées pertinentes[59]. Contrairement à Google, Facebook offre non seulement l'accès à des statistiques démographiques anonymisées, mais permet également à des tiers de faire la collecte et l'utilisation de l'ensemble des renseignements personnels des utilisateurs qui consentent à ces pratiques en échange de l'utilisation d'applications, tels des jeux, des questionnaires ou des jeux-questionnaires[60].

1.1.4. L'industrie des renseignements personnels

Alors que l'industrie du partage de données personnelles à des fins commerciales fut initialement établie dans le but d'assister les entreprises dans la création de modèles de mise en marché de leurs produits, aujourd'hui elle représente en soi l'une des industries les plus foisonnantes du secteur de l'information. La taille colossale des organisations qui forment cette industrie, les recettes substantielles qu'elles génèrent, ainsi que leur présence accrue dans une multitude de facettes de notre quotidien peuvent nous procurer des indices sur montant de renseignements personnels qui sont recueillis, agréés, analysés et partagés à notre sujet. Les exemples cités dans cette section, bien qu'ils ne représentent qu'une mince part du volume total de cette industrie, serviront néanmoins à jeter davantage de lumière sur l'ampleur de cette pratique. À partir de cette analyse, nous serons en mesure de mieux évaluer l'impact que représente cette industrie sur nos vies privées.

---

[57] William McGeveran, « Disclosure, Endorsement, and Identity in Social Marketing » [2009] U. Ill. L. Rev. 1105, à la p. 1114 [McGeveran, « Disclosure »].

[58] Nicholas Carlson, « Facebook Has More Than 600 Million Users, Goldman Tells Clients » (5 janvier 2011), *Business Insider*, en ligne : Businessinsider.com <http://www.businessinsider.com/facebook-has-more-than-600-million-users-goldman-tells-clients-2011-1>.

[59] McGeveran, « Disclosure », *supra* note 57 à la p. 1115.

[60] CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2009-008, « Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* » [CPVP, Résumé n° 2009-008, « Facebook »], en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.cfm>.

Comme nous l'avons mentionné précédemment, l'industrie du partage de renseignements personnels s'est formée en partie avec l'arrivée des courtiers en données. Un joueur qui a marqué significativement ce secteur depuis les dix dernières années est la société ChoicePoint, Inc. Anciennement basée dans l'État de la Géorgie aux États-Unis, cette entreprise, qui fut acquise en 2007 par la société britannique Reed Elsevier au coût de 3,6 milliards de dollars, prétendait détenir au moment de son acquisition plus de 17 milliards de dossiers individuels portant sur des particuliers et des entreprises[61]. Œuvrant principalement aux États-Unis et au Canada, ChoicePoint se spécialisait dans la vente de renseignements à des organisations du secteur privé, telles les sociétés d'assurance et de marketing direct, mais aussi à des organisations publiques, notamment à certaines agences de maintien de l'ordre[62].

Au cours des années 2000, ChoicePoint a rapidement réussi à accaparer une grande part du marché des courtiers en données en faisant de nombreuses acquisitions de sociétés spécialisées dans la collecte et l'analyse de données[63]. Toutefois, ChoicePoint a retenu particulièrement l'attention du public en 2006 lorsque le Federal Trade Commission des États-Unis ordonna à l'entreprise de payer des amendes totalisant 15 millions de dollars pour avoir vendu par mégarde des dossiers contenant des renseignements personnels à des voleurs d'identité[64]. Selon les autorités, cette vente aurait permis à elle seule plus de 800 cas de vol d'identité[65].

Un autre courtier en données très actif tant aux États-Unis qu'au Canada est multinationale Acxiom. Cette société, basée dans l'État de l'Arkansas aux États-Unis, possède une filiale canadienne depuis 2006[66]. Selon son site Web, Acxiom maintient des

---

[61] En somme, cela représente plus de 250 téraoctets de renseignements concernant la vie d'environ 220 millions d'adultes : Chris Jay Hoofnagle, « Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement » (2003-2004) 29 N.C. J. Int'l L. & Com. Reg. 595, aux pp. 603-03 [Hoofnagle, « Big Brother's »]; Solove et al., *Information Privacy Law*, *supra* note 36 à la p. 630.

[62] Hoofnagle, « Big Brother's », *ibid.* à la p. 600. Voir généralement Electronic Privacy Information Center, « ChoicePoint », en ligne : epic.org <http://epic.org/privacy/choicepoint/>.

[63] Hoofnagle, « Big Brother's », *supra* note 61 à la p. 601.

[64] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 47.

[65] *Ibid.*

[66] Acxiom, « Acxiom Announces New Canadian Data Centre », en ligne : Acxiom.com <http://www.acxiom.com/news/press_releases/2006/Pages/AcxiomAnnouncesNewCanadianDataCentre.aspx>.

bases de données comportant des sources multiples de renseignements personnels, dont certaines données démographiques, des données portant sur les propriétaires de maison, sur les habitudes de consommation, sur le mode de vie, en plus d'offrir des listes d'adresses physiques, de courriels et de téléphones de plus de 176 millions d'individus aux États-Unis seulement[67]. Acxiom a enregistré des revenus de plus de 1 milliard de dollars en 2010[68].

Acxiom partage le marché actuel du commerce de données avec plusieurs autres organisations. Parmi les plus notables, on retrouve la multinationale Experian, dont le revenu en 2009 se chiffrait à 3,9 milliards de dollars[69]. Experian offre notamment un service de recherche en marketing nommé BehaviorBank, qui donne accès à ses clients à une base de données comportant des renseignements sur le style de vie de plus de 47 millions de foyers[70]. Un autre joueur important est la société Infogroup, Inc., basée dans l'État du Nebraska aux États-Unis, qui prétend pour sa part posséder des renseignements sur le style de vie de plus de 210 millions de consommateurs[71].

L'une des branches importantes de ce secteur, et généralement la mieux connue du public, regroupe les agences de crédits, dont les deux multinationales TransUnion et Equifax. Ces agences offrent des services aux organisations qui désirent vérifier la solvabilité de leurs clients, dont les banques, les émetteurs de cartes de crédit, ainsi que certains détaillants[72]. Or, la qualité des services offerts par les agences de crédit dépend de leur capacité de collecter des renseignements sur le plus grand nombre possible d'individus afin d'assurer la mise à jour de leurs dossiers. Par exemple, la filiale canadienne d'Equifax affirme avoir en sa possession des dossiers à jour sur plus de 22 millions de Canadiens[73],

---

[67] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p.46.

[68] Acxiom, « Acxiom Announces Fourth Quarter and Fiscal Year 2010 Results », en ligne : Acxiom.com <http://www.acxiom.com/news/press_releases/2010/Pages/AcxiomAnnouncesFourthQuarterandFiscalYear2010Results.aspx>.

[69] Experian, « Company Profile », en ligne : experian.com <http://www.experian.com/corporate/experian-profile.html>.

[70] Experian, « BehaviorBank Lifestyle Data », en ligne : experian.com <http://www.experian.com/marketing-services/targeted-consumer-marketing.html?cat1=customer-acquisition&cat2=target-prospects>.

[71] Infogroup, « Data Services », en ligne : Infogroup.com <http://www.infogroup.com/our-services/data-services.aspx>.

[72] Solove et al., *Information Privacy Law*, *supra* note 36 à la p. 702.

[73] Equifax, « Industry-Specific », En ligne : equifax.com <http://www.equifax.com/consumer/industry-specific/en_ca>.

alors que TransUnion Canada affirme avoir de l'information sur plus de 20 millions de Canadiens[74].

Certaines organisations se spécialisent également dans la vente de renseignements personnels au grand public. C'est notamment le cas de la société Accusearch, Inc., qui opère sur Internet sous la bannière d'Abika.com. L'entreprise, basée dans l'État du Wyoming aux États-Unis, offre une gamme de services de recherche de renseignements personnels au sujet d'individus obtenus à partir de multiples bases de données publiques et privées[75]. L'un des services les plus controversés offerts par Abika.com est la vente de « profils psychologiques » d'individus identifiables. Abika.com crée ces profils à partir de renseignements sur les comportements et les traits de personnalité de ces individus que l'entreprise obtient à partir de sources multiples de données[76].

Le second secteur important de l'industrie de la collecte, du couplage et du partage de renseignements personnels est le marketing direct sur Internet. Comme nous l'avons mentionné, le moteur de recherche Google représente aujourd'hui l'un des joueurs les plus redoutables de ce secteur. En 2008, Google a fait l'acquisition de la société DoubleClick, une régie publicitaire qui prétendait déjà posséder en 2000 des renseignements sur plus de 100 millions d'internautes[77]. Avec l'acquisition de DoubleClick, Google s'est emparé de presque 70 % du marché total de la vente de publicités en ligne[78]. En 2010, les revenus de Google, dont la quasi-totalité provient de la vente d'espaces publicitaires, se chiffraient à 29,3 milliards de dollars[79]. Pour sa part, le réseau social Facebook, qui possède plus de 9 %

[74] Transunion Canada, « Fast Facts », en ligne : Transunion.ca <http://www.transunion.ca/ca/aboutus/aboutus_en.page>.
[75] CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2009-009, « Plainte en vertu de la LPRPDÉ à l'égard d'Accuserach Inc. s/n Abika.com » [CPVP, Résumé n° 2009-009], en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009_009_rep_0731_f.cfm>.
[76] *Ibid.*
[77] Ira S. Rubinstein, Ronald D. Lee et Paul M. Schwartz, « Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches » (2008) 75 U. Chi. L. Rev. 261, à la p. 271.
[78] Moffat, « Regulating Search », *supra* note 49 à la p. 486.
[79] Securities and Exchange Commission, en ligne : sec.gov <http://www.sec.gov/Archives/edgar/data/1288776/000119312511032930/d10k.htm>.

du marché de la publicité en ligne, est estimé d'avoir généré des revenus d'environ 2 milliards de dollars en 2010[80].

1.2. Les impacts du profilage sur Internet

1.2.1. Profilage et surveillance

À la lumière de ce que nous avons vu dans la section précédente, il est apparent que les pratiques qui consistent à collecter et compiler des montants importants d'information sur des individus dans le but de créer des profils comportementaux détaillés à leur sujet représentent une menace substantielle à la vie privée des particuliers. Mais, le plus inquiétant, c'est l'apparente ignorance chez le grand public du fait qu'un grand nombre d'organisations utilisent ce genre de pratiques sur une base quotidienne, et que les méthodes permettant la collecte et l'utilisation des renseignements personnels sont présentes dans la plupart des différentes technologies d'information et de communication. En effet, au moment où les scénarios les plus pessimistes à propos de la surveillance de l'État ont refait surface dans la conscience populaire, notamment à la suite de la mise en place de nouvelles mesures de sécurité en réponse aux attentats du 11 septembre 2001[81], le profilage effectué par les organisations du secteur privé semble quant à lui être passé pratiquement inaperçu[82]. Pourtant, en quoi les activités de surveillance des organisations publiques sont-elles si différentes des activités de profilage sur Internet par des organisations du secteur privé?

Dans une certaine mesure, il est concevable que ce manque général de compréhension de la part du public soit simplement relié au fait que ce phénomène est très récent et demeure difficile à conceptualiser et vulgariser de façon à ce que ces impacts soient

---

[80] Brian Womack, « Facebook 2010 Sales Said Likely to Reach $2 Billion, More Than Estimated » (16 décembre 2010), en ligne : Bloomberg.com <http://www.bloomberg.com/news/2010-12-16/facebook-sales-said-likely-to-reach-2-billion-this-year-beating-target.html>.

[81] Par exemple, le *Patriot Act* des États-Unis a apporté plusieurs changements controversés aux méthodes de surveillance, dont l'expansion de la capacité du gouvernement de mener des fouilles sans préavis, la permission de collecter des renseignements liés à l'ADN d'individus trouvés coupables de crimes violents, l'augmentation des capacités du gouvernement de surveiller les activités informatiques de suspects sans l'obtention de mandats, et l'augmentation de la capacité du gouvernement d'avoir accès à des dossiers détenus par de tierces parties. Voir Adam D. Moore, Privacy Rights*: Moral and Legal Foundations*, University Park, Pennsylvania University Press, 2010, aux pp. 191-2.

[82] Voir CPVP, Rapport « Profilage », *supra* note 2 à la p. 31, où le CPVP mentionne que « […] la façon dont les données sont recueillies et utilisées est en grande partie invisible pour la plupart des utilisateurs […] ».

plus appréciables pour le commun des mortels. En revanche, les auteurs et les experts en matière de vie privée ont écrit abondamment sur les conséquences liées à la surveillance au cours du dernier siècle. Le sociologue David Lyon définit la surveillance comme toute forme d'observation de certains comportements humains dont l'objectif surpasse la simple curiosité[83]. Il rajoute que, de manière générale, la surveillance est une attention focalisée, systématique et routinière portée sur les détails personnels d'un individu à des fins d'influence, de gestion, de protection ou d'orientation[84]. Pour sa part, Helen Nissenbaum fait une légère distinction entre la surveillance et le suivi des activités d'un individu (qu'elle nomme *tracking* et *monitoring* selon la terminologie anglaise). Selon elle, la surveillance est davantage associée à un ensemble de présomptions politiques, notamment le fait d'être accomplie par une figure d'autorité ou de pouvoir à des fins de contrôle social ou pour modifier le comportement de la personne surveillée[85]. À l'inverse, Lyon considère plutôt que la collecte de renseignements personnels à des fins de marketing s'insère logiquement dans l'élaboration contemporaine de la surveillance[86].

Or, avant la démocratisation des technologies permettant la collecte et la conservation de données à grande échelle, le débat en la matière reposait essentiellement sur la conceptualisation du droit contre les intrusions dans la vie privée des particuliers effectuées par des gouvernements ou d'autres organisations du secteur public[87]. En effet, au cours de la plus grande partie du 20e siècle, seul l'État possédait les moyens nécessaires pour garder efficacement un œil sur les affaires privées des individus. En réalité, ce n'est que depuis les deux dernières décennies que les organisations du secteur privé disposent des outils nécessaires à la collecte massive de renseignements portant sur les intérêts et les activités des consommateurs[88]. Par contre, le sujet de la surveillance excessive exercée par l'État et les conséquences qui en découlent ont fait leur entrée dans la conscience collective depuis déjà un certain temps. Inspirés notamment par les dérapages des régimes totalitaires

[83] David Lyon, *Surveillance Studies: An Overview*, Cambridge, Polity, 2007, à la p. 13 [Lyon, *Surveillance Studies*].
[84] *Ibid*., à la p. 14.
[85] Helen Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 22.
[86] Lyon, *Surveillance Studies*, *supra* note 83 à la p. 46.
[87] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 36.
[88] *Ibid*., à la p. 38.

en Europe au cours du siècle dernier et le climat politique de l'époque, certains auteurs et critiques publièrent des œuvres qui permirent au grand public d'apprécier davantage les effets pervers de la surveillance. C'est notamment le cas de l'écrivain anglais George Orwell, qui, avec son roman *1984*, popularisa le sujet avec sa représentation de l'État totalitaire caractérisé par l'analogie du Big Brother (« Grand Frère » en français, bien que la traduction française du roman conserve l'expression Big Brother), cette figure omnisciente et omniprésente qui observe constamment ses sujets[89].

Sans aucun doute, Orwell a offert une des conceptions les plus populaires, accessibles et utiles de la surveillance avec son œuvre *1984*. Mais, chez les théoriciens, le concept du Big Brother trouve son égal dans le panoptisme, une théorie de gouvernance développée par le philosophe français Michel Foucault[90]. Le panoptisme de Foucault s'inspire du Panoptique, un modèle de prison conçu au 18e siècle par le philosophe Jeremy Bentham, dont la configuration architecturale particulière permet à un garde placé au centre de la prison d'observer les prisonniers dans leurs cellules sans que ceux-ci puissent savoir à quel moment ils sont observés, mais tout en sachant qu'ils peuvent être observés en tout moment[91]. Foucault se sert de ce concept comme une analogie servant à décrire les sociétés de surveillance dans lesquelles les dirigeants, à l'aide de technologies, tirent leurs pouvoirs de leur capacité d'observer sans être vus[92]. Ainsi, le Panoptique et Big Brother représentent chacun une vision du contrôle social absolu assuré par une surveillance omniprésente de la population par un pouvoir centralisé.

Certains auteurs ont adapté l'analogie du Big Brother afin d'illustrer les atteintes à la vie privée causées par la compilation de renseignements personnels par des organisations du secteur privé, faisant référence à celles-ci en tant que « Little Brothers » (qui signifie « Petits

---

[89] George Orwell, *Nineteen Eighty-Four*, London, Secker & Warburg, 1949. Voir Lyon, *Surveillance Studies*, *supra* note 83 à la p. 52.
[90] Michel Foucault, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975. Voir Solove, *Digital Person*, *supra* note 6 à la p. 30.
[91] Marcy Peek, « The Observer and the Observed: Re-imagining Privacy Dichotomies in Information Privacy Law » (2009) 8 Nw. J. Tech. & Intell. Prop. 51, à la p. 53.
[92] Lyon, *Surveillance Studies*, *supra* note 83 aux pp. 57 et 58.

frères » en français)[93]. Concernant la collecte de renseignements sur Internet, le professeur et juriste Paul Schwartz explique que l'efficacité et la capacité illimitée du Web pour effectuer de la surveillance numérique ont engendré une myriade de « Little and Big Brothers »[94]. À ce propos, l'expert des technologies d'information Roger Clark utilise le terme « *dataveillance* »[95] pour décrire les pratiques de compilation massive de données[96]. Comme l'indique Daniel Solove, la *dataveillance* représente une nouvelle forme de surveillance qui consiste à observer les individus, non pas de manière directe comme à travers de l'objectif d'une caméra, mais par la collecte de faits et de renseignements à leur sujet[97].

Toutefois, comme l'explique Solove, l'analogie du Big Brother est insuffisante pour décrire adéquatement les problèmes associés à la compilation massive de renseignements personnels par des organisations du secteur privé[98]. Comme il l'indique, en observant l'évolution de l'utilisation des bases de données personnelles, on remarque que celles-ci ne se sont pas développées de façon à servir les fins d'un quelconque complot, mais qu'elles évoluent plutôt en fonction des besoins technologiques qui émergent de l'expansion des bureaucraties des secteurs public et privé. En effet, ces pratiques ont émergé d'un groupe de différents acteurs avec une multitude d'objectifs différents qui tente de prospérer dans une société de plus en plus informatisée[99]. Mais, le défaut le plus important de l'analogie du Big Brother selon Solove est qu'il ne décrit pas correctement la nature des pouvoirs derrière les pratiques de profilage. Comme il l'explique, la compilation de données et le profilage effectués par les organisations du secteur privé ne renferment pas le caractère répressif que le contrôle social total, comme celui exercé par le Big Brother, peut avoir sur la société[100].

Cependant, Solove précise qu'il ne faut tout de même pas écarter les effets pervers de la surveillance effectuée par la compilation de données personnelles. Comme il le

---

[93] Solove, *Digital Person*, *supra* note 6 à la p. 32.
[94] *Ibid.*
[95] L'expression « *dataveillance* » est une contraction des mots « *data* », qui signifie « donnée », et « surveillance ».
[96] Roger Clark, « Information Technology and Dataveillance », tel que cité dans Solove, *Digital Person*, *supra* note 6 à la p. 33.
[97] Solove, *Digital Person*, *supra* note 6 à la p. 33.
[98] *Ibid.*
[99] *Ibid.*, à la p. 34.
[100] *Ibid.*

mentionne, le simple fait qu'un individu soit conscient qu'il est observé peut certainement mener à une forme d'autocensure et d'inhibition de sa part[101]. Aussi, la surveillance peut dans certains cas inciter une internalisation des normes sociales, rendant conséquemment de plus en plus difficile la reconnaissance du caractère répressif de celles-ci. Pour Solove, ces enjeux sont tout aussi importants puisqu'ils concernent directement le type de société que nous bâtissons, notre façon de penser, ainsi que notre capacité à exercer un contrôle significatif sur nos vies[102].

1.2.2. Profilage et discrimination

En plus des conséquences liées aux caractéristiques du profilage comportemental qui s'apparentent à la surveillance, cette pratique peut également engendrer une certaine forme de discrimination sociale. C'est dans cet esprit que l'expert en communication et en étude des médias Oscar H. Gandy, auteur de l'ouvrage innovateur *The Panoptic Sort*, a cherché à établir une connexion entre le manque de protection à la vie privée et certaines formes d'inégalités sociales. À partir d'une recherche empirique centrée sur l'économie politique des renseignements personnels, Gandy tente de démontrer comment les technologies de compilation de données personnelles et de profilage sont fondamentalement discriminatoires[103]. Selon lui, les pratiques d'agrégation et de profilage, qu'il décrit comme une forme de « classement panoptique », accentuent les inégalités sociales par leur capacité à renforcer de manière inéquitable certains traits négatifs chez les individus[104]. En d'autres mots, le profilage des consommateurs par les organisations du secteur privé entraîne une forme de classement social qui rappelle celle engendrée par une gouvernance panoptique[105].

Cette thèse de Gandy s'inscrit dans une étude plus générale de la nature des renseignements obtenus à partir d'un processus de profilage. Pour Gandy, les renseignements personnels sont produits, reproduits et partagés continuellement en tant que

[101] *Ibid.*, à la p. 35.
[102] *Ibid.*
[103] Lyon, *Surveillance Studies*, *supra* note 83 à la p. 42.
[104] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 79.
[105] Lyon, *Surveillance Studies*, *supra* note 83 à la p. 42.

sous-produit inévitable de l'existence humaine[106]. À cet égard, il rappelle la nécessité de comprendre que ce type de renseignements personnels est un produit de l'observation du comportement d'un individu, et non du comportement même. En effet, l'information qui est collectée à partir de l'observation de comportement est en réalité une construction arbitraire[107]. Comme il le mentionne, un profil Internet n'est pas une représentation fidèle des attributs d'un individu, mais peut mieux être décrit comme une liste de différentes catégories qui ont été déterminées par une organisation comme étant pertinentes pour assister à une quelconque prise de décision administrative à l'égard d'un individu, d'un groupe ou d'une classe. L'objet fondamental d'un profil consiste donc à assigner un individu à une classe ou à une catégorie en fonction d'une décision ou d'une conséquence[108]. Ensuite, cette information peut être reproduite, emmagasinée et communiquée de la même manière que toutes autres formes d'information[109].

Pour Gandy, le développement et l'utilisation de profils de consommateurs favorisent le recours à la segmentation du marché comme moyen de faire croitre les ventes et le profit[110]. À son avis, les promoteurs et les firmes de marketing perpétuent une forme de rationalisation du marché en ayant recours à des techniques de classification des individus dans le but d'identifier ceux qui partagent certains attributs les rendant plus particulièrement attirants en tant que consommateurs potentiels[111]. Les firmes de marketing produisent ainsi des ventes grâce à des techniques d'analyse et de compilation des renseignements afin d'améliorer le placement stratégique de matériel promotionnel qu'ils jumèlent avec des consommateurs en fonction de leurs attributs. À cet égard, le profilage des consommateurs peut être interprété comme un facteur de productivité[112].

---

[106] Oscar H. Gandy, Jr., « Toward a Political Economy of Personal Information » (1993) 10 CSMC 70, à la p. 76 [Gandy, « Toward »].
[107] *Ibid.*
[108] Oscar H. Gandy, Jr., « Exploring Identity and Identification in Cyberspace » (2000) 14 Notre Dame J.L. Ethics & Pub. Pol'y 1085, à la p. 1099 [Gandy, « Exploring »].
[109] Gandy, « Toward », *supra* note 106 à la p. 76.
[110] Gandy, « Exploring », *supra* note 108 à la p. 1101.
[111] Lyon, *Surveillance Studies*, *supra* note 83 à la p. 42.
[112] Gandy, « Toward », *supra* note 106 à la p. 87.

Gandy soutient que la discrimination survient lorsque certains consommateurs sont écartés en fonction de certains marqueurs d'identification jugés non désirables, alors que d'autres sont conservés en tant que cibles à fort potentiel de profits[113]. En effet, lorsque filtrés et organisés par un tel classement panoptique, les individus risquent d'être discriminés en fonction des inégalités initiales qui les séparent. Conséquemment, certains individus classés selon des marqueurs plus favorables seront jugés dignes de différents privilèges, tels que des offres spéciales sur certains produits de consommation, des hypothèques, des rabais ou des cartes de crédit, alors que d'autres seront considérés comme ne méritant pas ces avantages[114].

Mais, le profilage des consommateurs peut aussi être compris comme une forme de gestion du risque[115]. Gandy fait référence à la notion du « modèle d'assurance » pour illustrer comment les organisations se servent de profils pour classifier les consommateurs selon leur potentiel de risque, puis refusent ou limitent l'accès à leurs services à de tels individus. Il donne l'exemple de certaines entreprises de location de voitures qui refusaient de servir les résidents d'une certaine région si ces derniers n'étaient pas en mesure de fournir une carte de crédit « or » ou « platine », ou d'autres renseignements, dont des preuves d'assurances automobiles personnelles, sous prétexte que les habitants de cette région étaient plus propices d'être impliqués dans un accident avec une voiture louée[116].

Or, pour Gandy, ces processus sont généralement fondés sur des présomptions erronées. En effet, il observe que l'utilisation du profilage dans le but de créer des modèles de prédiction du comportement humain suppose à tort que l'identité d'un individu peut être réduite, captée ou représentée par des attributs mesurables[117]. Par exemple, il indique que, du fait que les mesures les plus généralement utilisées sont celles qui concernent les comportements de consommation des individus, les « identités » qui découleront d'un

[113] Lyon, *Surveillance Studies*, *supra* note 83 à la p. 42.
[114] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 80.
[115] Gandy, « Toward », *supra* note 106 à la p. 87.
[116] *Ibid.,* à la p. 88.
[117] Solove, *Digital Person*, *supra* note 6 à la p. 181.

processus de profilage seront nécessairement unidimensionnelles[118]. Mais surtout, il avance que les marqueurs de classification inscrits dans les modèles de prédictions, tels les marqueurs raciaux et ceux liés aux sexes des consommateurs, entrainent une distribution inégale de certains désavantages[119]. Gandy soutient que cela est attribuable à la nature conservatrice du profilage, en ce sens où une telle technique de classification tend à reproduire et renforcer les décisions que les consommateurs ont pris dans le passé[120]. En raison du fait que les décisions antérieures des individus constituent la base servant à évaluer les options futures de services que leur fourniront les organisations, les désavantages ont tendance à se répéter de façon cumulative pour les individus les plus défavorisés[121].

Aussi, comme le mentionne Helen Nissenbaum, le classement panoptique nous prive d'autonomie d'une manière beaucoup plus subtile que les situations dans lesquelles certaines formes d'expression individuelles sont punies ou explicitement interdites[122]. La surveillance à grande échelle, l'agrégation et l'analyse des renseignements, soutient-elle, servent à amplifier l'éventail d'influences que les acteurs en position de contrôle, tels les gouvernements et les firmes de marketing, peuvent avoir sur les choix et les actions des individus. Ces techniques d'influence, qui s'apparente à celles utilisées par les escrocs, peuvent contribuer à l'exploitation des faiblesses des individus, à de l'iniquité dans les rapports de négociation, et à la non-divulgation d'opportunités pour certains groupes de personnes. Conséquemment, il semble juste de prétendre que les individus, en choisissant des emplois, des banques ou des produits non pas en raison de leur compatibilité avec leurs

[118] Gandy, « Exploring », *supra* note 108 à la p. 1100.
[119] Lyon, *Surveillance Studies*, *supra* note 83 à la p. 64.
[120] Solove, *Digital Person*, *supra* note 6 à la p. 181.
[121] Lyon, *Surveillance Studies*, *supra* note 83 à la p. 64. Voir Teresa Scassa, « Geographical Information as "Personal Information" » (2011) 10:2 OUCLJ 183, à la p. 210 [Scassa, « Geographical »], où l'auteure cite l'exemple d'une banque qui a refusé d'accorder un prêt à un individu pour l'achat d'une voiture, malgré le bon crédit de ce dernier. À la suite d'une enquête journalistique, il fut découvert que la banque avait publié un communiqué à ses employés les avisant de refuser toute demande de prêt provenant d'individu habitant dans certaines zones identifiées par des codes postaux, incluant notamment toutes les réserves indiennes du Canada : CBC News, « Laurentian Bank loan blacklist targets aboriginal reserves » (Ottawa, 26 septembre 2008), en ligne : Cbc.ca <http://www.cbc.ca/canada/ottawa/story/2008/09/26/ot-loan-080926.html>.
[122] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 83.

valeurs personnelles, mais parce qu'ils n'ont pas été renseignés à propos d'options plus adéquates, sont en vérité victimes d'une forme de supercherie[123].

[123] *Ibid*., à la p. 83.

CHAPITRE 2 – LE DROIT À LA VIE PRIVÉE ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La protection de la vie privée est une valeur que partage la population canadienne[124]. Mais, devant l'apparition de technologies capables de recueillir, diffuser, analyser, rassembler et conserver des quantités phénoménales d'information à des vitesses aveuglantes, il est raisonnable de supposer que la vie privée est plus menacée que jamais. C'est pourquoi il importe de se demander si nous disposons de mesures juridiques adéquates pour contrer les impacts que risquent d'engendrer ces pratiques. Dans le présent chapitre, nous aborderons les différentes approches visant la protection de l'intégrité de notre vie privée, d'abord en explorant le développement des conceptions théoriques et juridiques de cette notion, pour ensuite aborder plus en détail la notion de la protection des renseignements personnels qui sous-tend l'approche canadienne en matière de protection de la vie privée dans le cadre des activités des organisations du secteur privé. Cette discussion se poursuivra par l'étude des différentes lois en matière de protection des renseignements personnels au Canada et de la jurisprudence qui en découle.

2.1. La genèse du droit à la vie privée et les garanties constitutionnelles

On attribut généralement la première tentative de formulation d'une protection à la vie privée dans des termes juridiques à Samuel Warren et Louis Brandeis qui, vers la fin du 19e siècle, proposèrent d'élargir certains principes de la common law afin de permettre la création d'un « droit de ne pas être importuné par autrui » (de l'anglais *the right to be left alone*)[125]. Mais, au cours du 20e siècle, le droit à la vie privée aux États-Unis s'est également

[124] Voir Les associés de recherche EKOS, Inc.**,** « les Canadiens et la vie privée » (mars 2009), en ligne : <http://www.priv.gc.ca/information/survey/2009/ekos_2009_01_f.pdf>, une enquête réalisée en 2009 pour le compte du CPVP qui a révélé que 90 % des Canadiens sont préoccupés par les répercussions des nouvelles technologies sur leur vie privée.

[125] Samuel Warren et Louis Brandeis, « The Right to Privacy » (1890) 4 Harv. L. Rev. 193, où les auteurs avançaient que le droit de leur époque n'offre aucun remède pour les intrusions dans la vie privée d'un individu, malgré que ces intrusions peuvent créer de la souffrance psychologique et émotionnelle chez certains. Selon eux, le droit pouvait néanmoins évoluer de manière à garantir une telle protection de la vie privée. Voir Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, New Haven, Yale University Press, 2007, aux pp. 108-110 [Solove, *Reputation*].

développé autour de certaines garanties constitutionnelles visant la protection des individus contre l'intrusion de l'État dans leurs affaires privées[126]. Parallèlement, bien que la Constitution canadienne ne mentionne pas explicitement le droit à la vie privée, la Cour suprême du Canada, dans l'affaire *Hunter c. Southam*[127], accorde à celui-ci un statut semi-constitutionnel en fonction du droit à la protection contre les fouilles, les perquisitions ou les saisies abusives de l'État figurant à l'article 8 de la *Charte canadienne des droits et libertés*[128]. Dans l'arrêt *R. c. Plant*, la Cour suprême avance que la protection constitutionnelle du droit à la vie privée reconnue par les tribunaux canadiens s'articule principalement autour d'une conception de la vie privée qui repose sur les valeurs sous-jacentes de dignité, d'intégrité et d'autonomie[129]. Elle rajoute que « l'article 8 de la *Charte* protège un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État »[130].

L'impact des nouvelles technologies sur la vie privée a aussi été discuté explicitement par les tribunaux[131]. La Cour suprême du Canada a conclu, dans l'arrêt *R. c.*

---

[126] En 1886, dans l'affaire *Boyd v. United States*, (1886) 116 US 616, la Cour suprême des États-Unis décida d'élargir la portée du IV^e^ amendement en affirmant que la protection contre les atteintes à la propriété pouvait être interprété comme une garantie de protection contre les fouilles et les saisies déraisonnables de la part de l'État. Voir Ronald E. Leenes, dir., *Constitutional Rights and New Technologies: A Comparative Study*, La Haye, T.M.C. Asser, 2008, à la p. 233 [Leenes, *Constitutional*].

[127] *Hunter c. Southam*, [1984] 2 R.C.S. 145 [*Hunter*].

[128] Dans *Hunter*, la Cour suprême du Canada mentionne pour la première fois le statut quasi constitutionnel du droit à la vie privée. La Cour suprême a également confirmé cette idée dans *R. c. Dyment*, [1988] 2 R.C.S. 417, aux pp. 427-8, où elle indique que « [l]'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique ». Voir aussi *Lavigne c. Canada* (Commissariat aux langues officielles), [2002] 2 R.C.S. 773, par. 24 et 25, où la Cour suprême reconnait le statut quasi-constitutionnel de la *Loi sur la protection des renseignements personnels*, L.R.C., 1985, c. P-21, ainsi que *Eastmond c. Canadien Pacifique Ltée*, [2004] A.C.F. no 1043, 2004 CF 852, par. 100 [*Eastmond*], où la Cour fédérale accorde un statut similaire à la LPRPDÉ.

[129] *R. c. Plant*, [1993] 3 R.C.S. 281, au par. 17 [*Plant*].

[130] *Ibid*., par. 20.

[131] Voir *Olmstead v. United States*, (1928) 277 U.S. 438, où la majorité de la Cour suprême des États-Unis conclu que l'interception d'une conversation téléphonique privée ne constituait pas une violation à la vie privée. Or, dans cette affaire, le juge Brandeis, coauteur de l'article « The Right to Privacy » alors juge à la Cour suprême des États-Unis, affirma dans un jugement dissident que les nouvelles technologies de l'époque permettaient au gouvernement de porter atteinte à la vie privée des citoyens de façon plus subtile et plus significative que par le passé, et qu'il était indispensable que les principes constitutionnels s'adaptent aux changements technologiques afin de garantir une protection adéquate contre cette menace. Cette décision fera jurisprudence aux États-Unis jusqu'en 1967, lorsqu'elle sera renversée par l'arrêt *Katz v. United States*, (1967) 389 US 347. Pour la Cour suprême des États-Unis dans *Katz*, la notion de vie privée peut être décrite comme

Wong, que la portée de l'article 8 de la *Charte canadienne* était suffisamment large pour accorder une protection contre la surveillance par l'entremise de nouvelles et futures technologies[132]. Malgré cela, les tribunaux ont également fait état de certaines limites à la protection constitutionnelle de la vie privée. Dans l'arrêt *Hunter*, la Cour suprême rappelle l'importance de rechercher un équilibre entre les droits des individus et le besoin d'effectuer des fouilles et des perquisitions[133]. La Cour précise cette notion d'équilibre dans l'arrêt *Plant* en préconisant l'adoption d'une « méthode contextuelle »[134]. À cet effet, la Cour suprême dans *R. c. Edwards* a noté qu'en tenant compte de l'ensemble des circonstances, il est important de déterminer l'existence d'une attente subjective de vie privée qui doit être évaluée en fonction du caractère raisonnable de cette attente sur le plan objectif[135].

De manière générale, les garanties constitutionnelles du droit à la vie privée peuvent être regroupées en différentes catégories, dont celles qui protègent l'espace, celles qui protègent les individus, et celles qui protègent l'information[136]. La troisième, soit l'intimité informationnelle (*informational privacy* en anglais), est plus pertinente dans le contexte du profilage comportemental. Certes, les garanties constitutionnelles du droit à la vie privée ne procurent habituellement aucun remède pour les préjudices causés par des organisations du secteur privé. Mais, il demeure pertinent de s'attarder aux développements récents dans ce domaine du droit canadien afin de démontrer certains des enjeux qui ont fait surface dans la

---

« son droit de ne pas être importuné par autrui ». Également, elle élargit considérablement la protection constitutionnelle de la propriété en affirmant que le IV[e] amendement de la Constitution des États-Unis « protège les personnes et non les lieux ». Voir Leenes, *Constitutional*, *supra* note 126 à la p. 234. Voir aussi Solove et al., *Information Privacy Law*, *supra* note 36 à la p. 33.

[132] *R. c. Wong*, [1990] 3 R.C.S. 36, [1990] A.C.S. no 118 [*Wong*]. Il est intéressant de noter que le juge LaForest dans l'arrêt *R. c. Wong* précise, au paragraphe 36, qu'il n'appartient pas aux tribunaux, mais bien au législateur d'établir les limites d'utilisation de ces technologies « de même pour toute nouvelle technologie que les progrès de la science mettront à la disposition de l'État dans les années à venir ».

[133] *Hunter*, *supra* note 127 par. 25 : « […] il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi ».

[134] *Plant*, *supra* note 129 par. 19 : « L'examen de facteurs tels la nature des renseignements, celle des relations entre la partie divulguant les renseignements et la partie en réclamant la confidentialité, l'endroit où ils ont été recueillis, les conditions dans lesquelles ils ont été obtenus et la gravité du crime faisant l'objet de l'enquête, permet de pondérer les droits sociétaux à la protection de la dignité, de l'intégrité et de l'autonomie de la personne et l'application efficace de la loi ».

[135] *R. c. Edwards*, [1996] 1 R.C.S. 128, par. 45 [*Edwards*].

[136] Jerry Kang, « Information Privacy in Cyberspace Transactions » (1997-1998) 50 Stan. L. Rev. 1193, à la p. 1202.

jurisprudence concernant la protection juridique des renseignements obtenus à partir de l'utilisation de nouvelles technologies.

À ce sujet, la Cour suprême du Canada, dans l'arrêt *R. c. Tessling*[137], s'est penchée sur la constitutionnalité de l'utilisation par la Gendarmerie royale du Canada (GRC) d'une technologie de captage d'énergie thermique d'une maison aux fins d'une enquête portant sur la production de marijuana. Selon la Cour, bien que l'intimé avait une attente subjective de vie privée à l'égard de l'émanation de chaleur provenant de sa maison, cette attente n'était pas raisonnable d'un point de vue objectif puisque l'obtention de ses renseignements ne révèle rien sur la vie privée, ni sur un ensemble de renseignements biographiques d'ordre personnel de l'intimé[138]. Ainsi, la Cour suprême n'a pas voulu reconnaitre l'argument de l'intimé selon lequel l'information que cherchait à obtenir la GRC n'était pas uniquement le « profil thermique » de sa maison, mais plutôt la déduction que cette information permet de faire sur ce qui se déroule à l'intérieur de la maison[139].

Similairement, dans l'affaire *R. c. Gomboc*[140], la majorité des juges de la Cour suprême a également conclu que l'intimé n'avait aucune attente raisonnable de vie privée à l'égard des renseignements pouvant être déduits par les policiers à l'aide d'une technologie permettant de mesurer la consommation d'électricité d'une maison pour détecter la présence de cultures de marijuana[141]. Les tribunaux ont également traité de la question de l'abandon de l'attente raisonnable de vie privée dans le cadre de l'intimité informationnelle. Dans *R. c. Patrick*[142], la Cour suprême s'est penchée sur l'attente objective de vie privée à l'égard du contenu de sacs d'ordures saisis par des policiers à la limite de la propriété de l'appelant, dans lesquels fut découverts certains éléments nécessaires à la fabrication d'ecstasy. Selon l'appelant Patrick dans cette affaire, les sacs à ordures sont des « sacs d'information » contenant des détails sur le mode de vie et des renseignements d'ordre biographique. Bien que la Cour n'ait pas totalement rejeté cet argument, elle a toutefois conclu que l'appelant

[137] *R. c. Tessling*, [2004] 3 R.C.S. 432, 2004 CSC 67.
[138] *Ibid*., par. 62.
[139] *Ibid*., par. 52.
[140] *R. c. Gomboc*, [2010] 3 R.C.S. 211, 2010 CSC 55
[141] *Ibid*., par. 50.
[142] *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579.

avait renoncé à toute attente objective de vie privée à l'égard du contenu de sacs d'ordures lorsque celui-ci les avait déposés à l'arrière de sa résidence pour être ramassé par les éboueurs[143].

À la lumière de ce qui précède, on dénote une tendance chez la Cour suprême qui consiste à traiter les atteintes à l'intimité informationnelle comme étant peu critiques, particulièrement dans les contextes où les renseignements en cause sont de nature plutôt indirecte. Également, il est étonnant de constater que la Cour suprême dans *Patrick* a conclu que le risque pris par l'appelant en déposant les sacs à ordures derrière sa propriété n'a pas seulement eu l'effet de réduire son attente raisonnable de vie privée, mais plutôt de l'éliminer complètement[144]. Dans la prochaine section, nous aborderons la façon dont les lois en matière de protection des renseignements personnels traitent ces questions dans le contexte des activités des organisations du secteur privé.

2.2. L'encadrement législatif de la protection des renseignements personnels au Canada et dans les provinces

2.2.1. La genèse des lois canadiennes en matière de protection des renseignements personnels

Bien que rien ne semble ralentir la croissance du marché de l'agrégation et du partage de renseignements personnels à des fins commerciales, il demeure que le Canada dispose tout de même d'un cadre législatif en matière de protection des renseignements personnels. Soucieux des impacts découlant de l'émergence de nouvelles technologies d'information et de communication capables de collecter, d'analyser et de diffuser des quantités sans précédent de renseignements, le gouvernement canadien mit en place vers la fin du 20^{e} siècle une série de mesures visant la protection des renseignements personnels des citoyens[145].

---

[143] *Ibid*., par. 63.

[144] Dans *Patrick*, l'opinion dissidente de la juge Abella semble toutefois se départir de cette conclusion. Voir William Mackinnon, « Discarding Reasonable Expectations of Privacy: A Critique of R. V. Patrick » (2010) 47 Alta. L. Rev. 1037, à la p. 1045.

[145] Voir *Englander c. TELUS Communications Inc*., [2005] 2 R.C.F. 572, par. 8-17 [*Englander*], pour une discussion sur la genèse de la loi canadienne en matière de protection des renseignements personnels dans le secteur privé.

Or, bien avant que le gouvernement canadien ne légifère en la matière, les pays européens commençaient déjà à formuler les grandes lignes de leur modèle de protection des renseignements personnels. Dès 1968, le Conseil de l'Europe adoptait la Recommandation 509 visant à établir des limitations non contraignantes aux organisations quant à la durée de conservation de renseignements personnels[146]. En 1981, les membres du Conseil de l'Europe ratifient la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*[147], qui sera complémenté en 1995 par l'adoption de la *Directive 95/46/CE*[148], une mesure imposant des limites encore plus contraignantes aux transferts de données à caractère personnel[149].

Aussi, à cette époque, l'Organisation pour la coopération et le développement économiques (OCDE) établit les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*[150], qui seront également ratifiées par le Canada[151]. C'est d'ailleurs en fonction du respect de ses obligations en vertu de la ratification des *Lignes directrices* de l'OCDE que le gouvernement canadien adopta en 1982 la *Loi sur la protection des renseignements personnels*[152], régissant les activités du secteur public fédéral. Cette loi marqua aussi la création du Commissariat à la protection de la vie privée du Canada[153].

---

[146] Jeremy Warner, « The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps » (2005) 2:1 UOLTJ 75, à la p. 6.
[147] CE, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981, S.T.C.E. nº 108, en ligne : <http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm>.
[148] CE, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [1995] J.O. L 281/31 [CE, *Directive 95/46/CE*], en ligne : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:NOT>.
[149] Lyette Doré, « La législation canadienne sur la protection des renseignements personnels dans le secteur privé » *Développement récents en droit de l'accès à l'information 2003*, Cowansville (Qc), Yvons Blais, 2003, à la p. 244 [Doré, « Législation »].
[150] OCDE, *Annexe à la Recommandation du Conseil du 23 Septembre 1980 : Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, en ligne : ocde.org <http://www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html> [OCDE, *Lignes directrices*].
[151] Doré, « Législation », *supra* note 149 à la p. 242.
[152] *Loi sur la protection des renseignements personnels*, L.R.C., 1985, c. P-21 [LPRP].
[153] Doré, « Législation », *supra* note 149 à la p. 243.

En matière de protection des renseignements personnels dans le cadre des activités des organisations du secteur privé, le public canadien devra attendre jusqu'à l'aube du 21e siècle pour voir apparaître la première mesure législative de portée nationale. La *Loi sur la protection des renseignements personnels et les documents électroniques*[154] (LPRPDÉ), en vigueur depuis le 1er janvier 2001, fut introduite pour la première fois en octobre 1998 dans un effort du gouvernement fédéral de procurer aux citoyens canadiens une protection envers les activités des organisations qui recueillent, utilisent et communiquent des renseignements personnels à des fins commerciales[155]. Dans une certaine mesure, la Loi représente la réponse canadienne aux initiatives des membres de la communauté européenne qui, au cours des années 1980 et 1990, adoptèrent une série de mesures visant à protéger les renseignements personnels des individus devant l'expansion rapide des nouvelles technologies d'information et de communication[156].

Sur le plan de sa structure, la LPRPDÉ tire sa particularité du fait que certaines de ses dispositions revoient à une série de normes regroupées dans un code, intitulée le *Code type sur la protection des renseignements personnels*, qui se retrouve en annexe 1 de la Loi. Ce code fut initialement introduit en 1996 par l'Association canadienne de la normalisation (ACN)[157] après de nombreuses années de recherche et de débat entre plusieurs membres intéressés des secteurs publics et privés[158]. Sous la forme adoptée par l'ACN, le Code était conçu comme une norme volontaire servant de guide aux organisations du secteur privé pour la protection des renseignements personnels qu'ils collectent et utilisent[159]. Puisque cette mesure n'était manifestement pas destinée à procurer un modèle d'encadrement rigoureux caractéristique d'une mesure législative, le gouvernement canadien adopta la LPRPDÉ afin de conférer un caractère contraignant aux principes établis par le Code[160].

---

[154] LPRPDÉ, *supra* note 8.
[155] CPVP, « Document d'information : La *Loi sur la protection des renseignements personnels et les documents électroniques* », en ligne : <http://www.priv.gc.ca/legislation/02_06_07_f.cfm>.
[156] Voir Doré, « Législation », *supra* note 149 à la p. 242.
[157] *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96.
[158] Barbara McIsaac, Rick Shields et Kris Klein, *The Law of Privacy in Canada*, Toronto, Carswell, 2010, à la p. 4-31 [McIsaac et al., *Law of Privacy*].
[159] Doré, « Législation », *supra* note 149 à la p. 245; McIsaac et al., *Law of Privacy*, *ibid*. à la p. 4-32.
[160] Le caractère contraignant des dispositions du Code est garanti par le paragraphe 5(1) de la LPRPDÉ. Voir généralement Teresa Scassa, « Text and Context: Making Sense of Canada's New Personal Information Protection Legislation » (2000-2001) 32 Ottawa L. Rev. 1 [Scassa, « Text and Context »].

Au moment de son adoption, la LPRPDÉ n'avait effet que sur les activités des organisations du secteur privé sous compétence fédérale, c'est-à-dire les entreprises de télécommunication et de radiodiffusion, les institutions financières, les transports interprovinciaux et le secteur de l'aviation commerciale. Or, depuis le premier janvier 2004, la Loi s'applique également à toutes les organisations du secteur privé qui opèrent uniquement à l'intérieur d'une province[161], sauf pour les provinces qui ont adopté une loi essentiellement similaire[162].

2.2.2. Survol des dispositions de la LPRPDÉ

Au sens large, la LPRPDÉ prescrit un certain nombre de limitations aux organisations comme celles qui se spécialisent dans la collecte, le couplage et l'analyse de renseignements personnels à des fins commerciales. Mais, pour bien comprendre la portée de la LPRPDÉ, il est nécessaire de porter attention à son objet tel qu'il fut déterminé par le gouvernement canadien au moment de sa rédaction :

> La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant 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 et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[163].

De prime abord, on constate l'intention du législateur de veiller à ce qu'il y ait un certain équilibre entre le droit à la vie privée des individus et le droit des organisations de réaliser leurs activités. Dans l'arrêt *Englander c. TELUS Communications Inc.*[164], la Cour d'appel fédérale fait état de la notion d'équilibre qui sous-tend l'objet de la LPRPDÉ :

> […] Cet objet est de faire en sorte que lesdites collecte, utilisation et communication soient exécutées d'une manière qui concilie, dans toute la mesure du possible, le droit de la personne à la vie privée et les besoins de

[161] Voir Bibliothèque du Parlement, *Les lois fédérales du Canada sur la protection de la vie privée* par Nancy Holmes, PRB 07-44F, révisé le 25 septembre 2008, à la p. 6.
[162] À ce jour, trois provinces ont adopté une loi jugée essentiellement similaire à la LPRPDÉ, soit le Québec, l'Alberta et la Colombie-Britannique. Voir *infra* note 199 et 200.
[163] LPRPDÉ, *supra* note 8 art. 3.
[164] *Englander*, *supra* note 145.

> l'organisation. Il y a donc deux intérêts concurrents dans l'objet de la LPRPDÉ : le droit de la personne à la vie privée d'une part, et le besoin commercial d'accès aux renseignements personnels d'autre part.

On remarque par ailleurs que l'article 3 contient la seule référence au concept du droit à la vie privée présente dans le libellé de la LPRPDÉ, qui semble plutôt favoriser la protection du concept plus spécifique de renseignement personnel défini comme « [t]out renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail »[165]. Comme nous le verrons dans le prochain chapitre, les tribunaux ont mentionné que la portée de la définition de « renseignement personnel » doit être interprétée de façon large[166].

Comme nous l'avons mentionné, une importante partie de la LPRPDÉ reprend intégralement les dix principes adoptés par l'ANC dans son *Code type*. À cet effet, le paragraphe 5(1) assure le caractère contraignant des dispositions du Code, ce dernier figurant en annexe 1 de la Loi, afin d'assurer une pleine protection aux individus envers la collecte, l'utilisation et la communication de leurs données par des organisations[167]. Également, le

---

[165] LPRPDÉ, *supra* note 8 art. 2.

[166] *Rousseau c. Wyndowe*, [2006] A.C.F. no 1631, [2006] F.C.J. No. 1631, conf. pour d'autres motifs par [2008] A.C.F. no 151, 2008 CAF 39, par. 40 [*Rousseau*] : « Le paragraphe 2(1) de la LPRPDE définit comme suit l'expression « renseignement personnel » : « Tout renseignement concernant un individu identifiable ». La loi a donc une portée très large »; *Johnson c. Bell Canada*, [2009] 3 R.C.F. 67, 2008 CF 1086, par. 30 : « […] puisque la Loi définit un renseignement personnel comme tout « renseignement concernant un individu identifiable », elle a donc une très large portée ».

[167] Dans *Englander*, *supra* note 145 par. 46, la Cour d'appel fédérale indique que « […] étant donné le caractère non législatif de sa rédaction, l'annexe 1 ne se prête pas à l'interprétation rigoureuse habituellement possible. Cela étant, la meilleure solution pour la Cour est de se confier aux critères de la souplesse, du sens commun et du pragmatisme ». Dans *Wansink c. TELUS Communications Inc*., [2007] A.C.F. no 122, 2007 CAF 21, par. 19 [*Wansink*], un arrêt subséquent de la Cour d'appel fédérale, le juge Décary tente de préciser cet argument en rajoutant que, malgré qu'il soit impossible de dire que le point de vue ci-haut s'applique à l'interprétation de la LPRPDÉ elle-même, les mentions répétées de l'annexe 1 ainsi que les dispositions du paragraphe 5(1) de la loi « incitent la Cour à adopter à l'égard de la Loi elle-même une approche moins rigoureuse que celle qu'elle adopterait normalement à l'égard d'une loi ». Dans l'affaire *Morgan c. Alta Flights (Charters) Inc*., [2005] A.C.F. no 523, 2005 CF 421, par. 20, conf. par [2006] A.C.F. no 447, 2006 CAF 121 [*Morgan*], la Cour fédérale précise que les tentatives de collecte de renseignements ne constituent pas une violation de la Loi : « Les obligations de la Loi en matière de protection du droit à la vie privée se trouvent à l'annexe 1 de la Loi. On y trouve les obligations et les recommandations que les organismes doivent suivre ou devraient suivre (selon le cas) lorsqu'elles s'occupent de renseignements personnels. […] Aucun de ces principes ni aucune des dispositions de la Loi ne parle de « tentatives ». Les actes envisagés par la Loi impliquent la collecte, l'utilisation et la communication effectives de renseignements. Les principes et les dispositions de la Loi sont de toute évidence structurés de manière à présumer que les renseignements réclamés par un organisme sont effectivement recueillis […] ».

paragraphe 5(3) précise que toute collecte, utilisation ou communication de renseignements personnels ne peut être faite qu'à des fins « qu'une personne raisonnable estimerait acceptables dans les circonstances ». Pour le juge Décary dans *Englander*, cette disposition renforce la notion d'équilibre qui figure à l'objet de la Loi, en ce sens qu'elle établie « que le droit à la vie privée n'est pas absolu »[168].

En ce qui concerne les principes du Code figurant à l'annexe 1 de la Loi, le premier principe impose aux organisations une responsabilité envers les renseignements personnels dont elles ont la gestion[169]. Cette responsabilité s'applique non seulement pour les renseignements dont une organisation a en sa possession ou sous sa garde, mais également aux renseignements qu'elle confie à une tierce partie[170]. Ce principe précise aussi les démarches que doivent prendre ces organisations afin répondre à leur responsabilité[171]. Le deuxième principe établit que les fins pour lesquelles les renseignements personnels seront recueillis doivent être déterminées par l'organisation avant ou au moment de la collecte[172], que ces fins doivent être documentées[173] et que toutes nouvelles fins doivent être précisées avant l'utilisation[174].

Une grande partie de la LPRPDÉ est consacrée à l'établissement de règles à l'égard de l'obtention du consentement d'un individu à la collecte, l'utilisation et la communication de ses renseignements personnels. À cet égard, le troisième principe figurant en annexe 1 de la LPRPDÉ établit, sous réserve de certaines dispositions figurant à l'article 7 de la Loi, la nécessité pour les organisations d'obtenir le consentement de toute personne pour faire la collecte, l'utilisation ou la communication de ses renseignements personnels[175], et ce, avant ou au moment de la collecte[176]. Pour que le consentement obtenu par l'organisation soit valable, le troisième principe oblige à ce que les organisations fassent un effort raisonnable

[168] *Englander*, *supra* note 145 par. 38.
[169] LPRPDÉ, *supra* note 8 ann. 1, art. 4.1.
[170] *Ibid*., ann. 1, art. 4.1.3.
[171] *Ibid*., ann. 1, art. 4.1.4.
[172] *Ibid*., ann. 1, art. 4.2.
[173] *Ibid*., ann. 1, art. 4.2.1.
[174] *Ibid*., ann. 1, art. 4.2.4.
[175] *Ibid*., ann. 1, art. 4.3.
[176] *Ibid*., ann. 1, art. 4.3.1.

pour communiquer de façon compréhensible à la personne concernée les fins auxquelles ses renseignements seront utilisés ou communiqués[177]. Aussi, il est interdit aux organisations d'exiger le consentement d'un individu à la collecte, à l'utilisation ou à la communication de ses renseignements en échange d'un service, sauf si cela est nécessaire pour réaliser les fins légitimes et clairement indiquées de l'organisation[178].

Aussi, la Loi établie que la forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la sensibilité des renseignements[179], en plus de spécifier que les attentes raisonnables de la personne concernée sont aussi pertinentes pour l'obtention du consentement[180]. La Loi précise également que, toujours selon les circonstances, les renseignements susceptibles d'être perçus comme sensibles exigeront un consentement explicite de la personne intéressée, alors que pour les renseignements moins sensibles, un consentement implicite sera généralement suffisant[181]. Enfin, le troisième principe permet à une personne de « retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable »[182].

Comme nous l'avons mentionné, l'article 7 de la Loi énumère les circonstances dans lesquelles il est possible de collecter, d'utiliser et de communiquer des renseignements personnels à l'insu de la personne concernée et sans son consentement. Parmi les dispositions qui figurent à l'article 7, certaines nous intéressent particulièrement aux fins de ce travail. Entre autres, on prévoit que la collecte de renseignements personnels ne nécessite pas de consentement lorsqu'elle est « manifestement dans l'intérêt de l'intéressé », mais que son consentement ne peut être obtenu en temps opportun[183], lorsqu'elle est faite uniquement à des fins journalistiques, artistiques ou littéraires[184], ou lorsqu'il s'agit d'un renseignement réglementaire accessible au public[185].

---

[177] *Ibid*., ann. 1, art. 4.3.2.
[178] *Ibid*., ann. 1, art. 4.3.3.
[179] *Ibid*., ann. 1, art. 4.3.4.
[180] *Ibid*., ann. 1, art. 4.3.5.
[181] *Ibid*., ann. 1, art. 4.3.6.
[182] *Ibid*., ann. 1, art. 4.3.8.
[183] *Ibid*., art. 7(1)a).
[184] *Ibid*., art. 7(1)c).
[185] *Ibid*., art. 7(1)d).

Les aliénas 7(2)c) et 7(3)f) de la LPRPDÉ prévoient respectivement que l'utilisation ou la communication d'un renseignement ne nécessitent pas le consentement de l'intéressé si ce renseignement est utilisé ou communiqué à des fins statistiques, d'études ou de recherches érudites, ces fins ne peuvent être réalisées sans que le renseignement soit utilisé ou communiqué, celui-ci est utilisé ou communiqué d'une manière qui en assure le caractère confidentiel, le consentement est pratiquement impossible à obtenir et l'organisation informe le commissaire de l'utilisation avant de la faire. Ainsi, bien que le gouvernement canadien ait voulu accorder une certaine ouverture aux organisations qui collectent et partagent des renseignements personnels, cette ouverture est néanmoins limitée à quelques circonstances très précises.

D'autres dispositions ayant une portée plus large figurent aussi à l'annexe 1 de la LPRPDÉ. Le quatrième principe du Code impose des limites quant à la collecte des renseignements personnels[186]. Ce principe introduit les deux notions importantes de nécessité et d'honnêteté. L'article 4.4.1 défend aux organisations de recueillir arbitrairement des renseignements et exige que celles-ci restreignent la quantité et la nature des renseignements collectés « à ce qui est nécessaire pour réaliser les fins déterminées ». L'article 4.4.2 exige que toute collecte de renseignements doive se faire de manière honnête et licite dans le but explicite d'empêcher toute tentative par une organisation de tromper ou de les induire en erreur les gens.

Le cinquième principe pour sa part impose des limites à l'utilisation, la communication et la conservation des renseignements. L'article 4.5 énonce que, sans le consentement de la personne concernée, tous renseignements ne doivent pas être utilisés ou communiqués à des fins autres que celles établies au moment de la collecte. De plus, les organisations ne doivent conserver les renseignements personnels « qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées ». Il est intéressant de noter que l'article 4.5.3, qui indique que les organisations devraient détruire, effacer ou dépersonnaliser les renseignements personnels lorsqu'ils en ont plus besoins pour les fins déterminées, semble être formulé de manière non contraignante.

[186] *Ibid*., ann. 1, art. 4.4.

Les sixième et septième principes imposent respectivement des obligations quant à l'exactitude des renseignements[187] ainsi qu'aux mesures de sécurité qui doivent être établies pour les protéger[188]. Le huitième principe, qui porte sur la transparence, établi que les organisations doivent assurer la disponibilité de renseignements précis concernant leurs politiques et leurs pratiques de gestion des renseignements personnels, que l'obtention cette information ne doit pas nécessiter d'efforts déraisonnables et que ces renseignements doivent être fournis sous une forme compréhensible.

Le neuvième principe, sur l'accès aux renseignements personnels, impose à toute organisation l'obligation d'informer une personne, à la demande de celui-ci, de l'existence de tous renseignements personnels à son sujet qu'elle a en sa possession, ainsi que l'usage qui en est fait et du fait qu'ils ont été communiqués à une tierce partie. Le paragraphe 8(1) de la LPRPDÉ établit que cette demande doit se faire par écrit. À la réception d'une telle demande, l'organisation doit accorder à cette personne l'accès à ces renseignements, sauf si le dévoilement de ces renseignements révélerait un renseignement personnel sur un tiers[189]. Il peut par la suite contester l'exactitude de ces renseignements et demander à ce que toute correction nécessaire soit apportée. Finalement, le dixième principe établit la possibilité de porter plainte en cas de non-respect des principes du Code.

---

[187] Dans *Nammo c. TransUnion of Canada Inc*., [2010] A.C.F. no 1510, 2010 CF 1284, par. 39 [*Nammo*]**,** la Cour fédérale précise que, selon le principe 4.6.1 de la Loi, « les renseignements personnels ne doivent pas nécessairement être complètement exacts, complets et à jour. La Loi exige plutôt que les renseignements personnels soient aussi exacts, complets et à jour « que l'exigent les fins auxquelles ils sont destinés ». Par conséquent, c'est à la lumière de la fin à laquelle les renseignements sont destinés qu'il faut décider si les renseignements sont exacts, complets et à jour ».

[188] Bien que la question de la sécurité des renseignements personnels conservés par des organisations du secteur privée ne soit pas abordée en profondeur dans ce travail, elle demeure néanmoins un enjeu important. À titre d'exemple, en 2008, la société américaine TJX, Inc. a dû payer des dommages de 24 million de dollars après que des hackers se soient infiltrés dans le système informatique de l'entreprise pour y voler plus de 94 million de numéros de cartes de crédit et de débit de clients de TJX. Plus récemment, la société japonaise Sony a également été la cible de hackers qui ont infiltré le système de jeu en ligne PlayStation pour avoir accès à des renseignements sur plus de 77 million de joueurs. Voir Nick Bilton et Brian Stelter, « Sony Says PlayStation Hacker Got Personal Data » (26 avril 2011), *New York Times*, en ligne : nytimes.com <http://www.nytimes.com/2011/04/27/technology/27playstation.html>; John T. Soma, J. Zachary Courson et John Cadkin, « Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets » (2008-2009) 15 Rich. J.L. & Tech. 1, à la p. 13; Bergert, « Balancing Consumer Privacy », *supra* note 38 à la p. 37.

[189] LPRPDÉ, par. 9(1). Toutefois, le paragraphe 9(2) indique que cette limitation ne s'applique pas si le tiers consent à la communication à l'intéressé, ou si l'information est nécessaire parce que la vie, la santé ou la sécurité d'un individu est en danger.

Cependant, plusieurs des organisations qui collectent et utilisent des renseignements personnels au Canada sont en réalité basées dans des pays étrangers. Dans l'ensemble, la LPRPDÉ a effet sur toutes les pratiques de collecte, d'utilisation ou de communication de renseignements personnels ayant lieu sur le territoire canadien[190]. Toutefois, le caractère contraignant de la LPRPDÉ sur les organisations étrangères n'est pas assuré par la Loi elle-même, mais plutôt par une série d'accords internationaux visant la protection de la vie privée dans la circulation transfrontalière des renseignements personnels. De manière plus générale, les *Lignes directrices*[191] de l'OCDE, complétées par la *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée*[192] de 2007, forment la base d'une grande part de la coopération internationale à ce sujet[193]. Aussi, le Canada est un participant à l'initiative de la Coopération économique Asie-Pacifique (APEC) relativement à l'application transfrontalière des lois en matière de protection des renseignements personnels[194], en plus de prendre part à un certain nombre de résolutions et de projets internationaux[195]. Aux États-Unis, d'où proviennent plusieurs des organisations qui collectent et utilisent des renseignements personnels de Canadiens, le gouvernement a adopté en 2006 le *US SAFE WEB Act*[196], qui assure la coopération du FTC et des autres autorités pertinentes pour assisté dans la tenue d'enquêtes sur les pratiques d'organisations situées sur le territoire américain[197].

---

[190] CPVP, « Lignes directrices sur le traitement transfrontalier des données personnelles » (janvier 2009), en ligne : <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.cfm>.

[191] OCDE, *Lignes directrices*, *supra* note 150.

[192] OCDE, *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée* (2007), en ligne : <http://www.oecd.org/dataoecd/12/48/38876531.pdf>, visant à traduire « l'engagement des gouvernements à améliorer leurs cadres nationaux pour l'application des législations sur la vie privée afin de mieux permettre à leurs autorités de coopérer avec des autorités étrangères, et à se prêter mutuellement assistance dans l'application des législations protégeant la vie privée ».

[193] CPVP, Rapport « Profilage », *supra* note 2 à la p. 45.

[194] Voir *ibid*. à la p. 46 : « L'entente établit un processus dans le cadre duquel les autorités participantes peuvent demander de l'aide pour la collecte d'éléments de preuve, l'échange de renseignements sur une organisation ou une question faisant l'objet d'une enquête, la prise de mesures et le transfert de plaintes à une autre administration ».

[195] Le Canada prend notamment part à la Conférence annuelle des Commissaires à la protection des données et de la vie privée, est membre du Global Privacy Enforcement Network (GPEN), et participe avec l'Organisation internationale de la normalisation (ISO) sur des questions portant sur la protection des renseignements personnels. Voir *ibid*.

[196] *US SAFE WEB Act*, 12 U.S.C. § 3412 (2006).

[197] Voir É.-U., FTC, « Summary of the US SAFE WEB Act », en ligne : ftc.gov <http://www.ftc.gov/reports/ussafeweb/Summary%20of%20US%20SAFE%20WEB%20Act.pdf>. Voir aussi FTC, « Protecting Consumer Privacy », *supra* note 1 à la p. 17.

2.2.3. Survol des lois provinciales

À ce jour, trois provinces canadiennes ont adopté une loi considérée comme étant essentiellement similaire à la LPRPDÉ[198]. Avant même que le gouvernement fédéral canadien ne prenne l'initiative de mettre sur pied un cadre législatif visant la protection des renseignements personnels collectés, utilisés ou communiqués par des organisations du secteur privé, la province du Québec adopta en 1993 la *Loi sur la protection des renseignements personnels dans le secteur privé*[199]. Pour leur part, les provinces de l'Alberta et la Colombie-Britannique ont chacune adopté en 2003 leur version du *Personal Information Privacy Act* (PIPA)[200].

Comme on pourrait s'y attendre, les dispositions de ces trois lois provinciales s'apparentent de manière globale à celles que l'on retrouve dans la LPRPDÉ. L'objet de la Loi albertaine[201] et celui de la Loi britanno-colombienne[202], dont les formulations sont pratiquement identiques, reprennent essentiellement les grandes lignes de l'objet de la LPRPDÉ. Pour sa part, la Loi québécoise, qui se fixe aussi l'objet général d'établir des règles particulières quant à la collecte, la conservation, l'utilisation et la communication des renseignements personnels dans le cadre de l'exploitation d'une entreprise, exclut cependant la mention d'équilibre contenu dans les objets des deux autres lois provinciales ainsi que la loi fédérale. Comme il est précisé dans son objet, cette loi vise à compléter les droits en matière de protection des renseignements personnels prévus aux articles 35 à 40 du *Code civil du Québec*[203], ces dernières qui renvoient au droit plus général de toute personne au

---

[198] Les lois provinciales essentiellement similaires à la LPRPDÉ peuvent avoir préséance sur celle-ci aux termes de l'aliéna 26(2)b) de la LPRPDÉ, qui indique que le gouverneur en conseil peut, par décret : « s'il est convaincu qu'une loi provinciale essentiellement similaire à la présente partie s'applique à une organisation – ou catégorie d'organisations – ou à une activité – ou catégorie d'activités –, exclure l'organisation, l'activité ou la catégorie de l'application de la présente partie à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels qui s'effectue à l'intérieur de la province en cause ».
[199] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1 [Loi Qc.].
[200] Alberta : *Personal Information Protection Act*, S.A. 2003, c. P-6.5 [PIPA Alta.] ; Colombie-Britannique : *Personal Information Protection Act*, S.B.C. 2003, c. 63 [PIPA C.-B.].
[201] PIPA Alta., *ibid*. art. 3.
[202] PIPA C.-B., *supra* note 200 art. 2.
[203] *Code civil du Québec*, L.Q., 1991, c. 64.

respect de sa vie privée prévu à l'article 5 de la *Charte des droits et libertés de la personne*[204] du Québec.

Sur le plan de la mise en application générale, la Loi du Québec, de manière similaire à la LPRPDÉ[205], impose aux entreprises l'obligation de déterminer l'objet pour lequel les renseignements personnels d'autrui sont collectés et de restreindre la collecte aux fins nécessaires à cet objet[206]. Dans ce contexte, les tribunaux québécois ont interprété l'expression « fins nécessaires » comme signifiant les fins indispensables[207]. Une telle formulation ne figure toutefois pas dans les lois des deux provinces de l'Ouest, qui imposent plutôt aux organisations l'obligation, de façon similaire à la LPRPDÉ, de développer et de mettre en œuvre des politiques et des pratiques raisonnables pour permettre le respect des dispositions figurant dans ces lois[208].

Les trois lois provinciales accordent également, comme la Loi fédérale, une importance significative à l'obtention d'un consentement informé et volontaire de la part de l'intéressé lors de l'utilisation ou la communication de ses renseignements personnels[209], en plus d'interdire aux organisations d'exiger le consentement d'un individu en échange d'un service[210]. Concernant ce dernier principe, la Loi du Québec impose un fardeau supplémentaire aux organisations en stipulant qu'en cas de doute sur la légitimité des moyens utilisés pour obtenir un consentement, les renseignements collectés seront jugés non nécessaires[211].

---

[204] *Charte des droits et libertés de la personne*, L.R.Q., c. C-12.
[205] LPRPDÉ, *supra* note 8 ann. 1, art. 4.2, 4.2.2.
[206] Loi Qc., *supra* note 199 art. 4-5.
[207] *X. v. Le Groupe Jean-Coutu (PJC) inc.*, J.E. 2000AC-63 (C.Q.). Voir McIsaac et al., *Law of Privacy*, *supra* note 158 à la p. 4-101.
[208] PIPA Alta., *supra* note 200 art. 6(1); PIPA C.-B., *supra* note 200 art. 5; LPRPDÉ, *supra* note 8 ann. 1, art. 4.1.4.
[209] La Loi québécoise, contrairement aux lois de l'Alberta et de la Colombie-Britannique, ne contient pas de disposition explicite relativement à l'obtention du consentement lors de la collecte initiale des renseignements personnels. La Loi du Québec prévoit plutôt une obligation d'information de la collecte, un droit de refus à l'intéressé et un principe de nécessité pour les renseignements collectés. Voir Philippa Lawson et Mary O'Donoghue, « Approaches to Consent in Canadian Data Protection Law » dans Ian Kerr, Valerie Steeves et Carole Lucock, dir., *Lessons From the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, New York, Oxford University Press, 2009, 21, à la p. 34 [Lawson et O'Donoghue, « Approaches to Consent »].
[210] PIPA Alta., *supra* note 200 art. 7(2); PIPA C.-B., *supra* note 200 art. 7(2); Loi Qc., *supra* note 199 art. 9.
[211] Loi Qc., *supra* note 199 art. 9.

Toujours au sujet de la validité du consentement, les lois de l'Alberta et de la Colombie-Britannique énoncent toutes deux que tout consentement obtenu de manière malhonnête, soit à l'aide de pratiques trompeuses ou en procurant de la fausse information quant à la collecte, l'utilisation ou la communication des renseignements personnels, sera jugé invalide[212]. Bien qu'à cet effet, la Loi québécoise ne contienne aucune disposition explicite, elle mentionne toutefois qu'un consentement n'a effet que s'il est manifeste, libre, éclairé et donné qu'à des fins spécifiques[213]. De surcroît, les trois lois provinciales exigent, sous réserve de certaines exceptions, un consentement additionnel pour la collecte, l'utilisation et la communication de renseignements personnels à des fins autres que celles prévues au moment de la collecte[214].

Chacune des trois lois provinciales place également un accent sur l'obligation des organisations d'informer la personne concernée de l'utilisation qui sera faite des renseignements personnels collectés à son sujet, et ce, avant ou au moment de la collecte[215]. À ce sujet, les trois provinces ont adopté une approche bien plus contraignante que celle qui figure à la LPRPDÉ. En effet, la loi fédérale indique plutôt que les organisations doivent faire un « effort raisonnable » pour s'assurer que la personne intéressée est informée des fins auxquelles serviront ses renseignements personnels[216].

La Loi québécoise comporte certaines dispositions qui touchent plus directement le sujet du présent travail. Au moment de l'élaboration de la Loi, l'industrie du marketing direct, soucieuse des conséquences de l'adoption d'une telle mesure législative sur leur industrie, a eu plusieurs consultations avec le gouvernement du Québec[217]. Comme résultat, la Loi québécoise contient certaines dispositions qui adressent la nécessité d'établir un certain équilibre entre les pratiques de l'industrie et le droit à la vie privée des individus. À cet effet, l'article 22 de la Loi permet aux entreprises de communiquer à un tiers, à des fins

[212] PIPA C.-B., *supra* note 200 art. 10; PIPA Alta., *supra* note 200 art. 7(3).
[213] Loi Qc., *supra* note 199 art. 14.
[214] Loi Qc., *supra* note 199 art. 12-14, 18; PIPA Alta., *supra* note 200 art. 8(4), 17, 20; PIPA C.-B., *supra* note 200 art. 8(4), 15(1), 18(1).
[215] Loi Qc., *supra* note 199 art. 8; PIPA Alta., *supra* note 200 art. 13; PIPA C.-B., *supra* note 200 art. 10.
[216] LPRPDÉ, *supra* note 8 ann. 1, art. 4.3.2.
[217] McIsaac et al., *Law of Privacy*, *supra* note 158 à la p. 4-105.

de prospection commerciale ou philanthropique, une liste nominative de ses clients ou des renseignements permettant la création d'une telle liste, et ce, sans le consentement des personnes concernées. Au sens de la Loi, une liste nominative « est une liste de noms, de numéros de téléphone, d'adresses géographiques de personnes physiques ou d'adresses technologiques où une personne physique peut recevoir communication d'un document ou d'un renseignement technologique ». Les articles 23 à 26 de la Loi québécoise établissent cependant le droit des personnes concernées de demander le retrait de leurs renseignements personnels figurant sur une telle liste.

2.2.4. Les commissariats à la protection de la vie privée

Au Canada et dans les provinces dotées d'une loi sur la protection des renseignements personnels, ce sont les commissaires à la vie privée qui ont le rôle principal d'assurer le respect de la vie privée des individus. À l'échelle du pays, ce rôle est garanti par le Commissariat à la protection de la vie privée du Canada (CPVP), qui fut institué par l'adoption de la *Loi sur la protection des renseignements personnels* en 1983. Alors que le mandat initial du CPVP consistait à veiller uniquement sur les pratiques de traitement des renseignements personnels employées par les ministères et organismes fédéraux, depuis le 1er janvier 2001, son rôle s'étend également aux organisations du secteur privé visé par la LPRPDÉ.

Les pouvoirs conférés au CPVP par l'article 12 de la LPRPDÉ lui commandent de faire l'examen de toute plainte[218], qu'elle soit formulée par tout intéressé en vertu du paragraphe 11(1) de la LPRPDÉ, ou par l'initiative même du Commissariat en vertu du paragraphe 11(2) de la même loi. Parmi les pouvoirs qui lui sont conférés, le CPVP a le pouvoir d'assigner et de contraindre des témoins à comparaître devant lui, de faire prêter serment, de recevoir des éléments de preuve indépendamment de leur admissibilité devant les tribunaux, de visiter tout local autre qu'une maison d'habitation occupée par l'organisation en cause, de s'entretenir en privé avec les personnes dans ce local et d'y mener les enquêtes nécessaires, et d'examiner les documents utiles à l'examen de la plainte

[218] LPRPDÉ, *supra* note 8 art. 12(1).

se trouvant dans ce local[219]. La loi stipule également que le CPVP peut avoir recours à la médiation ou la conciliation afin de parvenir au règlement de la plainte[220]. À la suite de l'examen de la plainte, le commissaire doit dresser un rapport où il présente ses conclusions et ses recommandations, fait état des règlements entre les parties, et demande à l'organisation de donner avis des mesures prises ou envisagées pour la mise en œuvre des recommandations[221].

En plus du pouvoir d'examen des plaintes, l'article 18 de la LPRPDÉ accorde au Commissariat le pouvoir de procéder à la vérification des pratiques de gestion des renseignements personnels d'une organisation « s'il a des motifs raisonnables de croire que celle-ci a contrevenu à l'une des dispositions de la section 1 ou n'a pas mis en œuvre une recommandation énoncée dans l'annexe 1 »[222]. L'étendue des pouvoirs de vérification du Commissariat est en tous points identique à l'étendue des pouvoirs d'examen des plaintes[223]. Mais, bien que le commissaire à la protection de la vie privée dispose d'une gamme de pouvoirs pour assurer le respect de la vie privée des Canadiens, l'article 20 de la LPRPDÉ interdit la divulgation de tout renseignement obtenu lors de l'exercice de ses fonctions, incluant notamment le nom des organisations sujettes à une enquête du commissaire. Cette limitation comporte cependant certaines exceptions, particulièrement dans les cas où le commissaire juge qu'il est dans l'intérêt public de dévoiler des détails sur les pratiques d'une organisation en matière de gestion des renseignements personnels[224].

Or, la LPRPDÉ permet également au CPVP de porter lui-même une plainte « s'il a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question relative à l'application de la [première partie de la Loi] »[225]. À la suite du dépôt du rapport d'enquête du CPVP, un plaignant peut faire une demande devant la Cour fédérale pour que celle-ci entende toute question qui a fait l'objet de la plainte ou qui est mentionnée dans le rapport du

[219] *Ibid*., art. 12(1)a)-f).
[220] *Ibid*., art. 12(2).
[221] *Ibid*., art. 13(1)a)-c).
[222] *Ibid*., art. 18(1).
[223] *Ibid*., art. 18(1)a)- f).
[224] *Ibid*., art. 20(2).
[225] *Ibid*., art. 11(2).

Commissaire[226]. Ce recours est aussi applicable dans cas où le CPVP à lui-même pris l'initiative d'une plaine[227].

À propos des provinces canadiennes, tant en Colombie-Britannique qu'en Alberta, le rôle de commissaire est assuré par l'*Information and Privacy Commissioner*, dont les pouvoirs sont attribués par les lois sur l'accès à l'information respectives aux deux provinces[228]. Similairement, c'est la Commission d'accès à l'information, habilitée par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[229], qui assure le rôle de commissaire à la vie privée dans la province du Québec[230]. Dans l'ensemble, les pouvoirs des commissaires provinciaux sont en plusieurs points similaires à ceux du CPVP. Leurs rôles consistent donc à veiller au respect des lois en matière de protection des renseignements personnels, à recevoir des plaintes à ce sujet et à effectuer des enquêtes en cas de plainte[231]. Or, contrairement au CPVP, les lois provinciales sur la protection des renseignements personnels de l'Alberta et du Québec ne spécifient pas que les commissaires disposent du pouvoir de porter eux-mêmes une plainte, alors que la loi de la Colombie-Britannique ne fait qu'indiquer que, peu importe si une plainte a été déposée ou non, le commissaire doit mener une enquête lorsqu'il suspecte la présence d'une violation de la loi[232]. Par contre, les commissaires provinciaux sont dotés du pouvoir de faire des ordonnances à des organisations afin que celles-ci se conforment aux dispositions de leurs

---

[226] *Ibid*., art. 14(1).
[227] *Ibid*., art. 14(3). Il est important de noter que les tribunaux ont à maintes reprises confirmé que les plaintes portées devant la Cour en vertu de l'article 14 ne sont pas des demandes de contrôle juridique visant l'examen des rapports ou des recommandations du CPVP, mais qu'elles constituent des requêtes *de novo* qui accordent un plein pouvoir discrétionnaire à la Cour. Voir *Eastmond*, *supra* note 128 par. 118; *Englander*, *supra* note 145 par. 48; *Morgan*, *supra* note 167 par. 16-17; *Nammo*, *supra* note 187 par. 28.
[228] Alberta: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25 ; Colombie-Britannique : *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165. Voir McIsaac et al., *Law of Privacy*, *supra* note 158 aux pp. 4-72.5 et 4-89.
[229] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1.
[230] Loi Qc., *supra* note 199 art. 41.1.
[231] PIPA Alta., *supra* note 200 art. 36-38; PIPA C.-B., *supra* note 200 art. 36-38; Loi Qc., *supra* note 199 art. 42-53.
[232] PIPA C.-B., *supra* note 200 art. 36(1)a). Aussi, contrairement à l'application de l'article 14 de la LPRPDÉ, les décisions des commissaires provinciaux sont susceptibles d'un contrôle judiciaire, et non d'un procès *de novo* : PIPA Alta., *supra* note 200 art. 54.1(1); PIPA C.-B., *supra* note 200 art. 53; Loi Qc., *supra* note 199 art. 61-69.

lois respectives[233], alors que le CPVPC, dont le rôle est plutôt similaire à celui d'un ombudsman, ne possède pas de tels pouvoirs en vertu de la LPRPDÉ[234].

[233] PIPA Alta, *supra* note 200 art. 52; PIPA C.-B., *supra* note 200 art. 52; Loi Qc., *supra* note 199 art. 55.

[234] Voir Christopher Berzins, « Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building » (2002) 27 Queen's L.J. 609, à la p. 640, où l'auteur préconise la création d'un tribunal de la protection de la vie privée pour contrer les lacunes du rôle d'ombudsman du CPVP. Voir aussi CPVPC, « Examen, prévu par la loi, de la Loi sur les renseignements personnels et les documents électroniques. Aperçu de la consultation du CPVP » (27 novembre 2006), en ligne : <http://www.priv.gc.ca/parl/2006/sub_061127_f.cfm#003>.

CHAPITRE 3 – L'APPLICATION DU DROIT EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE CONTEXTE DU PROFILAGE

Nous avons vu qu'au Canada, les individus disposent d'un certain nombre d'outils permettant d'assurer que leur vie privée soit suffisamment protégée contre les pratiques qui consistent à compiler et analyser les renseignements personnels collectés à partir de l'utilisation d'Internet ou d'autres technologies d'information et de communication. Malgré cela, certaines organisations parviennent à créer des dossiers numériques fortement détaillés portant sur tous les aspects de la vie de consommateurs, et ce, par la simple collecte des fragments d'information que ces derniers laissent derrière eux, parfois de façon volontaire, mais parfois à leur insu. Devant ce constat, devons-nous supposer que les protections législatives et juridiques canadiennes en matière de vie privée et de protection des renseignements personnels sont, tout compte fait, insuffisantes, voir inefficaces, pour contrer les effets indésirables de ces pratiques? À cet égard, nous discuterons dans le présent chapitre de trois aspects centraux aux différentes lois sur la protection des renseignements personnels au Canada qui nécessitent une attention particulière dans le contexte du profilage comportemental : soit la nature des renseignements, les fins acceptables, ainsi que le consentement.

3.1. La nature des renseignements

3.1.1. L'interprétation législative des « renseignements personnels »

Comme nous l'avons déjà mentionné, lorsque nous les prenons individuellement, les différents fragments d'information recueillis à notre sujet au quotidien ne dévoilent ordinairement que très peu de choses à notre sujet. Mais, en compilant dans un tout les nombreux fragments d'information recueillis à propos d'un individu, on peut bien souvent obtenir une image fortement révélatrice de ce dernier[235]. En d'autres mots, la nature des renseignements personnels qu'une organisation détient à propos d'un individu peut être

[235] Voir CPVP, Rapport « Profilage », *supra* note 2 à la p. 18. Voir aussi Solove, *Understanding*, *supra* note 2 à la p. 118; Arthur J. Cockfield, « The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government » (2003-2004) 1 U. Ottawa L. & Tech. J. 325, à la p. 336.

significativement transformée par les processus de couplage et d'analyse. Même si, dans leur forme initiale, les fragments d'information collectés sont d'une insignifiance totale ou qu'ils ne dévoilent rien de substantiel à propos d'un individu particulier, les données engendrées par les techniques de profilage commercial risquent néanmoins de dévoiler des renseignements plus précis, et parfois plus délicats, que les éléments individuels qui les constituent[236].

Malgré ce qui précède, la classification des renseignements compilés, fabriqués ou déduits à partir d'une multitude de données collectées par une organisation se situe dans une zone grise de la loi. De manière générale, les lois canadiennes en matière de protection des renseignements personnels dans le secteur privé ne spécifient pas la forme que doit prendre un renseignement pour être considéré « personnel »[237]. La définition offerte par la LPRPDÉ semble indiquer que tous les renseignements « concernant un individu identifiable » jouissent d'une certaine protection en tant que renseignement personnel[238]. Il en est de même pour les lois provinciales[239]. Dans tous les cas, cette protection passe avant tout par l'obligation pour les organisations d'obtenir un consentement de la part d'un individu pour toute collecte, utilisation ou divulgation des renseignements qui le concerne. Or, les renseignements qui sont traités et compilés dans des profils comportementaux d'individus particuliers sont-ils des renseignements « personnels » au sens de la législation canadienne

---

[236] Voir CPVP, Rapport « Profilage », *ibid*., où le Commissariat à la protection de la vie privée du Canada a récemment indiqué que : « [g]râce aux outils de plus en plus puissants de forage de données, il est possible de dresser le portrait complet d'une personne à partir de ce qu'elle écrit sur elle-même et les autres sur des sites de réseautage social, à partir des capacités de cartographie qui nous montrent, à nous et aux autres, où et comment nous vivons, à partir des contacts avec nos amis, de même qu'à partir du lien qui peut être fait entre nos préférences, les endroits où nous nous trouvons ainsi que l'utilisation que nous faisons de nos biens ».

[237] Scassa, « Geographical », *supra* note 121 à la p. 190.

[238] LPRPDÉ, *supra* note 8 art. 2(1). Voir Lisa M. Austin, « Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices » (2006-2007) 44 Can. Bus. L.J. 21, à la p. 34.

[239] Alta PIPA, *supra* note 200 art. 1(1)k) : « personal information » means information about an identifiable individual; C.-B. PIPA, *supra* note 200 art. 1 : « personal information » means information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information; Loi Qc., *supra* note 199 art. 2 : « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier ». Aussi l'article 1 de la loi québécoise spécifie qu'elle « s'applique à ces renseignements quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles: écrite, graphique, sonore, visuelle, informatisée ou autre. Elle s'applique aussi aux renseignements personnels détenus par un ordre professionnel dans la mesure prévue par le Code des professions (chapitre C-26). La présente loi ne s'applique pas à la collecte, la détention, l'utilisation ou la communication de matériel journalistique, historique ou généalogique à une fin d'information légitime du public ».

en matière de vie privée, de manière à ce que leur collecte, utilisation ou communication par des organisations nécessitent l'obtention du consentement de l'intéressé?

Les tribunaux canadiens ont interprété de façon assez large la définition de « renseignement personnel » telle qu'elle figure dans le libellé des lois sur la protection des renseignements personnels[240]. La Cour suprême du Canada dans l'affaire *Dagg* a spécifié que la définition de « renseignement personnel », tel qu'elle figure à la LPRP, doit être interprétée de façon large afin d'assurer une protection suffisante aux individus[241]. Dans l'affaire *Rousseau c. Wyndowe*, le juge Teitelbaum de la Cour fédérale avance que la portée de la définition de « renseignement personnel » de la LPRPDÉ est encore plus large que celle de la LPRP[242]. Il rajoute que « l'élément essentiel de la définition de "renseignement personnel" dans la LPRPDÉ est que l'individu doit être identifiable, de sorte que les renseignements véritablement anonymes ne sont pas des renseignements personnels »[243].

Pour mieux nous éclairer à ce sujet, il est utile d'établir certains parallèles avec la jurisprudence traitant de l'interprétation des « renseignements personnels » sous les lois sur l'accès à l'information[244]. À cet égard, la Cour d'appel fédérale dans l'affaire *Canada (Commissaire à l'information) c. Canada (Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports)*[245], une décision portant sur la *Loi sur l'accès à l'information* fédérale[246]. Dans cette affaire, le juge Desjardins avance que :

---

[240] *Rousseau*, *supra* note 166. Voir Scassa, « Geographical », *supra* note 121 à la p. 191.

[241] *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403, par. 69 [*Dagg*] : « Comme l'a souligné le juge en chef adjoint Jerome dans *Canada (Commissaire à l'information) c. Canada (Solliciteur général)*, [...] la formulation de cet article est « délibérément large » et « illustre tout à fait les efforts considérables qui ont été déployés pour protéger l'identité des individus ». Elle semble destinée à viser tout renseignement sur une personne donnée, sous la seule réserve d'exceptions précises. »

[242] *Rousseau*, *supra* note 166 par. 29, où le juge Teitelbaum indique que cette affaire est la première à traiter de la question des renseignements personnels selon la LPRPDÉ.

[243] *Ibid*., par. 31.

[244] Dans *Dagg*, *supra* note 241 par. 45, 55-57, la Cour suprême du Canada indique que la LPRP et *Loi sur l'accès à l'information*, L.R.C. (1985), c. A-1 [LAI féd.] forment ensemble un « code homogène ». Voir aussi *Canada (Commissaire à l'information) c. Canada (GRC)*, 2003 CSC 8, [2003] 1 R.C.S. 66, par. 21-22; *Compagnie H. J. Heinz du Canada Ltée c. Canada (Procureur général)*, 2006 CSC 13, par. 2, 22 et 25; *Canada (Commissaire à l'information) c. Canada (Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports)*, [2006] A.C.F. no 704, 2006 CAF 157, par 35 [Arrêt *Transport*].

[245] Arrêt *Transport*, *ibid.*

[246] LAI féd., *supra* note 244.

> **[...]** les renseignements, quels que soient leur forme et leur support, sont pertinents s'il s'agit de renseignements « concernant » un individu et s'ils permettent d'identifier l'individu ou rendent possible son identification. Il existe des précédents selon lesquels un individu « identifiable » est une personne dont il est raisonnable de croire qu'elle pourra être identifiée à l'aide des renseignements en cause s'ils sont combinés avec des renseignements d'autres sources.[247]

On remarque de cette citation de la Cour d'appel fédérale que pour qualifier un renseignement de « renseignement personnel », il doit d'abord s'agir d'un renseignement « concernant » un individu, et cet individu doit être « identifiable »[248].

D'abord, pour déterminer si un renseignement quelconque est un renseignement « concernant » un individu, il faut que celui-ci concerne principalement une personne elle-même[249]. Comme l'indique le juge Desjardins dans l'arrêt *Transport*, un tel renseignement doit porter sur des sujets « qui font intervenir le droit de l'individu à sa vie privée »[250], donc qui intègre les notions « d'intimité, d'identité, de dignité et d'intégrité de l'individu »[251]. En ce qui concerne la détermination des renseignements « concernant » un individu identifiable issus des activités du secteur privé, le CPVP a notamment conclu que, selon la LPRPDÉ, les relevés de vente attribués à une employée afin de comparer son rendement au travail à celui de ses collègues « constituent des renseignements la concernant en tant qu'individu identifiable »[252]. Aussi, le CPVP a déterminé que la prise de photographies d'appartements de locataires sans leur consentement aux fins d'assurance est une information concernant un individu identifiable et constitue des renseignements personnels en vertu de la LPRPDÉ[253]. À la lumière de ces faits, il est difficile d'imaginer un contexte dans lequel un renseignement

---

[247] Arrêt *Transport*, *supra* note 244 par. 43.
[248] Scassa, « Geographical », *supra* note 121 à la p. 191.
[249] Voir *Dagg*, *supra* note 241 par. 94, où la majorité de la Cour suprême du Canada a conclu que « les renseignements qui concernent principalement des personnes elles-mêmes ou la manière dont elles choisissent d'accomplir les tâches qui leur sont confiées sont des « renseignements personnels » ».
[250] Arrêt *Transport*, *supra* note 244 par. 53.
[251] *Ibid*. par. 52.
[252] CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2003-207, « Une entreprise de téléphones cellulaires satisfait aux conditions rattachées au consentement négatif », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030806_02_f.cfm>.
[253] CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2006-349, « Prise de photographies d'appartements de locataires sans leur consentement pour fins d'assurance », en ligne : <http://www.priv.gc.ca/cf-dc/2006/349_20060824_f.cfm>.

collecté à partir du suivi des activités d'un individu particulier sur le Web et compilé dans un profil comportemental pour ensuite être utilisé dans le but de transmettre de la publicité ciblée à cet individu ne serait pas un renseignement « concernant » ce dernier.

Or, dans le récent arrêt *Leon's Furniture Ltd. v. Alberta (Information and Privacy Commissioner)*[254], la Cour d'appel de l'Alberta a conclu que la collecte par l'appelant de numéros de plaques d'immatriculation des véhicules de ses clients dans le but d'éviter la fraude était raisonnable puisque ces renseignements ne sont pas « personnels » au sens de la loi albertaine en matière de protection des renseignements personnels dans le secteur privé[255]. Pour la Cour, puisque la loi précise qu'un renseignement personnel doit concerner un individu identifiable, elle exclut de sa définition tous renseignements génériques et statistiques, ainsi que tous renseignements portant sur un objet ou une propriété[256]. De plus, elle estime que tout renseignement personnel doit se rapporter directement à un individu, de sorte que les renseignements indirects ou collatéraux ne sont pas des renseignements personnels. Pour sa part, la juge Conrad en dissidence supporte plutôt l'opinion formulée par le commissariat à l'information et à la vie privée de l'Alberta selon laquelle les plaques d'immatriculation sont non seulement des renseignements concernant un objet, mais aussi des renseignements concernant un individu. Comme elle l'indique, l'information que peut dévoiler une plaque d'immatriculation ne se limite pas à des renseignements sur le véhicule puisqu'en entrant ce renseignement dans une base de données appropriée, il est relativement facile d'avoir accès à une multitude de renseignements portant sur un individu particulier[257].

Ensuite, pour déterminer le test approprié pour établir si un renseignement concerne un individu « identifiable », on retrouve dans la jurisprudence canadienne deux approches élaborées par les tribunaux. On retrouve la première dans *Ontario (Attorney General) v.*

---

[254] *Leon's Furniture Ltd. v. Alberta (Information and Privacy Commissioner)*, [2011] A.J. No. 338, 2011 ABCA 94 [*Leon's Furniture*].
[255] PIPA Alta., *supra* note 200.
[256] *Leon's Furniture*, *supra* note 254 par. 47. Il est aussi intéressant de noter dans cette affaire que la majorité de la Cour d'appel de l'Alberta soutient que la loi s'intéresse davantage à la protection des renseignements dans le cadre de transactions commerciales ou financières qu'aux renseignements concernant les choix, les opinions et le statut d'un individu.
[257] *Ibid*., par. 119. À noter que la Cour suprême du Canada entendra l'appel de cette décision : *Alberta (Information and Privacy Commissioner) c. Leon's Furniture Ltd*., [2011] C.S.C.R. no 260.

Pascoe[258], une affaire de la Cour divisionnaire de l'Ontario et confirmée par la Cour d'appel de l'Ontario, qui porte sur la divulgation, en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* de l'Ontario[259], de dossiers relatifs à des procédures médicales effectuées par un médecin de la région de Toronto. Dans cette affaire, la Cour divisionnaire établit qu'un renseignement est considéré « personnel » s'il y a une attente raisonnable qu'un individu puisse être identifié par ce renseignement[260]. Bien que dans *Pascoe*, les renseignements divulgués ne comportaient pas le nom du médecin en question, la Cour a reconnu que les dossiers divulgués pouvaient en soi, ou par jumelage avec d'autres renseignements de sources multiples, permettre l'identification de l'individu même si celui-ci n'est pas nommé directement. La Cour précise également que ces sources peuvent inclure la connaissance individuelle de personnes familières avec les circonstances ou les événements inclus dans les dossiers[261].

Or, plus récemment, une deuxième approche a été formulée par la Cour fédérale dans l'affaire *Gordon c. Canada (Ministre de la Santé)*[262], concernant le refus par le ministre de la Santé de divulguer le champ « province » dans la base de données du Système canadien d'information sur les effets indésirables des médicaments CADRIS (*Canadian Adverse Drug Reaction Information System*) suite à une demande d'accès à l'information effectué par le demandeur en vertu de la *Loi sur l'accès à l'information*[263] du Canada. Pour déterminer si l'information du champ « province » pouvait effectivement dévoiler l'identité d'individus

---

[258] *Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner)*, [2001] O.J. No. 4987, 154 O.A.C. 97, (*sub nom. Ontario (Attorney General) v. Pascoe*) 2001 CanLII 32755, conf. par *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300, 166 O.A.C. 88 [*Pascoe*].

[259] *Loi sur l'accès à l'information et la protection de la vie* privée, L.R.O. 1990, c. F.31, art. 2(1) : « renseignements personnels » Renseignements consignés ayant trait à un particulier qui peut être identifié.

[260] *Pascoe*, *supra* note 258 par. 14 : « While the records in question do not name the physician, it is common ground that the records may themselves, or in combination with other information, identify the individual even if he or she is not specifically named. The test is accepted as follows: If there is a reasonable expectation that the individual can be identified from the information, then such information qualifies under subs. 2(1) as personal information ».

[261] *Ibid*., par. 15.

[262] *Gordon c. Canada (Ministre de la Santé)*, [2008] A.C.F. no 331, 2008 CF 258 [*Gordon*].

[263] LAI féd., *supra* note 244. L'article 19 de la LAI féd. indique que tout « responsable d'une institution fédérale est tenu de refuser la communication de documents contenant les renseignements personnels visés à l'article 3 de la *Loi sur la protection des renseignements personnels* », sauf lorsque l'individu concerné a donné son consentement, lorsque le public a accès à ces renseignements, ou lorsque la communication est conforme aux exceptions établies par l'article 8 de la LPRP.

particuliers, le juge Gibson adopta le test proposé par le CPVP, agissant comme intervenant dans cette affaire. Pour le CPVP :

> [l]es renseignements seront des renseignements concernant un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources.[264]

Ainsi, le juge Gibson dans *Gordon* conclut que la divulgation du champ « province » augmenterait considérablement la possibilité que des renseignements « concernant un individu identifiable, quels qu'en soient la forme et le support » soient utilisés avec d'autres renseignements dans le but d'identifier des individus particuliers[265].

Bien que l'approche de « l'attente raisonnable » formulée dans *Pascoe* semble plus en harmonie avec la jurisprudence portant sur l'interprétation du droit à la vie privée sous l'article 8 de la *Charte*[266], le CPVP semble pour sa part favoriser l'approche de la « forte probabilité » de l'affaire *Gordon* en ce qui a trait aux recours intentés en vertu de la LPRPDÉ[267]. Dans une enquête récente portant sur l'utilisation d'une technique d'« ingénierie sociale »[268] pour obtenir des renseignements confidentiels, le CPVP a indiqué qu' :

> [i]l y avait effectivement une forte probabilité que Locatecell.com ou le journaliste (ou quiconque, finalement) auraient été en mesure de recouper suffisamment d'informations pour être éventuellement en mesure de découvrir l'identité du détenteur du BlackBerry, en communiquant avec

---

[264] *Gordon*, *supra* note 262 par. 34.
[265] *Ibid*., par. 43
[266] En effet, cette approche semble s'harmoniser avec le test développé par la Cour suprême dans *R. c. Edwards*, *supra* note 135, qui consiste à déterminer l'existence d'une attente subjective de vie privée qui doit être évaluée en fonction du caractère raisonnable de cette attente sur le plan objectif.
[267] Voir CPVP, « Interprétations de la LPRPDÉ », en ligne : <http://www.priv.gc.ca/leg_c/interpretations_02_f.cfm>, où le CPVP fait référence à l'affaire *Gordon* pour résumer l'interprétation des renseignements personnels par les tribunaux : « Un renseignement concerne un « individu identifiable » lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles ».
[268] CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2007-372, « Les communications aux courtiers en données exposent les faiblesses des mesures de sécurité en télécommunications », en ligne : <http://www.priv.gc.ca/cf-dc/2007/372_20070709_f.cfm> : « L'ingénierie sociale est un ensemble de techniques utilisées pour manipuler les gens et les amener à faire des choses ou à divulguer des renseignements confidentiels. L'obtention de renseignements personnels par faux-semblant, par exemple, consiste à créer et à utiliser un scénario afin d'obtenir des renseignements de la part d'une personne ciblée, habituellement au téléphone ».

> toutes les personnes figurant sur le relevé d'appels. Ainsi, le relevé d'appels, lorsque pris dans son ensemble dans le présent contexte, était de l'information sur une personne « identifiable ».[269] [Nous soulignons]

Or, comme l'indique la professeure Teresa Scassa, bien qu'on puisse prétendre que moins de renseignements seront considérés « personnels » sous le test de l'attente raisonnable que sous le test de la forte possibilité, il n'est pas clair que les seuils établis par chacune de ces approches sont substantiellement différents[270]. Dans le contexte du profilage en ligne et de la publicité comportemental, il semble justifié de prétendre que le test de l'attente raisonnable, bien que plus limité, est suffisant pour permettre de considérer les renseignements obtenus par profilage comme étant des renseignements personnels, puisque ces renseignements seront généralement couplés avec une gamme de renseignements portant sur le même individu. De plus, comme nous le verrons dans la prochaine sous-section, même les renseignements qui sont traités de manière anonyme ou à partir de sources accessibles au public permettent néanmoins la découverte de renseignements additionnels à propos d'un individu.

3.1.2. La transformation de l'information

Dans le contexte du profilage comportemental et de la publicité sur Internet, les renseignements qui sont collectés et utilisés par les organisations, notamment les moteurs de recherche et les réseaux sociaux en ligne, seront généralement retranscrits sous une forme anonymisée avant d'être communiqués à des tiers[271]. Si nous supposons que de tels renseignements ne sont véritablement communiqués que sous une forme anonyme[272], cela n'empêche pas que leur utilisation permet tout de même de découvrir des renseignements

[269] *Ibid*.
[270] Scassa, « Geographical », *supra* note 121 aux pp. 199-202.
[271] Voir Ohm, « Broken Promises », *supra* note 56 à la p. 1703.
[272] Bien que les renseignements communiqués à des tiers, tels les renseignements relatifs aux activités en ligne et aux requêtes de recherche collectés par les moteurs de recherche, soient habituellement anonymisés de manière à ce qu'aucun individu ne soit identifiable par son nom, il demeure que le collecteur initial des renseignements détient l'intégralité de cette information. Cela est particulièrement vrai pour les services qui nécessitent l'inscription de l'utilisateur, tel que pour un compte Google ou Facebook.

supplémentaires sur des individus[273]. En effet, l'un des objectifs principaux d'une technique comme le profilage comportemental est la découverte d'information supplémentaire sur des individus particuliers ou des groupes d'individus à partir du traitement et du couplage de renseignements généraux. Ainsi, quel degré de protection en vertu de la LPRPDÉ avons-nous réellement à l'égard des renseignements qui seront découverts, déduits, transformés ou fabriqués à partir de la collecte d'autres renseignements à notre sujet?

La question de la transformation de la nature des renseignements n'a pas encore fait directement l'objet de requête devant les tribunaux, mais certains exemples issus de la jurisprudence peuvent tout de même nous éclairer sur ce sujet. Dans l'affaire *Wansink c. Telus Communications Inc*., la Cour d'appel fédérale reconnait que l'empreinte vocale d'un individu, bien que son utilisation sans le consentement de l'intéressé ne constitue pas une atteinte importante à la vie privée, constitue néanmoins un renseignement personnel[274]. Or, le juge Décary fait une remarque étonnante lorsqu'il avance que l'intimé dans cette affaire n'utilisait pas la voix elle-même de ses employés, « mais l'empreinte vocale, qui est une matrice de chiffres »[275]. Ce commentaire du juge Décary laisse présager que la Cour pourrait considérer que la numérisation d'un renseignement réduit son caractère personnel. Or, si cela est effectivement le cas, on pourrait alors prétendre que tous les renseignements personnels collectés à partir d'Internet ne bénéficient pas de la même protection qui est garantie pour les renseignements collectés dans le monde physique. Pourtant, le CPVP a déjà reconnu que les renseignements collectés à partir d'Internet sont des renseignements personnels[276].

---

[273] CPVP, Rapport « Profilage », *supra* note 2 à la p. 27, où le CPVP indique que « en raison des progrès technologiques, il est de plus en plus difficile de faire en sorte que les renseignements demeurent entièrement anonymes ».

[274] *Wansink*, *supra* note 167 par. 11.

[275] *Ibid*., par. 12.

[276] Voir CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2003-162, « Un client se plaint de la présence de « témoins » sur le site Web d'une compagnie aérienne », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_7_f.cfm>, où le CPVP reconnait que les cookies sont des renseignements personnels. Voir aussi CPVP, Rapport « Profilage », *supra* note 2 à la p. 27, où le CPVP indique qu'il reconnait « qu'il existe des zones grises [dans la LPRPDÉ] et qu'il faut toujours tenir compte du contexte, mais les exemples de conclusions du Commissariat […] montrent que les renseignements recueillis par l'entremise du suivi, du profilage et du ciblage en ligne ont déjà été considérés comme des renseignements personnels, et les organisations devraient en tenir compte dans l'élaboration de leurs pratiques ».

Le CPVP s'est également penché sur la question de la communication de renseignements personnels compilés dans des profils individuels sans le consentement des individus concernés. Au terme de l'enquête portant sur les services de compilation de profils psychologiques du site Internet Abika.com[277], le CPVP a conclu que la création de tels profils constituait une fin qu'une personne raisonnable jugerait inappropriée et contrevenait au paragraphe 5(3) de la LPRPDÉ. Bien qu'il ait également jugé qu'Abika avait collecté, utilisé et communiqué des renseignements personnels non publics sans le consentement de la personne intéressée en contravention du principe 4.3, le Commissariat a considéré inapproprié les pratique du site Internet consistant à créer sur commande des profils psychologiques détaillés d'individus à partir de sources multiples de renseignements.

Mais, dans le contexte du profilage commercial, il est tout autant pratique courante de collecter et de compiler des renseignements personnels accessibles publiquement. Sur ce point, il n'est pas clair que les données obtenues en compilant des renseignements personnels publics, même s'il nous procure de l'information additionnelle sur un individu, jouissent de protections similaires à celles garanties pour les renseignements personnels non publics. Au Canada, le CPVP s'est attaqué à cette question dans une enquête portant sur la nécessité d'une entreprise d'obtenir le consentement des individus pour le couplage et la vente de renseignements accessibles publiquement[278]. Dans ce cas particulier, l'entreprise en cause fournissait des listes de renseignements démographiques personnalisées concernant des consommateurs à d'autres entreprises à des fins de marketing direct. Pour créer ces listes, l'entreprise compilait et couplait des données collectées à partir de diverses sources publiques, dont les noms, les adresses et les numéros de téléphone de consommateurs à partir des répertoires téléphoniques, avec des renseignements obtenus de Statistique Canada sous une forme anonyme.

[277] CPVP, Résumé n° 2009-009, *supra* note 75.
[278] Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2009-004, « Aucun consentement n'est requis pour l'utilisation de renseignements personnels accessibles au public combinés à des statistiques démographiques propres à un lieu géographique », en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009_004_0109_f.cfm> [CPVP, Résumé n° 2009-004].

Pour les plaignants dans cette affaire, le couplage de renseignements personnels accessibles au public à des statistiques démographiques propres à un lieu géographique entraîne la création de renseignements pouvant se rapporter à des individus identifiables, et donc, nécessite l'obtention d'un consentement de la personne visée pour tout usage ou communication. Cependant, le CPVP soutient dans ses conclusions que la compilation des listes de consommateurs de l'organisation « ne modifiait pas le statut des renseignements des pages blanches en les faisant passer de renseignements personnels accessibles au public à des renseignements personnels visés par les dispositions relatives au consentement ». Pour le CPVP, les renseignements publics figurant à ces listes avaient simplement été classés selon des critères géo-démographiques obtenus de Statistique Canada :

> [l]'entreprise n'associe pas de renseignements personnels, issus par exemple de listes d'abonnements à des magazines ou de registres publics, aux données des pages blanches. En revanche, l'entreprise utilise les renseignements groupés de [Statistique Canada], qui ne sont pas des renseignements personnels aux termes de la *Loi*, pour trier les renseignements personnels auxquels le public a accès.[279]

Pour le CPVP, la compilation de ces renseignements sous la forme de listes de consommateurs n'a pas modifié le statut des renseignements contenus dans les pages blanches. Selon le Commissariat, puisque les renseignements personnels auxquels le public a accès sont soustraits à l'obligation d'obtenir le consentement, ils demeurent également soustraits à cette obligation lorsqu'ils sont vendus sous forme de listes de consommateurs, malgré le fait que ces listes pourraient permettre de découvrir de nouveaux renseignements sur les individus figurant dans les annuaires téléphoniques.

Malgré ce qui précède, le CPVP avise que cette conclusion ne peut s'appliquer à tous les processus de couplage de données. Or, le Commissariat ne procure aucune indication permettant de déterminer dans quelles circonstances un individu pourrait s'attendre à ce que des renseignements publics à son sujet jouissent d'une certaine protection une fois qu'ils sont compilés et analysés à des fins secondaires, telle la création de profils comportementaux. Pourtant, les lois en matière de vie privée au Canada imposent tout de même des limites pour l'utilisation des renseignements personnels rendus publics. En effet,

[279] *Ibid.*

la LPRPDÉ stipule qu'aucun consentement n'est requis *uniquement* pour la collecte, l'utilisation et la communication de renseignements réglementaires auxquels le public a accès[280].

Les catégories de renseignements qui ne nécessitent pas de consentement sont explicitement énumérées dans le *Règlement précisant les renseignements auxquels le public a accès*[281]. Ceux-ci comprennent spécifiquement : les renseignements personnels figurant dans un annuaire téléphonique accessible au public, si l'abonné peut refuser que ces renseignements y figurent; les renseignements personnels qui figurent dans un répertoire, listage ou avis à caractère professionnel ou d'affaires qui est accessible au public; les renseignements personnels qui figurent dans un registre, qui sont recueillis aux termes d'une autorisation législative et pour lesquels un droit d'accès public est autorisé par la loi; les renseignements personnels qui figurent dans un dossier ou un document d'un organisme judiciaire ou quasi judiciaire accessible au public; les renseignements personnels qui figurent dans une publication, y compris les magazines, livres et journaux, sous forme imprimée ou électronique, qui sont accessibles au public, si l'intéressé a fourni les renseignements[282]. De plus, le règlement spécifie clairement que, pour certains de ces renseignements, la collecte, l'utilisation et la communication doivent être directement liées à la raison pour laquelle ils figurent dans le dossier ou le document[283].

On remarque à la lecture de cette liste que les législateurs canadiens ont voulu restreindre autant que possible les catégories de renseignements auxquels le public a accès[284]. Une telle approche restrictive démontre que, malgré la notion voulant que la

---

[280] LPRPDÉ, *supra* note 8 art. 7(1)*d*), (2)*c.1*) et (3)*h.1*).
[281] *Règlement précisant les renseignements auxquels le public a accès*, DORS/2001-7, art.1.
[282] *Ibid*., art. 1(a) à (e).
[283] *Ibid*., art. 1(b), (c) et (d). Les lois provinciales comportent également des dispositions similaires : PIPA Alta., *supra* note 200 art. 14(e), 17(e), 20(j), qui renvoie à Alberta Alta. Reg. 366/2003, art. 7; PIPA C.-B., *supra* note 200 art. 12(1)e), 15(1)e), 18(1)e), qui renvoie à Colombie-Britannique B.C. Reg. 473/2003, art. 6. Pour sa part, la Loi québécoise, *supra* note 199 art. 1, mentionne simplement que : « [l]es sections II et III de la présente loi ne s'appliquent pas à un renseignement personnel qui a un caractère public en vertu de la Loi ».
[284] Voir CPVP, Rapport « Profilage », *supra* note 2 à la p. 21, où le CPVP indique qu'« au Canada, les renseignements personnels qui figurent dans le domaine public ne peuvent pas nécessairement être utilisés à différentes fins. Par exemple, la LPRPDÉ indique que certains renseignements personnels auxquels le public a accès (au sens de la réglementation de la LPRPDÉ) peuvent être recueillis, utilisés et communiqués sans le

divulgation publique d'un renseignement signifie une perte de contrôle sur celui-ci, la LPRPDÉ accorde néanmoins une protection aux renseignements personnels rendus publics sans le consentement de l'intéressé. Mais, encore une fois, l'imposition d'une telle contrainte aux organisations permet difficilement de protéger les renseignements qui peuvent être dévoilés par un processus de compilation et d'analyse de montant massif de données.

Plusieurs utilisateurs du moteur de recherche en ligne d'AOL ont appris cette leçon au mois d'août 2006, lorsque le fournisseur Internet a rendu publique une liste de plus de 20 millions de requêtes de recherche provenant de plus de 650 000 utilisateurs sur une période de trois mois[285]. Bien que les requêtes de recherches n'identifiaient pas directement les utilisateurs par leurs noms, certains des renseignements s'y trouvant permettaient tout de même de dévoiler l'identité d'utilisateurs. En effet, plusieurs requêtes groupées sous le même utilisateur comportaient des recherches portant sur des adresses, des noms propres et même des renseignements sensibles tels des numéros de carte de crédit, susceptibles de concerner un individu particulier[286].

Dans de tels cas, les données mises en contexte avec l'ensemble des requêtes du même utilisateur permettent en effet de déduire un certain montant d'information additionnel à son sujet. Par exemple, certains dossiers d'utilisateurs d'AOL comprenaient des requêtes portant sur des sujets très intimes, voire gênants, tels l'inceste et le suicide. D'autres comportaient des requêtes permettant d'illustrer d'apparentes intentions criminelles, telles des recherches comme « comment tuer sa conjointe », couplées avec des requêtes de photos de cadavres et d'accidents de voiture[287]. Comme l'indique le professeur Omer Tene, des requêtes de recherche détaillées comme celles divulguées par AOL illustrent le montant

---

consentement de la personne; les fins auxquelles les renseignements peuvent être recueillis, utilisés ou communiqués sont néanmoins limitées » [nous soulignons].

[285] Tene, « What Google Knows », *supra* note 35 à la p. 1443; Ohm, « Broken Promises », *supra* note 56 à la p. 1717.

[286] Tene, « What Google Knows », *supra* note 35 à la p. 1449.

[287] Tene, « What Google Knows », *supra* note 35 à la p. 1444; Ohm, « Broken Promises », *supra* note 56 à la p. 1718.

d'information que dévoilent les utilisateurs à leur sujet lorsqu'ils se servent de moteurs de recherche[288].

À la lumière de ce qui précède, il semble raisonnable de s'attendre à ce que les renseignements issus des pratiques de compilation et d'analyse de renseignements bénéficient d'une certaine protection juridique. Bien que la protection garantie par la LPRPDÉ comporte certaines exceptions, notamment pour les renseignements règlementaires accessibles au public, elle offre néanmoins un certain recours dans les cas où une organisation fait la collecte, l'utilisation ou la communication de tels renseignements sans le consentement de l'intéressé. Or, il demeure que l'absence d'un test concret et objectif, tel que ceux établis dans *Pascoe* et *Gordon*, permet difficilement de déterminer quels renseignements, une fois transformés, bénéficient véritablement d'une protection en vertu de la Loi.

3.1.3. La sensibilité des renseignements

Le couplage et la réorganisation de fragments d'information permettent non seulement d'augmenter la qualité des renseignements personnels qu'une organisation possède à propos d'un individu, mais également de découvrir des choses nouvelles sur cette personne[289]. C'est notamment le cas avec les techniques de ciblage comportemental. En combinant des modèles mathématiques et statistiques de plus en plus avancés à des systèmes informatiques ayant des capacités d'analyses inégalées, certaines organisations sont dorénavant capables d'extraire des données descriptives et prédictives très précises à partir d'un montant limité d'information[290]. Or, considérant la précision des données qu'une organisation peut produire à partir de la collecte de nombreux fragments d'information sur une longue période de temps, ne serait-il pas raisonnable de s'attendre à ce que ces renseignements soient traités comme étant d'un plus haut degré de sensibilité, et donc, nécessitant une plus grande protection que les renseignements collectés initialement?

[288] Tene, « What Google Knows », *supra* note 35 à la p. 1443.
[289] Solove, *Understanding*, *supra* note 2 à la p. 119.
[290] Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 42.

La notion selon laquelle certaines catégories de données considérées comme plus sensibles nécessitent une protection supplémentaire n'est pas étrangère aux différents régimes de protection des renseignements personnels. Par exemple, le préambule de la *Directive 95/46/CE* du Conseil de l'Europe précise que, malgré la nécessité des États membres de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public le justifie, ceux-ci doivent néanmoins « prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes »[291]. Pour sa part, l'OCDE n'établit aucune catégorie précise de renseignements jugés sensibles dans ses *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, sous prétexte qu'il n'existe aucune interprétation universellement reconnue de ce qui constitue une donnée sensible, mais mentionne que toute donnée peut devenir sensible selon le contexte et l'utilisation qui en est faite[292].

À la lumière de ces passages, il n'est pas déraisonnable de croire que, suivant une approche contextuelle, l'information issue de l'analyse d'une multitude de données personnelles collectées sur une longue période de temps pourrait être interprétée comme étant de nature plus sensible que les renseignements initialement collectés. Mais la détermination des mesures de protection adéquates pour ces renseignements ainsi que la norme de contrôle appropriée pour évaluer la sensibilité de l'information se situent toujours dans une zone grise de la loi. Au Canada, la LPRPDÉ traite explicitement de la sensibilité des renseignements au troisième principe de l'annexe 1. L'article 4.3.4 énonce que :

> La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.[293]

[291] CE, *Directive 95/46/CE*, *supra* note 148 préambule par. 34.
[292] OCDE, *Lignes directrices*, *supra* note 150. Voir Scassa, « Text and Context », *supra* note 160.
[293] LPRPDÉ, *supra* note 8 ann. 1, art. 4.3.4.

Il ressort de ce principe de la LPRPDÉ, de façon similaire aux *Lignes directrices* de l'OCDE, que la détermination de la sensibilité d'un renseignement, tout comme la forme du consentement qu'une organisation doit obtenir, doit se faire en fonction du contexte[294]. Or, rien dans ce principe ne nous éclaire davantage sur la norme de contrôle appropriée pour déterminer dans quelle mesure le contexte aura une influence sur la sensibilité d'un renseignement. D'ailleurs, l'exemple fourni aux deux dernières phrases de ce principe semble suggérer que l'évaluation contextuelle de la sensibilité d'un renseignement ne repose pas autant sur les circonstances entourant sa collecte, son utilisation ou sa communication, mais plutôt sur la nature initiale du renseignement.

Il en va de même pour le principe 4.3.6, qui fournit quelques détails supplémentaires au sujet de la forme adéquate de consentement que les organisations doivent obtenir pour collecter et utiliser des renseignements sensibles :

> La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. […][295]

Également, le principe 4.7.2 indique que la nature des mesures de sécurité que doivent adopter les organisations pour protéger les renseignements personnels doit varier en fonction

---

[294] Cette notion a été discutée en détails dans l'affaire *Randall c. Nubodys Fitness Centres*, [2010] A.C.F. no 823 [*Randall*]. Pour des exemples de renseignements qui ont été jugés « sensibles » en vertu du droit canadien, voir CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2003-242, « Un homme s'oppose à ce que des travailleurs assignés temporairement traitent les renseignements liés à la paye », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031204_06_f.cfm> : les renseignements liés à la paye des employés; CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2003-226, « L'entreprise recueille sans raison valable des renseignements médicaux; les mesures de sécurité sont insuffisantes », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031031_f.cfm> : les renseignements de nature médicale; CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2006-324, « Un consommateur se plaint de devoir fournir des pièces d'identité afin d'obtenir son rapport de solvabilité », en ligne : <http://www.priv.gc.ca/cf-dc/2006/324_20060109_f.cfm> : le rapport de solvabilité d'un individu; CPVP, Résumé n° 2009-008, « Facebook », *supra* note 60 : les photographies, l'état civil, l'âge et les passe-temps. Dans *Cheskes v. Ontario (Attorney General)*, [2007] O.J. No. 3515, 87 O.R. (3d) 581, 159 C.R.R. (2d) 191, par. 61, la Cour supérieure de l'Ontario à conclu, sous la recommandation de la Commissaire à la protection de la vie privée du Canada, que les renseignements concernant la naissance et l'adoption était suffisamment sensibles pour bénéficier d'une protection sous l'article 7 de la *Charte canadienne des droits et libertés* qui garantit à chacun le droit à la vie, à la liberté et à la sécurité de sa personne.

[295] LPRPDÉ, *supra* note 8 ann. 1, art. 4.3.6.

de la sensibilité de ceux-ci[296]. Or, dans tous les cas, la Loi demeure silencieuse au sujet de la norme de contrôle appropriée pour déterminer les éléments contextuels pertinents pour juger la sensibilité d'un renseignement et de la forme de consentement approprié[297].

Comme l'indique la professeure Teresa Scassa, le fait de formuler ce principe en fonction du contexte dans lequel le renseignement fut collecté ne permet pas de rendre compte de la sensibilité liée à l'usage d'un renseignement[298]. Bien qu'un faible degré de consentement puisse être suffisant pour la collecte d'un renseignement personnel jugé peu sensible, cela n'écarte pas la possibilité que certaines utilisations subséquentes de ce renseignement puissent constituer une atteinte à la vie privée de la personne concernée[299]. Cela est particulièrement vrai en ce qui concerne les pratiques de profilage commercial. En effet, plusieurs des pratiques visant à collecter, agréer et analyser de nombreux renseignement portant sur des individus auront comme conséquence de créer des données plus précises et plus détaillées que les éléments initiaux qui les constituent[300]. L'incident impliquant la divulgation de requête de recherche par le fournisseur Internet AOL témoigne de ce fait. En toute vraisemblance, il ne serait donc pas déraisonnable de la part des individus concernés de s'attendre à ce que les données issues d'un tel processus soient traitées comme étant d'un plus haut degré de sensibilité.

La Cour fédérale a traité de la question de la sensibilité des renseignements dans *Randall c. Nubodys Fitness Centres*[301], une cause récente concernant la divulgation à un employeur de renseignements personnels liés à la fréquence d'utilisation d'un centre de conditionnement physique par ses employés. Dans cette affaire, la Cour soutient que cette information fait partie des renseignements les « moins sensibles, lorsqu'on les envisage

[296] *Ibid*., ann. 1, art. 4.7.2 : « La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés ».
[297] Scassa, « Text and Context », *supra* note 160 à la p. 14.
[298] *Ibid.*, à la p. 12.
[299] *Ibid.*
[300] Voir *supra* note 235.
[301] *Randall*, *supra* note 294.

objectivement »[302]. Par conséquent, la Cour indique que la collecte de ces renseignements par le centre de culture physique et leur transmission à l'employeur n'étaient pas déraisonnables. Cependant, elle note qu'en communiquant ces renseignements aux collègues du demandeur dans le but de créer une rivalité, l'employeur créa des circonstances particulières pour lesquelles un consentement implicite ne pouvait pas être déduit[303].

Malheureusement, la Cour ne fournit aucune indication quant au test sur lequel elle s'appuie pour déterminer que les renseignements en cause ne sont pas sensibles « objectivement ». De plus, malgré qu'elle reconnaisse que le contexte dans lequel les renseignements du demandeur furent divulgués a eu une influence sur leur sensibilité, il est important de noter que la Cour fédérale dans l'affaire *Randall* ne procure aucune indication quant aux circonstances particulières qui ont causé que les renseignements franchissent un certain seuil de sensibilité pour lequel un consentement explicite à la divulgation aurait été nécessaire. Le seul indice que fournit la Cour est la mention du fait que le demandeur se serait senti mal à l'aise avec la divulgation de ses renseignements à ses collègues[304]. À cet égard, peut-on affirmer que la détermination de la sensibilité de l'information dépend foncièrement de l'attente raisonnable de l'individu concerné[305]?

On retrouve une partie de la réponse à cette question dans l'une des premières enquêtes menées sous la LPRPDÉ concernant les pratiques de collecte de données d'Air

[302] *Ibid*., par. 42.
[303] *Ibid*., par. 44.
[304] *Ibid*., par. 43.
[305] La LPRPDÉ mentionne spécifiquement, à l'article 4.3.5 de l'annexe 1, la pertinence de l'attente raisonnable : « Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé. Le consentement ne doit pas être obtenu par un subterfuge ».

Canada pour son programme de fidélisation Aéroplan[306]. Dans ses conclusions, le CPVP indique que :

> […] la pratique d'utiliser l'information des membres du Plan pour faire la publicité des produits, services et promotions spéciales est en elle-même acceptable, [mais] qu'une personne raisonnable ne s'attendrait pas à ce qu'une telle pratique s'étende à la « fabrication sur mesure » de l'information à partir d'informations concernant les intérêts personnels ou professionnels, les usages ou préférences pour certains services et les statuts financiers potentiellement sensibles des individus sans leur consentement explicite.[307]

D'abord, il est important de noter dans cette affaire que le CPVP a spécifiquement exprimé son inquiétude concernant les risques associés à l'utilisation et la communication de données fabriquées à partir des habitudes et préférences d'achat des membres du programme. D'ailleurs, le Commissaire confirme que les renseignements fabriqués par un tel processus sont suffisamment sensibles pour justifier l'obtention d'un consentement explicite. Ensuite, il semble manifeste à la lecture de ce passage que l'attente raisonnable de l'individu est en effet un élément central à la détermination de la nature d'un renseignement personnel.

Pourtant, certaines organisations continuent à accumuler des montants phénoménaux de renseignements portant sur tous les aspects de la vie privée d'individus à partir de leur interaction avec des services sur Internet. Il est clair que la LPRPDÉ procure aux individus un certain nombre d'outils qui servant à protéger leur vie privée contre les pratiques des organisations qui utilisent leurs renseignements personnels. Cependant, il n'est pas aussi clair que ces outils sont suffisamment contraignants pour garantir que cette protection des renseignements personnels soit proportionnelle aux attentes réelles de vie privée des individus.

---

[306] CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2002-42, « Air Canada permet à 1 % des membres Aéroplan de se « désister » des pratiques de partage d'information », en ligne : <http://www.priv.gc.ca/cf-dc/2002/cf-dc_020320_f.cfm> [CPVP, Résumé n° 2002-42].
[307] *Ibid.*

3.2. Les fins acceptables

L'une des principales garanties de protection des renseignements personnels qu'offre la LPRPDÉ consiste à limiter le plus possible le montant de renseignements qui est collecté, utilisé et communiqué à notre sujet. À ce sujet, comme il est mentionné dans l'objet de la LPRPDÉ, ainsi que repris au paragraphe 5(3), les organisations ne peuvent collecter et utiliser des renseignements personnels « qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances »[308]. Dans une enquête récente, le CPVP a conclu que cette disposition signifie que les organisations ne doivent recueillir auprès de leurs clients « que le minimum de renseignements personnels dont elles ont besoin à des fins d'affaires légitimes »[309]. En ce qui concerne l'utilisation de renseignements à des fins secondaires, le CPVP a conclu que, peu importe les circonstances, aucune personne raisonnable jugerait appropriée l'utilisation à des fins secondaires de marketing de renseignements personnels de clients collectés à partir de leur formulaire de demande de carte de crédit[310].

Or, le CPVP a également reconnu certaines limites à cette garantie. Par exemple, concernant l'utilisation de renseignements accessibles publiquement, le CPVP a jugé que les pratiques d'une entreprise fournissant des listes de renseignements démographiques personnalisées de consommateurs à des fins de marketing direct à partir de renseignements publics couplés à des données de Statistique Canada n'étaient pas contraire au critère de la personne raisonnable, puisqu'il estime « qu'en rendant les renseignements des répertoires téléphoniques accessibles au public, le Parlement était conscient qu'ils pouvaient être, et seraient, utilisés à des fins de commerce et de marketing »[311]. Le CPVP a également reconnu que garantir la sécurité, diminuer les comportements illégaux et limiter le risque de

[308] LPRPDÉ, *supra* note 8 art. 5(3).
[309] CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2009-014, « La détection de la fraude n'est pas un motif acceptable pour recueillir des numéros de permis de conduire aux fins d'une adhésion à un magasin », <http://www.priv.gc.ca/cf-dc/2009/2009_014_0529_f.cfm>.
[310] CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2002-83, « Communication alléguée sans consentement de renseignements personnels pour des fins secondaires de marketing par une banque », <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_1_f.cfm>.
[311] CPVP, Résumé n° 2009-004, *supra* note 278.

responsabilité sont des fins légitimes pour avoir recours à l'utilisation d'un système de vidéosurveillance dans une station d'autobus[312].

Dans tous les cas, comme l'indique le juge Gibson dans *Turner c. Telus Communications Inc*., le paragraphe 5(3) « appelle une pondération des droits du point de vue d'une personne raisonnable »[313]. Pour déterminer quelles fins sont acceptables dans des circonstances particulières, la Cour fédérale dans *Eastmond* s'est servie du test à quatre points formulé par le CPVP dans son enquête sur cette affaire, qu'il énonce comme suit :

- La mesure est-elle manifestement nécessaire pour répondre à un besoin particulier?
- Est-il probable qu'elle répondra efficacement à ce besoin?
- La perte de vie privée est-elle proportionnelle à l'avantage obtenu?
- Existe-t-il un moyen qui porte moins atteinte à la vie privée et permette d'arriver au même but?[314]

Bien que la Cour ait déterminé dans cette affaire que le test ci-dessus n'est pas nécessairement pertinent pour toutes les circonstances dans lesquelles une organisation procède à la collecte de renseignements personnels[315], il s'avère tout de même utile pour dégager certaines des notions fondamentales de ce principe dans un contexte donné, tel celui de l'utilisation de renseignements collectés à partir des activités en ligne d'un individu.

---

[312] CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2009-001, « Contestation de la vidéosurveillance dans une station d'autobus par un employé de l'entreprise », <http://www.priv.gc.ca/cf-dc/2009/2009_001_0219_f.cfm>.

[313] *Turner c. Telus Communications Inc*., [2005] A.C.F. no 1981, 2005 CF 1601, par 39 [*Turner*].

[314] *Eastmond*, *supra* note 128 par. 13.

[315] *Ibid*., par. 130. La Cour rajoute au paragraphe suivant que « [l]e Parlement a clairement prévu que le caractère acceptable des fins pour lesquelles les renseignements personnels sont recueillis doit être analysé de manière contextuelle, en examinant où, quand, comment et pourquoi les renseignements sont recueillis. De plus, les fins acceptables de la collecte peuvent différer des fins acceptables de l'utilisation et des fins acceptables de la communication des renseignements recueillis, ce qui laisse supposer une flexibilité et une variabilité en fonction des circonstances ». En Alberta, la majorité de la Cour d'appel dans l'arrêt *Leon's Furniture*, *supra* note 254 a rejeté l'opinion du commissariat à l'information et à la vie privée de l'Alberta, qui avait appliqué un test similaire à celui de *Eastmond*, à savoir s'il existe un moyen qui porte moins atteinte à la vie privée pour accomplir la même fin. Selon le commissariat dans cette affaire, le principe des fins objectivement acceptables appelle à une approche minimaliste pour toute collecte et utilisation de renseignements personnels. Or, pour la majorité de la Cour d'appel de l'Alberta, les plaques d'immatriculation des véhicules sont destinées à être utilisées à des fins d'identification, et leur utilisation par l'appelante dans le but de prévenir la fraude constituait une fin légitime selon la loi albertaine.

Certes, si l'on considère que l'objectif initial derrière l'utilisation de techniques de profilage comportemental vise généralement le financement d'un service quelconque à partir de la communication de publicité à ses utilisateurs, on peut supposer que dans la plupart des cas les fins de la collecte et de l'utilisation des renseignements personnels seront objectivement acceptables selon le test de *Eastmond*. Mais, il demeure que le montant d'information que collectent et utilisent certaines organisations leur confère un certain pouvoir qui, si utilisé à des fins dont l'acceptabilité pourrait être remise en question, risquerait d'avoir des conséquences indésirables pour les personnes concernées. Le juge Gibson rejette toutefois cette interprétation préventive du paragraphe 5(3) de la LPRPDÉ dans l'affaire *Turner*, lorsqu'il stipule que « le critère des fins qu'une personne raisonnable estimerait acceptables dans les circonstances doit être appliqué compte tenu des circonstances telles qu'elles existent. » :

> J'accepte que les circonstances puissent changer, que de nouvelles utilisations et de nouvelles applications puissent être envisagées et adoptées, et que de nouvelles technologies visant à déjouer les mesures de sécurité puissent être développées. Je suis convaincu que ce n'est que lorsqu'elles seront concrètes et significatives, et non pas hypothétiques, qu'il conviendra de se pencher sur ces nouvelles utilisations et applications […].[316]

Ainsi, il semble que l'approche favorisée par la Cour fédérale dans *Turner* pour traiter de l'acceptabilité des fins de la collecte ou de l'utilisation des renseignements personnels est davantage axée sur la réparation que sur la prévention.

D'autre part, le principe des fins acceptables repose également sur la nécessité d'informer adéquatement les individus de ces fins et d'obtenir leur consentement avant la collecte ou l'utilisation de leurs renseignements. Cette question a été traitée par le CPVP dans une enquête portant sur le suivi d'employés à l'aide de technologies de localisation afin d'améliorer l'efficacité et la qualité des services. Selon le CPVP, une telle pratique constitue un objectif approprié si les employés sont suffisamment informés de celle-ci et y consentent[317]. Aussi, le CPVP a avancé dans son enquête portant sur les pratiques de

[316] *Turner*, *supra* note 313 par. 45.
[317] CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2009-011, « Le conducteur d'un véhicule de transports en commun s'oppose à l'utilisation de technologies (MDT et GPS) à bord des véhicules d'entreprise », <http://www.priv.gc.ca/cf-dc/2009/2009_011_0527_f.cfm>.

Facebook que la collecte de la date de naissance des utilisateurs aux fins d'application de la politique sur l'âge requis pour utiliser le site, laquelle étant destinée à protéger la sécurité des mineurs ainsi qu'à assurer la véritable identité des utilisateurs, constituait une fin légitime et appropriée aux termes du paragraphe 5(3). Or, le CPVP dans cette affaire a tenu à préciser que, pour être conforme aux dispositions de la LPRPDÉ, il est nécessaire que toutes les fins potentielles soient également explicitement indiquées. Dans ce cas, puisque les renseignements pouvaient potentiellement servir à des fins secondaires, dont notamment la publicité ciblée, le CPVP a indiqué qu'il serait nécessaire « de faire la distinction et d'expliquer clairement toutes les utilisations dans la Politique de confidentialité »[318]. Dans la prochaine section, nous discuterons plus en détail de la question de l'obtention du consentement.

3.3. L'obtention du consentement

3.3.1. Le contrôle des renseignements personnels

L'un des aspects les plus importants de protection de la vie privée consiste à reconnaître le besoin que les individus puissent exercer un certain contrôle sur l'information qui les concerne ou de leur procurer les outils nécessaires pour limiter l'accès à celle-ci. En effet, ce principe est largement reconnu comme un aspect central à la liberté et à l'autodétermination[319]. Comme l'indique la professeure Lisa Austin, le fait de placer le principe du consentement au centre de l'élaboration d'un encadrement législatif du droit à la protection des renseignements personnels permet de surmonter plusieurs des difficultés associées au concept de vie privée, puisque cela permet de décrire clairement le droit à la vie privée comme une forme de contrôle sur nos données[320]. Aussi, en garantissant aux individus un contrôle sur leurs renseignements, l'obtention du consentement sert à maintenir un certain équilibre entre les individus et les organisations[321].

---

[318] CPVP, Résumé n° 2009-008, « Facebook », *supra* note 60.
[319] Ian Kerr et al., « Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent », dans Ian Kerr, Valerie Steeves et Carole Lucock, dir., *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, New York, Oxford University Press, 2009, à la p. 9 [Kerr et al., « Soft Surveillance »].
[320] Lisa M. Austin, « Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA » (2006) 56 Univ. of Toronto L.J. 181, à la p. 187 [Austin, « Consent »].
[321] *Ibid*., à la p. 184.

C'est dans cet esprit que la plupart des lois en matière de protection des renseignements personnels incorporent la nécessité pour les organisations d'obtenir une forme quelconque de consentement auprès de la personne visée. Au Canada, l'obtention du consentement pour toute collecte, utilisation ou communication des renseignements personnels d'un individu est considérée comme un élément fondamental pour assurer une protection efficace et intégrale de la vie privée[322]. Comme nous l'avons vu au chapitre 2, la LPRPDÉ ainsi que les lois du Québec, de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels comportent toutes des dispositions étendues concernant la nécessité d'obtenir le consentement valide, explicite et éclairé d'un individu avant d'utiliser ses renseignements personnels de manière quelconque[323].

Sur le plan théorique, le modèle de protection de la vie privée fondé sur la nécessité de l'obtention du consentement est souvent compris comme un modèle de choix individuel, en ce sens qu'il permet à chacun de redéfinir sa propre conception de la vie privée en fonction du niveau désiré de contrôle ou de discrétion sur ses renseignements personnels[324]. Ainsi, les individus qui conçoivent la vie privée comme une partie déterminante de leur liberté et de leur autodétermination pourront adopter un comportement plus vigilant envers la collecte et la diffusion de leurs renseignements personnels, soit en évitant les services qui exigent la divulgation de certaines informations ou en employant des moyens techniques qui améliorent la sécurité de leurs données et de leur identité.

Malgré cela, on observe qu'au cours des dernières années, les méthodes permettant la collecte de donnée se sont de plus en plus incorporées dans plusieurs facettes de notre quotidien, rendant conséquemment plus difficile à contrôler le flux d'information personnelle qui en découle[325]. De ce point de vue, lorsqu'on considère l'ampleur du marché des données personnelles et le montant d'information collecté quotidiennement à notre sujet, il semble irréaliste de prétendre que les individus ont véritablement le plein contrôle sur les

[322] Scassa, « Text and Context », *supra* note 160 à la p. 8.
[323] Voir *supra* sous-section 2.2.2.
[324] Austin, « Consent », *supra* note 320 à la p. 187; Nissenbaum, *Privacy in Context*, *supra* note 4 à la p. 70.
[325] Kerr et al., « Soft Surveillance », *supra* note 319 à la p. 9.

renseignements qui sont produits, collectés, analysés et communiqués à leur sujet[326]. Or, il est essentiel que l'application de la LPRPDÉ ne permette pas que le l'obtention du consentement des individus ne devienne qu'une carte blanche aux organisations qui désirent faire la collecte et l'utilisation de renseignements personnels à des fins de profilage comportemental.

Le CPVP traite de la question du contrôle des renseignements personnels dans l'enquête portant sur les pratiques de Facebook[327]. Dans cette affaire, la Commissaire adjointe à la protection de la vie privée du Canada mentionne la nécessité que le réseau social en ligne informe ses utilisateurs du contrôle individuel qu'ils ont sur leurs paramètres de confidentialité. Bien qu'elle reconnaisse que Facebook fournit des paramètres de confidentialités très complets, la Commissaire adjointe estime toutefois que :

> […] comme Facebook a présélectionné les paramètres de confidentialité, et que plusieurs nouveaux utilisateurs, au moment de l'inscription, risquent de ne pas bien connaître la notion de paramètres de confidentialité et d'ignorer qu'ils peuvent exercer un contrôle sur l'échange de leurs renseignements personnels sur Facebook, je juge que ces mesures seules ne constituent pas un avis adéquat dans les circonstances.
>
> […] Facebook doit faire en sorte que les nouveaux utilisateurs puissent prendre des décisions éclairées quant à l'accès à leurs renseignements personnels et ce, dès le moment de l'inscription. Facebook offre aux utilisateurs des outils pour qu'ils puissent exercer un contrôle sur leurs renseignements personnels; Facebook doit maintenant s'assurer que les utilisateurs comprennent ces outils.[328] [Nous soulignons]

Malgré une telle reconnaissance de l'importance du contrôle des données par le CPVP, dans un contexte comme celui du profilage comportemental, le modèle de protection fondé sur le contrôle individuel des renseignements personnels permet difficilement de contrer les déséquilibres issus des pouvoirs de négociations entre les organisations et les individus.

---

[326] Voir CPVP, Rapport « Profilage », *supra* note 2 à la p. 33, où le Commissariat discute des préoccupations des personnes quant à la perte de contrôle sur les renseignements personnels qui sont collectés à leur sujet, notamment pour l'utilisation à des fins secondaires de profilage.
[327] CPVP, Résumé n° 2009-008, « Facebook », *supra* note 60.
[328] *Ibid.*

En effet, tant qu'un nombre suffisant d'utilisateurs d'un service qui collecte et utilise des renseignements personnels ne demandera pas un plus grand contrôle sur cette information, un consommateur individuel n'a pratiquement aucun pouvoir de négociation dans un tel marché[329]. Par exemple, selon sa *Déclaration des droits et responsabilités*, Facebook indique :

> 1. We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and become a fan.
>
> 2. For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you a minimum of three days notice. For all other changes we will give you a minimum of seven days notice. All such comments must be made on the Facebook Site Governance Page.
>
> 3. <u>If more than 7,000 users comment on the proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.</u>
>
> 4. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.[330] [Nous soulignons]

En imposant de telles politiques au moment de l'inscription à un service, il s'avère facile pour les organisations de réduire la capacité des utilisateurs à maintenir un contrôle individuel effectif sur leurs renseignements personnels. Dans de telles circonstances, le maintien du contrôle sur son information personnelle repose en grande partie sur la question de l'autonomie et du choix rationnel des individus à se souscrire ou non à de telles politiques en échange d'un service.

Or, il n'est pas clair que les utilisateurs de services en ligne ont toujours la possibilité de faire des choix informés en ce qui concerne le consentement à la collecte et à l'utilisation

---

[329] Austin, « Consent », *supra* note 320 à la p. 191.

[330] Facebook, « Statement of Rights and Responsibilities », en ligne : Facebook.com <http://www.facebook.com/terms.php>, art. 13.

de leurs renseignements à des fins secondaires[331]. En reprenant l'exemple de Facebook, le professeur James Grimmelmann indique que les utilisateurs du réseau social sont généralement soucieux de leur vie privée, mais qu'ils éprouvent systématiquement de la difficulté à évaluer correctement le coût que représente chacune de leurs actions sur leur vie privée[332]. Selon lui, cela résulte en partie de la façon dont les réseaux sociaux sur Internet agissent sur certains biais cognitifs sociaux. En effet, les sites comme Facebook créent chez les utilisateurs l'impression d'interagir dans un espace clos et à l'abri des regards d'autrui. Par conséquent, ces derniers deviennent moins vigilants, puisque cette distraction influence leur capacité de prédire correctement les conséquences qu'auront leurs activités sur leur vie privée[333].

Pour des organisations comme Facebook, dont le revenu dépend de la collecte et l'utilisation de renseignements personnels à des fins publicitaires ou de marketing, un tel manque de vigilance de la part de leurs utilisateurs n'est peut être pas toujours planifié, mais est certainement désiré. Sur ce point, si l'on concède que le contrôle des renseignements personnels est central à toute protection efficace de la vie privée, il est nécessaire d'assurer que ce contrôle ne soit pas perdu en raison d'un manque de compréhension des conséquences associées à la divulgation de données personnelles, ou par une certaine forme de manipulation de la part des organisations qui profitent de l'utilisation des renseignements personnels. Au sens pratique, cela se traduit par l'obtention d'un consentement valide de la part d'un individu avant toute collecte et utilisation de ses renseignements personnels.

---

[331] Voir Avner Levin et al., « The Next Digital Divide: Online Social Network Privacy » (mars 2008), aux pp. 25-26, en ligne :
<http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf>, une étude portant sur l'utilisation des réseaux sociaux en ligne qui démontre que sur les 92 % des jeunes Canadiens qui sont membres de tels sites, plus de la moitiés d'entre eux sont neutre ou non préoccupés du fait que des étrangers aient accès à l'information qu'ils affichent sur ces sites. Selon la même étude, seulement 42 % des jeunes Canadiens avaient lu les politiques de ces sites en matière de vie privée, mais que 70 % d'entre eux avaient ajusté la configuration de leur profil pour limiter l'accès à certains groupes ou individus. Voir aussi Bergert, « Balancing Consumer Privacy », *supra* note 38 à la p. 25.

[332] James Grimmelmann, « Privacy as Product Safety » (2009-2010) 19 Widener L.J. 793, aux pp. 796 et 802 [Grimmelmann, « Product Safety »].

[333] *Ibid*., à la p. 803. Voir aussi James Grimmelmann, « Saving Facebook » (2009) 94 Iowa L. Rev. 1137, aux pp. 1164-65.

3.3.2. La validité du consentement

La LPRPDÉ et les lois provinciales en matière de protection des renseignements personnels comportent chacune des dispositions visant à garantir que le consentement que les organisations obtiennent auprès des individus satisfasse un certain nombre de critères pour être considéré comme valide[334]. Comme nous l'avons vu, on retrouve notamment parmi celles-ci l'obligation d'obtenir un consentement volontaire et informé, l'obligation d'adapter la forme du consentement selon la nature des renseignements, l'imposition de limitations quant à la collecte, l'utilisation et la conservation des renseignements, ainsi que le droit de retirer son consentement. Dans certains cas, les tribunaux et les commissariats à la protection de la vie privée ont également conclu que des entreprises ont manqué à leurs obligations en ne spécifiant pas adéquatement les fins pour lesquelles elles collectaient et utilisaient des renseignements personnels[335]. Aussi, comme nous l'avons vu, les tribunaux ont mis une emphase particulière sur l'acceptabilité de ces fins aux yeux d'une personne raisonnable et objective. Malgré cela, il semble que plusieurs organisations introduisent dans les conditions d'utilisations de leurs services des clauses contractuelles qui permettent de contourner les protections garanties par les dispositifs législatifs telle la LPRPDÉ.

Avec Internet et les autres technologies d'information et de communication, l'obtention du consentement des consommateurs pour la collecte et l'utilisation de renseignements se fait généralement sous la forme d'une entente contractuelle[336]. Cependant,

---

[334] Voir *supra* sous-section 2.2.2.

[335] *Englander*, *supra* note 145; CPVP, Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ n° 2003-152, « Un câblodistributeur accusé de recueillir trop de renseignements personnels comme condition de service », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030414_2_f.cfm>; CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2003-203, « Un particulier laisse percer ses inquiétudes quant aux clauses de consentement sur un formulaire de demande de carte de crédit » en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030805_01_f.cfm>; CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2003-244, « Communication présumée de renseignements personnels sans consentement, à des fins commerciales secondaires, par la société de télécommunications « A » », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031107_02_f.cfm>; CPVP, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2005-296, « Remise en question du libellé du consentement et de l'activité de surveillance » en ligne : <http://www.priv.gc.ca/cf-dc/2005/296_050314_02_f.cfm>. Alberta Information and Privacy Commissioner, « Report on the Investigation into Collection, Use and Disclosure of Customer Information Re: EPCOR » (26 juillet 2004), Investigation Report P2004-IR-001, en ligne : <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2310>. Voir Lawson et O'Donoghue, « Approaches to Consent », *supra* note 209 à la p. 34.

[336] Andrea M. Matwyshyn, « Resilience: Building Better Users and Fair Trade Practices in Information »

malgré qu'ils paraissent similaires aux ententes contractuelles traditionnelles, en général, les contrats en ligne sont de nature particulièrement unilatérale[337]. En effet, alors que la notion traditionnelle du contrat peut être définie comme un accord consensuel négocié de bonne foi entre deux partis libres et informés, les contrats visant l'obtention du consentement d'un individu à la collecte et l'utilisation et la communication de ses renseignements personnels sont pour leur part remarquablement standardisés et non négociables[338]. Même lorsqu'une politique en matière de vie privée parait convenable, les organisations se réservent habituellement le droit de modifier et de porter des amendements à leurs politiques en tout temps et sans préavis[339].

Devant cette constatation, certains experts en droit de la responsabilité contractuelle ont avancé que, dans le contexte des ententes contractuelles sur Internet, le consentement éclairé et le pouvoir de négociation des utilisateurs de services ne sont rien de plus que des concepts fictifs[340]. Comme le stipule le professeur Daniel Barnhizer, les contrats en ligne étirent la nature volontaire de l'entente contractuelle au-delà de sa capacité par le biais de méthodes, tels les *browse-wrap* et les *click-wrap*, ces contrats qui se présentent sur l'écran comme une fenêtre munie d'une barre de défilement et qui permettent l'acceptation de l'entente avec un clic de souris, souvent sans même avoir l'obligation d'en faire défiler le contenu[341].

À ce sujet, le CPVP évoque la nécessité pour les organisations de faire preuve de transparence dans la formulation d'entente contractuelle visant le consentement pour la

---

(2010-2011) 63 Fed. Comm. L.J. 391, à la p. 403. Voir Joshua A.T. Fairfield, « Anti-social Contracts: The Contractual Governance of Virtual Worlds » (2008) 53 R.D. McGill 427, pour une discussion plus générale sur la nature des contrats dans le monde virtuel.

[337] H. Brian Holland, « Privacy Paradox 2.0 » (2009-2010) 19 Widener L.J. 893, à la p. 907.

[338] *Ibid*.

[339] Dans *Kanitz v. Rogers Cable Inc.,* (2002) 58 O.R. (3e) 299, la Cour supérieure de l'Ontario a conclu que la l'affichage sur un site Internet d'une modification à une clause contractuelle constituait une forme de communication adéquate. Voir Vincent Gautrais, « The Colour of E-consent » (2003-2004) 1 UOLTJ 189, à la p. 204 [Gautrais, « E-Consent »].Voir aussi Tene, « What Google Know », *supra* note 35 à la p. 1468.

[340] Daniel D. Barnhizer, « Propertization Metaphors for Bargaining Power and Control of the Self in the Information Age » (2006) Clev. St. L. Rev. 69, à la p. 81 [Barnhizer, « Propertization »].

[341] *Ibid.* Pour une discussion plus détaillée sur les contrats *click-wrap* et *browse-wrap*, voir Robert A. Hillman et Jeffrey J. Rachlinski, « Standard-Form Contracting in the Electronic Age » (2002) 77 N.Y.U. L. Rev. 429, à la p. 431 [Hillman et Rachlinski, « Standard-Form »]; Gautrais, « E-Consent », *supra* note 339 à la p. 206.

collecte et l'utilisation de donnée, tel que le prévoit le huitième principe de l'annexe 1 de la LPRPDÉ. Comme il le mentionne dans un rapport portant sur le ciblage en ligne :

> [l]a LPRPDÉ exige que les organisations soient transparentes au sujet de leurs politiques et pratiques. Les renseignements fournis aux consommateurs sur le suivi et le ciblage en ligne sont, bien souvent, trop complexes ou constituent du jargon juridique.[342]

Comme le précise le CPVP, cette notion est essentielle pour permettre aux individus qui utilisent des services en ligne de décider eux-mêmes, et en pleine connaissance de fait, s'ils veulent ou non consentir à la collecte ou à l'utilisation de leurs données[343].

Pourtant, considérant le montant d'information qui est quotidiennement collecté à partir des activités d'utilisateurs de services sur Internet, les organisations ne semblent pas avoir de difficulté à obtenir le consentement des individus concernés. Selon Gary Marx, la perte de contrôle sur les pratiques de collectes de données est en partie due au phénomène de « volontarisme obligatoire » (*mandatory volunteerism* en anglais), qu'il décrit comme une méthode sournoise consistant à formuler un message dans le but de créer l'impression chez les autres qu'ils agissent de façon volontaire alors que ce n'est pas véritablement le cas[344]. On rencontre ce type de message dans la majorité des contrats sur Internet, où les options qui sont présentées au consommateur se limitent généralement au choix de consentir « librement » à la communication de ses renseignements personnels, ou bien de renoncer au service désiré. Un message ainsi formulé permet de guider l'opinion du consommateur vers le consentement à la divulgation de ses données tout en imprégnant chez lui l'impression qu'il a agi de façon parfaitement volontaire[345].

---

[342] CPVP, Rapport « Profilage », *supra* note 2 à la p. 30

[343] *Ibid.* Voir FTC, « Protecting Consumer Privacy », *supra* note 1 à la p. 25, où la Federal Trade Commission des États-Unis soutient que la difficulté qu'éprouvent les utilisateurs de nouvelles technologies d'information et de communication à donner un consentement éclairé découle notamment du manque de transparence dans les politiques en matière de vie privée des organisations.

[344] Gary Marx, « Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information », dans T. Monahan, *Surveillance and Security: Technological Politics and Power in Everyday Life*, London, Routledge, 2006, à la p. 37, tel que mentionné dans Ian Kerr et al., «Soft Surveillance », *supra* note 319 à la p. 9.

[345] *Ibid.*

À cet égard, certaines organisations introduisent des clauses dans les conditions d'utilisation de leurs services qui, en toute vraisemblance, rendent conditionnel à l'obtention d'un bien ou d'un service le consentement à la collecte, l'utilisation et la communication de ses renseignements personnels, bien que cela contrevienne au principe 4.3.3 de la LPRPDÉ. Par exemple, Google stipule dans ses conditions d'utilisation de compte que « [i]n order to use the Services, you must first agree to the Terms. You may not use the Services if you do not accept the Terms »[346]. Certes, les organisations en ligne qui ne collectent que les renseignements nécessaires pour réaliser leurs fins légitimes et explicitement indiquées seront exemptées de cette disposition de la Loi. Mais dans le contexte de profilage commercial, les ententes contractuelles en ligne visent plus particulièrement l'obtention du consentement pour l'utilisation des renseignements personnels à des fins secondaires, puisque ces renseignements seront généralement obtenus à partir de l'interaction d'un utilisateur avec un service[347].

Google en est un parfait exemple, en ce sens que le montant de renseignements collecté et analysé au sujet d'un individu connecté à un compte Google va bien au-delà de ce qui est nécessaire pour accomplir sa tâche principale, soit de générer des résultats de recherche pertinents. Dans ses *Règles de confidentialité*, auxquelles doivent consentir les utilisateurs d'un compte Google[348], l'entreprise stipule que :

> […] les informations collectées peuvent être utilisées aux fins suivantes :
>
> - fournir, gérer, protéger et améliorer nos services (y compris les services de publicité), et en développer de nouveaux ; et
>
> - protéger les droits ou la propriété de Google ou de ses utilisateurs.

[346] Google, « Terms of Service », art. 2.1, en ligne : Google.ca <http://www.google.ca/accounts/TOS> [Google, « Terms »].
[347] Voir É-U., *Statement of Federal Trade Commission Concerning Google/DoubleClick* (FTC n° 071-0170) 20 décembre 2007, en ligne : <http://www.ftc.gov/os/caselist/0710170/071220statement.pdf>, pour une discussion du FTC, dans le cadre de l'acquisition de DoubleClick par Google, portant sur la façon dont les moteurs de recherche génèrent des profits à partir de l'utilisation à des fins secondaires des renseignements obtenus par l'analyse des requêtes des utilisateurs.
[348] Voir Google, « Terms », *supra* note 346 art. 7.2.

> Dans le cas où nous serions amenés à utiliser ces informations dans un autre but que celui pour lequel elles ont été collectées, nous vous demanderons votre consentement préalable.[349] [Nous soulignons]

Bien entendu, une organisation comme Google pourrait se défendre en avançant que la collecte de renseignements personnels de ses utilisateurs à des fins de publicités ciblées est essentielle à sa capacité d'offrir l'ensemble de ses services, puisque la publicité représente le gagne-pain principal de l'entreprise[350].

C'est précisément le point qu'a voulu faire valoir Facebook devant le CPVP relativement aux pratiques publicitaires de son réseau social en ligne[351]. En défense à des allégations portant sur l'obligation des utilisateurs de Facebook de consentir à la collecte et la communication de leurs renseignements personnels à des fins secondaires lors de l'inscription, l'entreprise a tenté de démontrer que cela n'est pas en contravention du principe 4.3.3 de la LPRPDÉ puisque « la publicité constitue une importante source de revenu »[352], et donc ne constitue pas une fin secondaire. La Commissaire adjointe a confirmé la validité de ce point, en soutenant que :

> [d]ans le passé, lorsqu'il était question de marketing, le Commissariat faisait toujours la distinction entre les fins premières et secondaires. Les fins premières sont celles essentielles à la prestation d'un service. Les fins secondaires sont celles qui ne visaient pas les renseignements au moment de leur collecte initiale. Dans les cas étudiés auparavant où il était question de publicité, on considérait souvent que cette dernière constituait une fin secondaire – dans certaines circonstances, les utilisateurs pouvaient choisir d'en être exclus.
>
> Le modèle organisationnel de Facebook est différent de ceux des organisations sur lesquelles nous nous sommes penchés jusqu'à maintenant. Si le site est gratuit pour les utilisateurs, il ne l'est pas pour Facebook qui a besoin de revenus publicitaires afin de fournir le service. De ce point de vue, la publicité est essentielle à la prestation de ce service. Ceux et celles qui souhaitent utiliser le service doivent donc accepter de recevoir une certaine quantité de publicité.[353] [Nous soulignons]

---

[349] Google, « Règles de confidentialité », en ligne : <http://www.google.com/intl/fr/privacy/privacy-policy.html>.
[350] Moffat, « Regulating Search », *supra* note 49 à la p. 486.
[351] CPVP, Résumé n° 2009-008, « Facebook », *supra* note 60.
[352] *Ibid.*
[353] *Ibid.*

Certes, la nécessité de chercher un tel équilibre entre le droit à la vie privée des individus et le besoin des organisations est un principe directeur du modèle de protection des renseignements personnels au Canada. Comme en témoigne la Cour d'appel fédérale dans l'arrêt *Englander*, la LPRPDÉ est en soi un compromis visant à concilier ces deux intérêts concurrents[354].

Or, il demeure que l'application uniforme de ce principe peut s'avérer bien plus profitable pour les organisations que pour les utilisateurs. Comme nous l'avons vu au premier chapitre, il est incontestable que la collecte et l'utilisation des renseignements personnels de leurs utilisateurs constituent une valeur économique tangible et quantifiable pour des organisations comme Facebook et Google[355]. Ce qui est moins clair, c'est le coût véritable que représente pour un individu le fait de consentir à la collecte de ses renseignements personnels par de telles organisations. Mais, lorsqu'on considère qu'un tel consentement peut permettre la création de profils psychologiques détaillés à son sujet, de suivre en temps réel ses activités en ligne à l'aide de cookies, de formuler des prédictions sur son comportement à partir de ses intérêts et de ses achats et de lui livrer de la publicité ciblée en conséquence, il devient apparent que le compromis que doit faire l'utilisateur n'est pas exactement proportionnel à celui fait par l'organisation[356].

3.3.3. La forme du consentement

Nous avons vu que, selon la LPRPDÉ, les organisations doivent généralement obtenir un consentement explicite auprès d'un individu pour toute collecte, utilisation ou communication de renseignements personnels à son sujet susceptibles d'être considérés comme sensibles, alors que pour certains renseignements moins délicats, un consentement

[354] *Englander*, *supra* note 145 par. 38 et 39.
[355] En 2010, les revenus de la publicité en ligne ont atteint 2,23 milliard de dollars au Canada seulement. Voir Bureau de la publicité interactive du Canada, « En 2010, les revenus de la publicité en ligne au Canada se sont élevés à 2,23 milliards de dollars, dépassant ceux de la publicité dans les quotidiens », en ligne : <http://www.iabcanada.com/fr/blogue/la-publicite-en-ligne-2010>.
[356] Il est intéressant de noter que la Cour supérieure du Québec, dans l'affaire *St-Arnaud v. Facebook inc*., [2011] Q.J. No. 3161, 2011 QCCS 1506, a estimé que l'adhésion à un compte Facebook ne constitue pas une entente contractuelle au sens du *Code civil* du Québec puisque le service offert par le défendeur est gratuit. À cet égard, il est clair que pour cette Cour, le consentement à la collecte et à l'utilisation de renseignements personnels est d'une valeur inférieure, voir nul, en comparaison au service offert par Facebook.

implicite peut parfois suffire. Dans tous les cas, la forme du consentement que doivent obtenir les organisations dépend davantage sur les circonstances entourant la collecte des renseignements[357]. Sur ce point, nous avons également vu que l'attente raisonnable des individus joue un rôle central dans la détermination de la forme appropriée de consentement. Or, compte tenu de la nature des renseignements qui peuvent être générés par la compilation massive de données personnelles dans des profils comportementaux individuels, n'est-il pas concevable que des individus, s'ils étaient sciemment informés de ces pratiques, auraient de très hautes attentes de vie privée pour cette information et qu'ils exigeraient que les organisations obtiennent toujours un consentement explicite de leur part?

À ce propos, on considère habituellement le consentement explicite comme un consentement « positif », alors que le consentement implicite est plutôt « négatif »[358]. Le consentement positif, que l'on rencontre fréquemment sous la forme d'une « option d'adhésion » (*opt-in* en anglais), implique que la configuration par défaut des conditions d'utilisation d'un service n'inclut pas le consentement de l'utilisateur. Si celui-ci désire adhérer à l'option de divulguer ses renseignements, il doit poser un geste concret pour valider son consentement. Par exemple, dans une enquête portant sur les pratiques de collecte de renseignements personnels à des fins de promotion par le service de billetterie Ticketmaster, le CPVP a conclu que l'inclusion d'une case que les utilisateurs doivent cocher pour consentir à la collecte de renseignements à des fins de promotion constitue une forme suffisamment explicite de consentement[359]. Or, dans les contrats en ligne, c'est plutôt le modèle opposé qui domine, soit une « option de retrait » (*opt-out* en anglais). Dans ce cas, le consentement de l'utilisateur est présumé à partir de son acceptation initiale des conditions d'utilisation du service. Le retrait du consentement doit se faire par la suite, soit en l'indiquant au fournisseur du service, ou par le désabonnement au service.

---

[357] Voir *Randall*, *supra* note 294 par. 43.
[358] Voir CPVP, Rapport « Profilage », *supra* note 2 aux pp. 29-33, pour une discussion en détail sur ce sujet.
[359] CPVP, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2008-388, « Ticketmaster Canada Limited a révisé ses politiques et pratiques relativement à la LPRPDÉ en vue de protéger les renseignements personnels de ses clients », en ligne : <http://www.priv.gc.ca/cf-dc/2008/388_20080212_f.cfm>.

À ce sujet, on remarque que les lois en matière de protections des renseignements personnels au Canada et dans les provinces ont des approches différentes quant à la façon de déterminer la forme appropriée de consentement qui doit être obtenu. L'article 14 de la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec stipule que le consentement à la collecte, à l'utilisation et à la communication d'un renseignement personnel doit être « manifeste, libre, éclairé et être donné à des fins spécifiques »[360]. À la lecture du libellé de l'article 14, il semble juste de prétendre que les législateurs québécois ont prévu que les organisations obtiennent un consentement positif auprès de l'intéressé dans tous les cas sauf ceux indiqués dans la Loi, et non uniquement pour les renseignements sensibles[361].

En revanche, les lois de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels permettent aux organisations, sous réserve de certaines conditions, une utilisation plus générale du consentement négatif[362]. Selon les deux lois des provinces de l'Ouest, le consentement négatif est suffisant dans tous les cas où le consentement est informé, l'intéressé a eu l'occasion de refuser de donner son consentement, il ne l'a pas retiré dans un temps raisonnable, et où la collecte, l'utilisation ou la communication est raisonnable compte tenu de la sensibilité des renseignements[363].

Pour sa part, la LPRPDÉ demeure très vague quant à la détermination de la forme appropriée de consentement que doivent obtenir les organisations. En effet, ses indications se limitent essentiellement à l'importance de tenir compte de la nature des renseignements ainsi qu'au contexte. À propos de la nature des renseignements, nous avons précédemment tenté de démontrer que le fait d'agréer, d'analyser et de catégoriser une multitude de renseignements peu sensibles permet de transformer la valeur de cette information pour en créer des données qui pourront potentiellement révéler des détails très précis sur la vie d'individus identifiables. Comme nous l'avons vu, dans son enquête portant sur le

---

[360] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39, art. 14.
[361] Lawson et O'Donoghue, « Approaches to Consent », *supra* note 209 à la p. 38.
[362] *Ibid.*
[363] Alberta : *Personal Information Protection Act*, S.A. 2003, c. P-6.5, art. 8(3); Colombie-Britannique : *Personal Information Protection Act*, S.B.C. 2003, c. 63, art. 8(3). Voir Lawson et O'Donoghue, « Approaches to Consent », *ibid.*

programme de fidélisation Aéroplan de Air Canada, le CPVP a jugé que renseignements fabriqués à partir des habitudes et des préférences d'achats d'un individu étaient suffisamment sensibles pour justifier l'obtention d'un consentement positif de la personne concernée[364].

Or, pour déterminer la forme appropriée de consentement pour l'utilisation de renseignements personnels pour créer des profils de consommateurs, nous ne pouvons pas nous limiter au seul critère de la nature du renseignement, puisque celle-ci risque de varier largement en fonction du contexte et de l'utilisation qui en sera faite. Comme nous l'avons vu avec l'affaire *Randall* de la Cour fédérale et avec l'enquête menée par le CPVP portant sur le programme Aéroplan d'Air Canada, l'attente raisonnable de l'individu concerné est un élément contextuel central à l'évaluation de la forme appropriée de consentement que doivent obtenir les organisations. D'ailleurs, le Commissariat indique, dans un document d'autoévaluation pour les organisations publié sur son site Internet, qu'une pratique exemplaire consiste à obtenir un consentement explicite pour toute communication de renseignements personnels à de tierces parties ou pour toute fin secondaire « à laquelle le client ne s'attendrait pas raisonnablement pour l'obtention d'un bien ou d'un service […] »[365].

À la lumière de ce qui précède, il semble justifié de prétendre que les organisations qui créent des profils de leurs utilisateurs devraient toujours chercher à obtenir un consentement positif, peu importe la nature des renseignements collectés ou le contexte dans lequel le consentement est obtenu. À cet égard, le CPVP a clairement indiqué dans une enquête qu'il privilégie le consentement positif « en tant que méthode la plus appropriée et la plus respectueuse à utiliser en tout temps »[366]. Le Commissariat rajoute que le consentement négatif est acceptable « dans certains cas rigoureusement définis », qu'il énumère comme étant :

---

[364] CPVP, Résumé n° 2002-42, *supra* note 306.
[365] CPVP, « Outil d'autoévaluation – LPRPDÉ », en ligne : <http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_f.cfm>.
[366] CPVP, Résumé n° 2003-207, *supra* note 252.

- les renseignements personnels doivent être nettement non sensibles de par leur nature et leur contexte;

- la communication doit être limitée et bien définie quant à la nature des renseignements personnels qui seront utilisés ou communiqués et à la mesure dans laquelle ils sont censés l'être;

- les intentions de l'organisation doivent être circonscrites et bien définies, énoncées d'une manière raisonnablement claire et compréhensible et signalées à la personne au moment de recueillir ses renseignements personnels;

- l'organisation doit mettre en place une procédure efficace, facile et peu coûteuse qui permet d'emblée à ses clients de se désister ou de retirer leur consentement relativement aux activités secondaires de marketing, et elle doit les en aviser au moment de recueillir leurs renseignements personnels.[367]

Bien qu'il serait possible pour les organisations d'interpréter ce passage de façon suffisamment large pour justifier certaines pratiques, il semble néanmoins que l'intention du CPVP est de limiter le plus possible l'utilisation du consentement implicite pour la collecte et l'utilisation de renseignements personnels à des fins secondaires, tels le marketing ou le profilage en ligne[368].

En ce qui concerne la communication de renseignements personnels à des tiers, le CPVP reprend essentiellement la même logique dans l'enquête portant sur les pratiques de Facebook. Dans son évaluation des plaintes portées à l'égard de renseignements personnels communiqués par le réseau social à des développeurs d'applications, la Commissaire adjointe à la vie privée indique que :

---

[367] *Ibid.*

[368] Voir CPVP, Rapport « Profilage », *supra* note 2 aux pp. 29-30 : « Le Commissariat estime que pour recourir à un mécanisme de consentement négatif, par exemple pour obtenir un consentement pour l'utilisation de renseignements personnels à des fins secondaires de marketing, l'organisation doit répondre aux exigences suivantes : Il faut démontrer que les renseignements personnels ne sont pas à caractère délicat compte tenu de leur nature et du contexte. La situation prévoyant le partage d'information doit être limitée et clairement définie sur le plan de la nature des renseignements personnels devant être utilisés ou communiqués, ainsi que de la portée de l'utilisation ou de la communication prévue. Les objectifs de l'organisation doivent être limités et nettement définis, et énoncés d'une manière claire et facile à comprendre. En règle générale, l'organisation devrait obtenir au moment de la collecte le consentement de la personne concernée pour utiliser ou communiquer les renseignements personnels ».

> [e]n considération des principes 4.3 et 4.3.4, je suis préoccupée à l'idée que Facebook n'utilise pas la forme de consentement appropriée pour la communication des renseignements personnels des utilisateurs à des tiers développeurs d'applications. À mon avis, compte tenu que les renseignements personnels des utilisateurs sont possiblement sensibles, il y aurait lieu de recourir au consentement actif exprès dans tous les cas.[369] [Nous soulignons]

Malgré tout ce qui précède, il demeure difficile de prétendre que les organisations cherchent généralement à obtenir un consentement explicite auprès des individus pour l'utilisation de ses données à des fins secondaires. De toute évidence, l'obtention d'un consentement implicite pour la collecte et l'utilisation de renseignements personnels dans le but de créer des profils comportementaux détaillés sur des consommateurs semble largement inappropriée. Or, même si l'on convient que les pratiques de profilage en ligne nécessitent un consentement explicite, nous avons vu que la validité du consentement obtenu par entente contractuelle en ligne peut toujours être remise en question. Même si les dispositions en matière de protection des renseignements personnels, de détermination des fins acceptables et d'obtention du consentement qui figurent dans les lois canadiennes permettent de limiter et d'encadrer en partie les pratiques de profilage comportemental, il s'avère qu'une interprétation trop souple de celles-ci en faveur des intérêts des organisations risque de réduire leur portée et leur efficacité à plus long terme. Dans le prochain chapitre, nous aborderons l'approche européenne en matière de protection des renseignements personnels afin d'établir si nous pouvons en tirer des leçons.

[369] CPVP, Résumé n° 2009-008, « Facebook », *supra* note 60.

CHAPITRE 4 – LA PROTECTION DES RENSEIGNEMENTS PERSONNELS EN EUROPE ET L'ACTUALISATION DE LA LPRPDÉ

Bien qu'elle procure certains outils pour contrer les impacts les plus pervers des pratiques de profilage comportemental sur Internet, il est clair, à la lumière de ce que nous avons vu dans le chapitre précédant, que l'approche canadienne en matière de protection des renseignements personnels fait défaut à plusieurs égards. Or, avant l'adoption de la LPRPDÉ au Canada, les pays membres de la communauté européenne possédaient déjà un encadrement visant la protection de la vie privée des individus dans le cadre des pratiques de collecte et d'utilisation de renseignements personnels les concernant[370]. Au cours des deux dernières décennies, l'Union européenne a également adopté des mesures portant directement sur la protection des renseignements personnels dans le domaine des communications électroniques et les nouvelles technologies d'information et de communication[371]. Dans le présent chapitre, nous aborderons les mesures adoptées par la communauté européenne en matière de protection de la vie privée dans le but d'établir quelles leçons les législateurs et les tribunaux canadiens peuvent tirer de l'expérience européenne, pour terminer en comparant celle-ci à la direction que semble vouloir prendre le gouvernement canadien dans ses efforts de modernisations de la LPRPDÉ.

---

[370] Les membres du Conseil de l'Europe ont adopté en 1980 la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, *supra* note 147. La *Convention* établit notamment que les données à caractère personnel faisant l'objet d'un traitement automatisé doivent être : obtenues et traitées loyalement et licitement; enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités; adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées; exactes et si nécessaire mises à jour; conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées; et protégées par des mesures de sécurité appropriées.

[371] Voir CE, *Directive 95/46/CE*, *supra* note 148; *infra* note 384.

4.1. L'approche de l'Union européenne

4.1.1. Les Directives *95/46/CE* et *2002/58/CE*

Alors qu'au Canada, la reconnaissance d'un droit constitutionnel à la vie privée s'est faite par interprétation, notamment dans l'affaire *Hunter c. Southam*[372], la loi constitutionnelle européenne, pour sa part, a reconnu la vie privée comme un droit fondamental dès 1950, avec la *Convention européenne des droits de l'homme*[373], de même que plus récemment avec la *Charte des droits fondamentaux de l'Union européenne*[374] de 2000. En Europe, ce n'est pas seulement la vie privée, mais également la protection des renseignements qui est considérée comme un droit fondamental. En effet, l'article 8 de la *Charte des droits fondamentaux de l'Union européenne*, indique que « [t]oute personne a droit à la protection des données à caractère personnel la concernant »[375].

Contrairement au droit constitutionnel canadien qui fonde le droit constitutionnel à la vie privée comme un droit individuel contre l'intrusion de l'État dans les affaires privées, le droit à la vie privée selon la constitution européenne est fondé sur la valeur de la dignité humaine[376]. La particularité de cette approche émane du fait que de la dignité est un concept social plutôt que politique. Ainsi, la protection de la dignité se traduit, dans une certaine mesure, comme la protection du statut et de l'image d'un individu dans une société plutôt qu'uniquement contre l'État[377]. Autrement dit, la dignité ne souffre pas autant des actions du

---

[372] *Hunter*, *supra* note 127.

[373] CE, *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, 213 R.T.N.U. 221, S.T.E. 5, art. 8 [Convention européenne des droits de l'homme].

[374] CE, *Charte des droits fondamentaux de l'Union européenne*, 7 décembre 2000, C 364/01, art. 7 et 8 [*Charte UE*]. Voir Tene, « What Google Knows », *supra* note 35 à la p. 1474.

[375] *Charte UE*, *ibid*. art. 8(1). Voir Tene, « What Google Knows », *supra* note 35 aux pp. 1474-5. On retrouve également cette notion dans la Convention européenne des droits de l'homme, qui indique au paragraphe 1 de son article 8 que [t]oute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance » [nous soulignons], ainsi qu'à l'article 7 de la Charte UE, qui indique similairement que « [t]oute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

[376] James Q. Whitman, « The Two Cultures of Privacy: Dignity Versus Liberty » (2004)113 Yale L.J. 1151, à la p. 1164; Matthew A. Chivvis, « Consent to Monitoring of Electronic Communications of Employees as an Aspect of Liberty and Dignity: Looking to Europe » (2009) 19 Fordham Intell. Prop. Media & Ent. L.J. 799, à la p. 817; Voir Tene, « What Google Knows », *supra* note 35 à la p. 1475.

[377] Avner Levin et Mary Jo Nicholson, « Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground » (2005) 2 U. Ottawa L. & Tech. J. 357, à la p. 388 [Levin et Nicholson, « Middle Ground »].

gouvernement, mais peut toutefois souffrir des pensées et des perceptions des autres membres de la société[378]. Si l'objectif de la protection de la vie privée est ultimement de protéger la dignité d'un individu, alors il est clair que la dignité doit être protégée en société et que les intrusions de l'État sont moins perçues comme une source d'inquiétude[379].

Ainsi, afin de mieux protéger les valeurs sous-jacentes à la vie privée des citoyens du continent européen, Conseil de l'Europe a adopté en 1995 la *Directive 95/46/CE*[380] afin d'harmoniser les lois en matière de protection des renseignements personnels entre les pays membres de l'Union européenne[381]. L'objet de la directive, aux termes de son article premier, est « la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel »[382]. Cette conception se distingue de l'approche canadienne en matière de protection des renseignements personnels dans le secteur privé qui, comme nous l'avons vu au chapitre 2, est davantage inspiré du modèle d'autoréglementation de l'Association canadienne de la normalisation que du droit fondamental. À ce jour, tous les pays membres de l'Union européenne ont inclus les exigences de la *Directive 95/46/CE* dans leurs lois internes en matière de protections des renseignements personnels[383]. Pour complémenter cette directive, le Conseil a adopté en 2002 la *Directive 2002/58/CE*[384] dont l'objet est de supplémenter la *Directive 95/46/CE* sur les questions techniques relatives à la communication électronique.

---

[378] *Ibid*., à la p. 388.
[379] *Ibid*., à la p. 389. Cette conception n'est cependant pas totalement étrangère au droit canadien, comme nous l'avons vu dans l'arrêt *R. c. Plant*, *supra* note 129 où la Cour suprême du Canada indique que la protection constitutionnelle du droit à la vie privée reconnue par les tribunaux canadiens s'articule principalement autour d'une conception de la vie privée qui repose sur les valeurs sous-jacentes de dignité, d'intégrité et d'autonomie.
[380] CE, *Directive 95/46/CE*, *supra* note 148.
[381] Mark F. Kightlinger, « Twilight of the Idols? EU Internet Privacy and the Post Enlightenment Paradigm » (2007-2008) 14 Colum. J. Eur. L. 1, à la p. 9 [Kightlinger « Twilight »]; Garrie et Wong, « Future of Web Data », *supra* note 34 à la p. 139.
[382] CE, *Directive 95/46/CE*, *supra* note 148 art. 1(1).
[383] Maria Tzanou, « Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection » (2010) 6 Croatian Y.B. Eur. L. & Pol'y 53, à la p. 57.
[384] CE, *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, [2002] J.O. L 201/37, en ligne : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:NOT> [*Directive 2002/58/CE*].

Pour mettre en œuvre les exigences contenues dans ces directives, l'article 28 de la *Directive 95/46/CE* établit que tous les États membres doivent prévoir une ou plusieurs autorités publiques chargées de surveiller l'application des dispositions de la *Directive* sur leurs territoires respectifs. Celles-ci doivent exercer « en toute indépendance les missions dont elles sont investies »[385]. Lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des renseignements personnels, les États membres doivent consulter les autorités de contrôle[386]. Les autorités de contrôle disposent d'une gamme de pouvoir, dont certains pouvoirs d'investigation, des pouvoirs effectifs d'intervention, ainsi que le pouvoir de porter en justice les cas de violation des dispositions nationales adoptées en vertu de la *Directive*[387]. Les autorités de contrôle peuvent également être saisies « par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel »[388]. De plus, l'article 29 de la *Directive* prévoit la création du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel (Groupe de travail). Le Groupe, dont le caractère est « consultatif et indépendant »[389], est composé d'un représentant de chacune des autorités désignées par les États membres, de représentant des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission[390].

4.1.2. La définition des renseignements personnels selon l'UE

En ce qui a trait au caractère des renseignements produit par des pratiques de profilage, nous avons vu que, selon l'interprétation des tribunaux canadiens et du CPVP, il demeure difficile à établir si de tels renseignements profitent toujours d'une protection en vertu de la LPRPDÉ. Selon l'approche européenne, les renseignements obtenus à partir du suivi des activités d'un individu sur Internet constituent-ils des renseignements personnels?

---

[385] CE, *Directive 95/46/CE*, *supra* note 148 art. 28(1)
[386] *Ibid*., art. 28(2).
[387] *Ibid*., art. 28(3).
[388] *Ibid*., art. 28(4).
[389] *Ibid*., art. 29(1).
[390] *Ibid*., art. 29(2). Voir Kightlinger, « Twilight », *supra* note 381 à la p. 11. Voir aussi CE, Groupe de travail « Article 29 », en ligne : < http://ec.europa.eu/justice/data-protection/article-29/index_fr.htm>, pour plus d'information concernant la constitution et le fonctionnement du Groupe de travail.

À la première lecture de la *Directive 95/46/CE*, on remarque qu'elle contient plusieurs dispositions qui traitent de la protection des renseignements personnels de façon similaire aux dispositions figurant à la LPRPDÉ canadienne. Or, une étude plus approfondie dévoile que la *Directive* comporte certaines dimensions qui la distinguent de l'approche de la Loi canadienne. D'abord, en ce qui concerne la définition d'un renseignement personnel, alors que la LPRPDÉ ne définit qu'abstraitement ce dernier à son article 2, la *Directive* offre, pour sa part, une définition plus détaillée des données personnelles :

> « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale […][391]

Le Groupe de travail soutient que l'expression « toute information » qui figure dans la définition de « données à caractère personnel » de la *Directive 95/46/CE* appelle à une interprétation large[392]. À son avis, on peut inclure à cette définition des renseignements autant de nature objective que subjective, telles une opinion ou une impression sur un individu, et même des renseignements qui ne sont pas totalement vrais ou prouvés[393]. De plus, le Groupe précise que cette définition inclut les renseignements sous tous les formats ou supports[394].

Ensuite, de manière similaire à l'interprétation de la Cour d'appel fédérale dans *Canada (Commissaire à l'information) c. Canada (Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports)*[395], le Groupe de travail stipule également qu'un renseignement personnel doit être un renseignement « concernant » un individu « identifiable ». Selon l'approche des pays de l'Europe, on peut considérer qu'une

---

[391] CE, *Directive 95/46/CE*, *supra* note 148 art. 2(a).
[392] CE, Groupe de travail « Article 29 » sur la protection des données, « Avis 4/2007 sur le concept de données à caractère personnel », 01248/07/FR, WP 136, à la p. 6, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf> [WP 136].
[393] *Ibid*., à la p. 7.
[394] *Ibid*.
[395] Arrêt *Transport*, *supra* note 244.

information concerne une personne lorsqu'elle *a trait* à celle-ci[396]. Pour le Groupe de travail, bien que certains types de renseignements soient facilement catégorisables comme « concernant » un individu, tels un examen médical ou une image filmée de l'individu, d'autres sont plus difficiles à déterminer, telles les informations découlant de données concernant un lieu ou un objet[397]. Dans de telles circonstances, il est possible de considérer que ces renseignements concernent un individu de manière indirecte. À cet effet, il est nécessaire d'évaluer dans son contexte le contenu, la finalité ou le résultat du renseignement en question afin de déterminer s'il « concerne » effectivement un individu[398]. En ce qui concerne le profilage sur Internet, le Groupe de travail considère que le *clickstream data* constitue une forme de renseignement personnel[399].

D'autre part, la *Directive 95/46/CE* établit qu'une donnée est « personnelle » lorsqu'elle concerne une personne « identifiée ou identifiable ». Selon l'approche européenne, cette notion signifie qu'il faut que le renseignement permette de distinguer un individu parmi tous les autres, ou qu'il soit possible de le faire avec l'information en question[400]. Aussi, l'identification peut se faire directement ou indirectement. Le Groupe de travail considère comme « directe » une identification faite à partir d'identifiants qui font directement référence à la personne concernée, tels le nom, le numéro de téléphone ou le passeport de celle-ci, alors qu'une identification est « indirecte » lorsqu'une personne est identifiée par la combinaison de différents identifiants qui, à eux seuls, ne permettent pas l'identification directe[401]. Dans tous les cas, le Groupe précise qu'il faut évaluer le degré de possibilité d'identification en fonction du contexte[402]. Malgré cela, les données pseudonymisées et codées, tel qu'on les retrouve généralement dans les dossiers utilisés par les moteurs de recherche, seront considérées comme des renseignements portant sur un

[396] WP 136, *supra* note 392 à la p. 10.
[397] *Ibid*.
[398] *Ibid*., aux pp. 10-11.
[399] CE, Groupe de travail « Article 29 » sur la protection des données, « Recommandation 1/99 sur le traitement invisible et automatique des données à caractère personnel sur l'Internet effectué par des moyens logiciels et matériels », 5093/98/FR, WP 17, en ligne :
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp17fr.pdf>. Voir Garrie et Wong, « Future of Web Data », *supra* note 34 à la p. 144.
[400] WP 136, *supra* note 392 à la p. 13.
[401] *Ibid*., à la p.14.
[402] *Ibid*., aux pp. 13-14.

individu si celui-ci peut être identifié indirectement[403]. Il semble donc que le test approprié selon l'approche européenne pour déterminer si un renseignement permet d'identifier un individu est simplement la « possibilité » d'identification, plutôt que « l'attente raisonnable » de l'affaire *Pascoe*[404] ou la « forte probabilité » de l'affaire *Gordon*[405] au Canada.

Aussi, de manière similaire aux principes 4.3.4 et 4.3.6 de l'annexe 1 de la LPRPDÉ, l'article 8 de la *Directive* établit une série de limites pour la collecte et le traitement de renseignements de nature plus sensible. À cet égard, la *Directive* indique que :

> 1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.
>
> 2. Le paragraphe 1 ne s'applique pas lorsque :
>
> a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée […][406]

Immédiatement, on constate que la plus grande distinction entre la définition offerte par la *Directive* et celle de la LPRPDÉ réside dans le fait qu'elle contient une liste très précise des renseignements considérés comme sensibles. Certes, il est possible d'affirmer que le fait d'offrir une définition trop précise, voir arbitraire, des catégories de renseignements considérés comme sensibles risque de limiter la possibilité d'interpréter le degré de sensibilité d'un renseignement en fonction du contexte[407]. Par contre, les catégories visées par la définition semblent, dans une certaine mesure, assez larges pour contenir un grand nombre de renseignements qu'un individu pourrait estimer délicat.

---

[403] *Ibid*., aux pp. 20-21.
[404] *Pascoe*, *supra* note 258.
[405] *Gordon*, *supra* note 262.
[406] CE, *Directive 95/46/CE*, *supra* note 148 art. 8.
[407] Kightlinger, « Twilight », *supra* note 381 à la p. 16.

En général, la *Directive 95/46/CE* cherche à limiter autant que possible le traitement des renseignements personnels de nature sensible à des fins de profilage ou de publicité comportementale. Cependant, selon le Groupe de travail, lorsque des fournisseurs de réseaux publicitaires décident néanmoins d'avoir recours à de telles pratiques, particulièrement en établissant des catégories de centres d'intérêt en fonction de renseignements sensibles, ceux-ci doivent se conformer aux dispositions de l'article 8 de la *Directive 95/46/CE*. Le Groupe précise que :

> […] si un fournisseur de réseau publicitaire traitait le comportement d'une personne physique afin de « la placer » dans une catégorie de centres d'intérêt indiquant une préférence sexuelle particulière, il effectuerait un traitement de données sensibles au sens de l'article 8 de la directive 95/46/CE.[408]

Il est donc clair que, selon l'approche européenne, quiconque désire faire la collecte et le traitement de ce type de renseignements à des fins de profilage ou de publicité doit obligatoirement mettre en place des mécanismes qui permettent d'obtenir « un consentement préalable exprès, distinct du consentement recueilli pour le traitement des données en général »[409].

4.1.3. L'obtention du consentement selon l'UE

Un autre aspect de l'approche européenne qui se distingue en partie de l'approche canadienne en matière de protection des renseignements personnels concerne la validité des moyens employés pour obtenir le consentement d'une personne concernée. Contrairement à la LPRPDÉ, la *Directive* offre une définition du consentement, qu'elle définit comme « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement »[410]. La pleine étendue de cette définition est mieux appréciée lorsque lue en lien avec certaines dispositions de la *Directive* concernant l'obtention du consentement. À ce sujet, l'article 7 spécifie que les États membres doivent prévoir dans leurs lois internes que le

---

[408] CE, Groupe de travail « Article 29 » sur la protection des données, « Avis 2/2010 sur la publicité comportementale en ligne », 00909/10/FR, WP 171, à la p. 23, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf> [WP 171].
[409] *Ibid*., à la p. 23.
[410] CE, *Directive 95/46/CE*, *supra* note 148 art. 2(h).

traitement de données à caractère personnel ne peut être effectué que si certaines conditions sont respectées, notamment que « la personne concernée a indubitablement donné son consentement »[411]. La *Directive 2002/58/CE* comporte également une disposition concernant la protection des renseignements personnels de nature privée dans le secteur des télécommunications[412].

Le Groupe de travail a reconnu que la complexité grandissante des pratiques de collecte de renseignements, des modèles d'affaires, des relations commerciales et des applications technologiques fait obstacle dans plusieurs cas à la capacité ou la volonté d'un individu de prendre la décision de contrôler l'utilisation et la communication de ses renseignements[413]. L'approche européenne semble également plus réaliste en ce qui a trait à la connaissance générale des individus moyens en ce qui concerne l'utilisation et le traitement des renseignements à leur sujet qui sont collectés sur Internet, ainsi en ce qui a trait à leurs habiletés techniques et leur compréhension des différentes technologies qui permettent ces pratiques, et celles qui permettent de protéger leur vie privée. Plutôt que de supposer que les individus font toujours des choix rationnels, informés et autonomes lorsqu'ils permettent à des organisations de collecter et utiliser leurs renseignements, le Groupe de travail reconnait, dans un avis traitant de la publicité comportementale en ligne, que les « personnes concernées moyennes ne sont pas au courant du traçage de leur comportement de navigation, des finalités de celui-ci, etc. »[414]. Comme le Groupe mentionne, dans le cadre de la publicité comportementale « il se peut que les utilisateurs ne

---

[411] *Ibid*., art. 7(a).

[412] CE, *Directive 2002/58/CE*, *supra* note 384 art. 5(3) : Les États membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

[413] CE, Groupe de travail « Article 29 » sur la protection des données, « Opinion 15/2011 on the definition of consent », 01197/11/EN, WP 187, à la p. 10, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>, [WP 187].

[414] WP 171, *supra* note 408 à la p. 16.

connaissent pas ou ne comprennent pas la technologie sur laquelle repose la publicité comportementale, ni même qu'ils sont ciblés par ce type de publicité »[415].

L'approche européenne met également de l'emphase sur la nécessité d'obtenir le consentement de la personne concernée, ainsi que de l'informer des fins de cette collecte ou traitement, *avant* que ses renseignements soient collectés ou traités. Cette approche se distingue clairement de l'approche canadienne qui nécessite seulement que les organisations fassent un effort raisonnable pour informer les individus concernés et permet l'obtention du consentement au moment de la collecte[416]. Par exemple, l'approche européenne exige que, pour assurer que le consentement pour la collecte et le traitement des renseignements personnels à des fins de publicité comportementale soit valide, il faut également que l'utilisateur soit adéquatement informé « de l'identité du fournisseur de réseau publicitaire et des finalités du traitement »[417]. À cet égard, le Groupe adresse spécifiquement les pratiques de profilage en ligne, en soutenant que :

> [l]a personne concernée doit être clairement informée que le cookie permettra au fournisseur de réseau publicitaire de collecter des informations sur la consultation d'autres sites web, les publicités qui ont été affichées, celles sur lesquelles elle a cliqué, le moment, etc.
>
> Il devrait être expliqué en termes simples que le cookie servira à constituer des profils destinés à la diffusion de publicités ciblées. […] Des mentions telles que « *les annonceurs et d'autres tiers peuvent également utiliser leurs propres cookies ou balises* » sont clairement insuffisantes.[418]

Selon l'approche européenne, il est nécessaire que les organisations qui cherchent à obtenir le consentement d'un individu pour traiter ses renseignements personnels communiquent à ce dernier les fins mentionnées ci-haut de la manière « la plus conviviale possible »[419]. À cet égard, le Groupe de travail met l'emphase sur l'importance d'assurer que ces informations soient « aisément accessibles », mais aussi « extrêmement visibles »[420]. Par conséquent, selon la *Directive 95/46/CE*, « ces informations essentielles ne peuvent donc pas être cachées

---

[415] *Ibid*., à la p. 21.
[416] LPRPDÉ, *supra* note 8 ann. 1, art. 4.3.1, 4.3.2.
[417] WP 171, *supra* note 408 à la p. 21.
[418] *Ibid.*
[419] CE, *Directive 95/46/CE*, *supra* note 148 considérant 25.
[420] WP 171, *supra* note 408 à la p. 21.

dans des conditions générales et/ou dans des déclarations sur la politique de confidentialité »[421]. Ainsi, le Groupe estime qu'il est essentiel :

> […] que les fournisseurs de réseaux publicitaires trouvent des moyens d'informer *régulièrement* les utilisateurs que le suivi est en cours. À moins que des rappels clairs et non équivoques, recourant à des moyens simples, ne soient adressés aux personnes concernées, il est très probable qu'après un certain temps, ces dernières auront oublié que le suivi se poursuit et qu'elles y ont consenti.[422]

Par ailleurs, comme nous l'avons mentionné dans le chapitre précédent, l'une des approches que pourrait adopter le gouvernement canadien pour éviter toute ambigüité dans l'application de LPRPDÉ serait d'imposer l'obtention d'un consentement explicite pour toute collecte et utilisation de tous renseignements personnels[423]. C'est en partie l'approche qu'a favorisé l'Union européenne dans sa *Directive 95/46/CE*, qui exige les États membres incluent dans leurs lois concernant la protection des renseignements personnels des dispositions qui prévoient que le traitement de « données à caractère personnel » peut seulement être effectué lorsque l'individu concerné « a indubitablement donné son consentement »[424].

Comme l'indique le Groupe de travail de l'article 29, il n'est pas toujours clair ce qui constitue un véritable consentement « indubitable ». Certains utilisateurs des renseignements exploitent cette incertitude en utilisant des méthodes qui ne sont pas adéquates pour permettre l'obtention d'un vrai consentement indubitable. Cependant, l'utilisation de telles méthodes contrevient directement aux dispositions de la *Directive 95/46/CE*[425]. Le Groupe mentionne que le consentement peut parfois servir en tant que fondement pour justifier la

---

[421] *Ibid.*
[422] *Ibid.,* à la p. 22. Cette approche s'apparente en partie à celle privilégiée par le CPVP dans le Rapport « Profilage », *supra* note 2 à la p. 30, lorsqu'il indique que : « [l]a LPRPDÉ exige que les organisations soient transparentes au sujet de leurs politiques et pratiques. Les renseignements fournis aux consommateurs sur le suivi et le ciblage en ligne sont, bien souvent, trop complexes ou constituent du jargon juridique. Souvent, les personnes ne souhaitent pas lire les avis concernant la protection de la vie privée, lesquels n'offrent la plupart du temps que deux choix : les accepter ou les refuser. Même s'ils sont bien écrits et faciles à comprendre, il faudrait trouver des façons d'encourager les gens à les lire ».
[423] Arthur J. Cockfield, « Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance » (2003) 29 Queen's L.J. 364, à la p. 399.
[424] CE, *Directive 95/46/CE*, *supra* note 148 art. 7(a).
[425] WP 187, *supra* note 413 à la p. 10.

collecte et le traitement des renseignements personnels. Or, il perd de sa valeur lorsqu'il est étiré et altéré pour répondre à des situations pour lesquelles il n'a pas été conçu[426]. C'est pourquoi, selon l'approche européenne, l'utilisation du consentement dans le bon contexte est cruciale. Lorsqu'utilisé dans des circonstances inappropriées, par exemple dans les cas où il est peu probable que les éléments constituant la validité du consentement soient présents, la position de l'individu est particulièrement affaiblie[427].

Aussi, l'approche prescrite par la *Directive 95/46/CE* semble répondre plus adéquatement aux questions relatives à la forme du consentement qui doit être obtenu. À cet égard, le Groupe de travail reconnait que, dans certaines circonstances, l'absence d'un comportement, ou un comportement passif peut être interprété comme une manifestation du consentement. Toutefois, malgré la largeur de la notion de « manifestation » telle qu'incluse dans la définition du « consentement » de la *Directive 95/46/CE*, celle-ci semble néanmoins supposer la présence d'une action quelconque[428]. Par exemple, le besoin que la personne concernée « accepte » que ses renseignements soient utilisés semble indiquer que la simple inaction est insuffisante et qu'une forme d'action est requise pour constituer un consentement[429]. Sur ce point, le Groupe indique qu'il est « fallacieux de considérer que, de manière générale, l'absence d'action de la personne concernée […] est une manifestation claire et sans équivoque de sa volonté »[430].

De surcroît, il semble que l'approche européenne tend à reconnaitre une importance plus marquée pour l'obtention d'un consentement explicite et positif pour la collecte et l'utilisation de renseignements personnels à des fins de profilage et de publicité. Bien que le Groupe de travail considère que les mécanismes d'« opt-out » sont les bienvenus et doivent être encouragés puisqu'ils permettent plus facilement aux individus concernés de refuser les publicités, il soutient que « ces mécanismes n'expriment pas un consentement des personnes

[426] *Ibid.*
[427] *Ibid.*, à la p. 10.
[428] *Ibid.*, à la p. 12.
[429] *Ibid.*
[430] *Ibid.*, à la p. 16.

concernées »[431]. Ainsi, sur la question du profilage Internet à l'aide de cookies, le Groupe soutient que :

> [c]e n'est que dans des cas individuels très spécifiques que l'on pourrait parler de consentement implicite, par exemple lorsqu'un utilisateur expérimenté, qui est informé de la pratique de la publicité comportementale, sait qu'il peut la refuser mais choisit de poser l'acte volontaire de ne pas le faire (en particulier, s'il le fait avant qu'un cookie ne lui ait été envoyé).[432]

Le Groupe indique toutefois que le mécanisme de « opt-out » ne convient pas pour obtenir un consentement informé de « l'utilisateur moyen » pour deux raisons. D'abord, il soutient que les utilisateurs d'Internet ne sont généralement pas au courant que leurs renseignements sont collectés et utilisé, ni comment fonctionnent les technologies derrière ces pratiques et, surtout, ils ne connaissent par comment procéder pour retirer leur consentement par un « opt-out ». À cet effet, le Groupe reconnait que très peu d'individus exercent cette option « non parce qu'ils ont décidé, en toute connaissance de cause, d'accepter les publicités comportementales, mais parce qu'ils ne se rendent pas compte qu'en ne procédant pas à un «opt-out», ils acceptent en fait ces publicités »[433]. Ensuite, il rappelle que le consentement implique une participation active de l'individu concerné avant que toute collecte de ses renseignements ait lieu. Toutefois, dans un mécanisme d'« opt-out », le consentement de l'individu concerné est souvent déduit de sa non-réaction. Pour le Groupe, un tel consentement implicite ne satisfait pas aux conditions de l'article 5(3) de la *Directive* pour obtenir un consentement valable.

C'est pourquoi le Groupe de travail soutient que les mécanismes d'« opt-in », qui requièrent une « action positive de la personne concernée pour manifester son consentement », répondent mieux aux exigences des directives *95/46/CE* et *2002/58/CE*[434]. Comme il l'a mentionné dans un avis portant sur l'avenir du droit à la vie privée :

---

[431] *Ibid*., à la p. 18. Toutefois, l'utilisation des renseignements sensibles nécessite obligatoirement l'obtention du consentement explicite selon l'article 8 de la *Directive 95/46/CE*. Dans ces situations, la forme « opt-in » est la plus appropriée. Voir Kightlinger, « Twilight », *supra* note 381 à la p. 17

[432] WP 187, *ibid*.

[433] *Ibid*., à la p. 18.

[434] Dans le contexte canadien, le CPVP a adopté une position similaire. Voir CPVP, Rapport « Profilage », *supra* note 2 à la p. 29, où le CPVP indique qu'il « a toujours considéré que le « consentement positif »

> Les évolutions technologiques invitent également à un examen attentif du consentement. En pratique, l'article 7 de la directive 95/46/CE n'est pas toujours correctement appliqué, en particulier dans le contexte de l'internet, où un consentement implicite ne conduit pas toujours à un consentement non équivoque [comme le prévoit l'article 7, point a), de la directive]. Pour permettre aux personnes concernées de s'exprimer davantage en amont du traitement de leurs données à caractère personnel, il faut que le consentement soit donné explicitement (il faut par conséquent un accord préalable) pour l'ensemble du traitement basé sur le consentement.[435]

Le Groupe reconnait toutefois qu'il y a certains problèmes associés à la nécessité de toujours obtenir un consentement positif dans certains contextes. Par exemple, l'obligation d'obtenir un consentement explicite chaque fois qu'un cookie est utilisé pour de la publicité ciblée ne serait pas praticable. Il reconnait donc la nécessité de permettre que l'acceptation d'un cookie par l'utilisateur soit interprétée « comme valable non seulement pour l'envoi du cookie, mais aussi pour la collecte ultérieure de données provenant de ce cookie ». Or, pour limiter les abus liés à l'utilisation de ces méthodes, le Groupe propose l'implantation de certaines mesures, dont la limitation de la portée du consentement à un an, l'implantation de mesures d'information supplémentaires, et la possibilité de révoquer le consentement en tout temps[436].

4.2. L'actualisation de la LPRPDÉ

À la lumière de ce que nous avons vu dans la section précédente, on peut conclure que l'approche européenne, bien que peu différente de l'approche canadienne en ce qui concerne sa portée, semble néanmoins mieux articulée et plus contraignante à certains égards. Dans le but d'actualiser la LPRPDÉ en réponse à la menace grandissante de certaines pratiques associées à l'utilisation des nouvelles technologies d'information et de communication, le gouvernement du Canada a déposé en première lecture devant la Chambre des communes, un projet de loi visant la modification de certaines dispositions de

---

(explicite) était la méthode de consentement privilégiée, même si le « consentement négatif » peut être acceptable dans certaines situations ».

[435] CE, Groupe de travail « Article 29 » sur la protection des données et Groupe de travail « Police et justice », *L'avenir de la protection de la vie privée – Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel*, WP 168, à la p. 19, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_fr.pdf>.

[436] WP 187, *supra* note 413 à la p. 18.

la LPRPDÉ[437]. Bien qu'il soit mort au Feuilleton lorsque le Parlement a été dissout en mars 2011, le projet de loi C-29 illustre bien la direction future que veut prendre le gouvernement canadien en matière de protection des renseignements personnels.

Parmi les modifications proposées par ce projet de loi, on compte une modification substantielle à la définition de « renseignement personnel », qui lirait « Tout renseignement concernant un individu identifiable », supprimant ainsi la partie excluant le nom et le titre d'un employé d'une organisation et l'adresse et le numéro de téléphone de son lieu de travail. Cette dernière est plutôt reléguée au sens plus général de l'article 4.01, également rajouté par le projet de loi C-29, qui crée une exception à la loi pour certains types de renseignements dans le contexte des affaires[438].

Ensuite, l'une des dispositions proposées les plus intéressantes pour la question du profilage comportemental serait l'ajout de l'article 6.1, qui imposerait des conditions plus contraignantes pour obtenir un consentement valide de la part des individus pour la collecte, l'utilisation et la communication de leurs renseignements personnels :

> Pour l'application des articles 4.3 à 4.3.8 de l'annexe 1, le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce que ce dernier comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti.

De toute évidence, cette disposition serait un ajout considérable à la protection offerte par la LPRPDÉ en ce qui concerne la collecte et l'utilisation des renseignements personnels sur Internet. En effet, on peut supposer que cette disposition rendrait plus difficile aux organisations d'obtenir un consentement de la part d'un individu à partir d'ententes contractuelles trop vagues et trop larges. En plaçant l'emphase sur la nécessité de clarifier « la nature, les fins et les conséquences » liées au traitement des données, les organisations seraient vraisemblablement contraintes à spécifier aux utilisateurs comment les

---

[437] P.L. C-29, *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, 3e sess., 40e lég., 2010 (première lecture le 25 mai 2010).

[438] *Ibid*., art. 4 : « 4.01 La présente partie ne s'applique pas à une organisation à l'égard des coordonnées d'affaires d'un individu qu'elle recueille, utilise ou communique uniquement pour entrer en contact – ou pour faciliter la prise de contact – avec lui dans le cadre de son emploi, de son entreprise ou de sa profession ».

renseignements collectés à leur sujet peuvent être compilés pour créer des profils comportementaux. À la lumière de ce que nous avons discuté dans la section précédente, cette modification de la LPRPDÉ représente certainement un pas dans la bonne, mais elle semble tout de même faible lorsqu'on la compare à la notion qui vise à assurer que les informations relatives aux fins de l'utilisation des renseignements soient « aisément accessibles », mais aussi « extrêmement visibles », tel que recommande l'approche européenne[439].

Toutefois, malgré ces apparentes améliorations de la LPRPDÉ, certaines modifications incluses dans le projet de loi C-29 concernant la collecte, l'utilisation et la communication de renseignements sans le consentement de l'intéressé sont formulées d'une façon qui ouvre la porte à une interprétation très large en faveur des organisations. En effet, le projet de loi propose l'ajout de l'article 7.1, qui stipule au paragraphe 1 que les organisations qui sont parties à une éventuelle transaction commerciale peuvent utiliser et communiquer des renseignements personnels à l'insu de l'intéressé ou sans son consentement si à la fois :

> a) elles ont conclu un accord aux termes duquel l'organisation recevant des renseignements s'est engagée :
>
> > (i) à ne les utiliser et communiquer qu'à des fins liées à la transaction,
> >
> > (ii) à les protéger au moyen de mesures de sécurité correspondant à leur degré de sensibilité,
> >
> > (iii) si la transaction n'a pas lieu, à les remettre à l'organisation qui les lui a communiqués ou à les détruire, dans un délai raisonnable;
>
> b) les renseignements sont nécessaires pour décider si la transaction aura lieu et, le cas échéant, pour l'effectuer.

Aussi, le paragraphe 2 de cet article établi que si la transaction commerciale est déjà effectuée, les organisations qui en font parties peuvent utiliser et communiquer les

[439] WP 171, *supra* note 408 à la p. 21.

renseignements personnels, communiqués en vertu du paragraphe 1, à l'insu de l'intéressé ou sans son consentement dans le cas où :

> a) elles ont conclu un accord aux termes duquel chaque organisation s'est engagée :
>
> > (i) à n'utiliser et ne communiquer les renseignements dont elle a la gestion qu'aux fins auxquelles ils ont été recueillis ou auxquelles il était permis de les utiliser ou communiquer avant que la transaction ne soit effectuée,
> >
> > (ii) à les protéger au moyen de mesures de sécurité correspondant à leur degré de sensibilité,
> >
> > (iii) à donner effet à tout retrait de consentement fait en conformité avec l'article 4.3.8 de l'annexe 1;
>
> b) les renseignements sont nécessaires à la poursuite de l'entreprise ou des activités faisant l'objet de la transaction;
>
> c) dans un délai raisonnable après que la transaction a été effectuée, l'une des parties avise l'intéressé du fait que la transaction a été effectuée et que ses renseignements personnels ont été communiqués en vertu du paragraphe (1).

Le projet de loi prévoit aussi l'ajout de l'article 7.3, qui stipule que l'organisation peut, dans les cas visés aux paragraphes ci-haut, utiliser et communiquer un renseignement personnel à des fins autres que celles auxquelles il a été recueilli.

Si l'on se fit à la définition de « transaction commerciale » que propose le projet de loi C-29, force est de constater que celle-ci semble viser plus particulièrement les transactions issues de l'acquisition d'une entreprise ou d'une partie des actifs d'une société commerciale :

> « transaction commerciale » S'entend notamment des transactions suivantes :
>
> > a) l'achat, la vente ou toute autre forme d'acquisition ou de disposition de tout ou partie d'une organisation, ou de ses éléments d'actif;

> b) la fusion ou le regroupement d'organisations;
>
> c) le fait de consentir un prêt à tout ou partie d'une organisation ou de lui fournir toute autre forme de financement;
>
> d) le fait de grever d'une charge ou d'une sûreté les éléments d'actif ou les titres d'une organisation;
>
> e) la location d'éléments d'actif d'une organisation, ou l'octroi ou l'obtention d'une licence à leur égard;
>
> f) l'arrangement entre des organisations pour la poursuite d'activités d'affaires autres que le traitement de renseignements personnels visé à l'article 4.1.3 de l'annexe 1.

Or, le libellé de cette disposition permet d'établir, par l'insertion du terme « notamment », que cette liste n'est pas exhaustive. Conséquemment, il n'est pas impensable que dans ce contexte certaines organisations chercheraient à interpréter les articles 7.1 et 7.3 de façon à rendre plus permissives les dispositions de la LPRPDÉ concernant la nécessité d'obtenir le consentement. En effet, l'expression « transaction commerciale » ne se limite pas, dans le langage courant, aux transactions visées par la définition du projet de loi C-29. Le *Black's Law Dictionary* définit cette expression comme « une action qui à une influence les intérêts financiers ou économiques d'un acteur, incluant la création d'un contrat » [notre traduction][440].

Compte tenu de ce qui précède, il est essentiel que les efforts mis de l'avant pour modifier la portée de la LPRPDÉ, notamment avec la profusion des nouvelles technologies permettant la création de profils individuels de consommateurs et d'utilisateurs de services sur Internet, soient le plus clair que possible afin d'éviter que les organisations interprètent ces dispositions comme une forme de licence à la collecte et à l'utilisation de renseignements personnels.

[440] *Black's Law Dictionary*, 8e éd., *s.v.* « Business transaction » (An action that affects the actor's financial or economic interests, including the making of a contract).

CONCLUSION

Alors que les tribunaux cherchent désespérément à formuler une approche efficace et équilibrée pour assurer la protection de la vie privée et des renseignements personnels des individus, tout en garantissant que les intérêts des organisations soient aussi pris en compte, les pratiques visant la compilation de nombreux fragments d'information recueillis à propos d'un individu pour créer des profils comportementaux à son sujet à des fins de marketing et de publicité ne cessent de prendre de l'ampleur[441]. Les organisations du secteur privé dédiées à la collecte et au traitement des renseignements personnels de millions d'individus ne sont plus simplement les « Little Brothers » qu'ils furent à une époque. En effet, les moyens technologiques qui sont à leur disposition font en sorte que ces organisations sont dorénavant plus « Big » que « Big Brother » lui-même.

Comme nous l'avons mentionné au troisième chapitre, l'un des obstacles à la protection efficace contre ces pratiques réside dans le fait que la classification des renseignements compilés, fabriqués ou déduits à partir d'une multitude de données collectées par une organisation à partir des activités en ligne d'un individu se situe dans une zone grise de la loi. Les lois canadiennes en matière de protection des renseignements personnels dans le secteur privé ne sont pas spécifiques quant à la forme que doivent prendre les renseignements pour être considérés « personnels »[442]. Parallèlement, les tribunaux ne sont toujours pas arrivés à un consensus précis sur le seuil que doivent franchir les renseignements pour jouir d'une pleine protection en vertu de ces lois[443]. Cela pose encore plus de difficulté dans le contexte du profilage comportemental et de la collecte de renseignements sur Internet, puisque, comme nous l'avons discuté, ces renseignements sont par nature difficiles à catégoriser.

D'autre part, malgré la présence dans les lois en matière de protection des renseignements personnels de nombreuses dispositions portant sur la nécessité d'obtenir le consentement de l'individu concerné pour toute collecte, utilisation et communication de ses

[441] FTC, « Protecting Consumer Privacy », *supra* note 1 à la p. 23.
[442] Voir *supra* sous-section 3.1.1.
[443] Scassa, « Geographical », *supra* note 121 à la p. 212. Voir *Pascoe*, *supra* note 258; *Gordon*, *supra* note 262.

renseignements personnels, les organisations qui emploient des techniques de profilage comportemental ont très peu de difficulté à se servir du consentement comme une carte blanche qu'ils obtiennent par voie d'ententes contractuelles en ligne dont la validité peut très souvent être remise en question. Par souci de pragmatisme et de nécessité, les tribunaux perpétuent la notion selon laquelle ces pratiques font partie des intérêts légitimes des organisations qui doivent être mis en équilibre avec les intérêts des individus de protéger leur vie privée[444]. Or, comme nous l'avons vu, il n'est pas toujours clair que ce pari est véritablement équitable pour les particuliers.

Pour assurer que le droit à la vie privée résiste à l'émergence de nouvelles technologies capables de s'immiscer dans le plus profond de nos vies, il est impératif que nous repensions notre approche à l'égard de la protection de la vie privée et des renseignements personnels de façon à rendre compte du contexte dans lequel ils seront obtenus, utilisés ou communiqués. Mais, plus fondamentalement, il est important que les tribunaux, lorsqu'ils font le poids entre les intérêts des organisations et la vie privée des individus, incorporent dans leur évaluation les conséquences véritables sur la vie des individus que risque d'entrainer la surveillance constante des activités en ligne par des organisations du secteur privé.

Pourtant, la protection législative assurée par la LPRPDÉ comporte de nombreuses dispositions qui permettent aux individus de préserver un certain contrôle sur la façon par laquelle seront collectés et communiqués les renseignements qui les concernent[445]. À cet égard, la véritable faiblesse de l'approche canadienne c'est qu'elle suppose à tort que les individus font toujours des choix éclairés et rationnels lorsque vient le temps d'aliéner une partie de leur contrôle sur ces renseignements[446]. Sur cette question précise, l'approche européenne, qui impose aux organisations d'obtenir un consentement « indubitable » avant

[444] Voir *Englander*, *supra* note 145.
[445] Voir *supra* sous-section 2.2.2.
[446] Voir Kerr et al., « Soft Surveillance », *supra* note 319. Voir aussi Gautrais, « E-Consent », *supra* note 339; Barnhizer, « Propertization », *supra* note 340.

toute collecte ou utilisation des données[447], semble mieux adaptée pour faire face aux problèmes associés aux pratiques de profilage sur Internet.

Quoi qu'il en soit, il serait peu raisonnable de s'attendre à ce que nos vies demeurent complètement « privées » en cette ère de l'information. Le montant de renseignements qui est nécessaire au bon fonctionnement des technologies d'information et de communication comme Internet implique qu'une partie de nos activités en ligne sera collectée d'une manière ou d'une autre tant et aussi longtemps que nous l'utiliserons[448]. Toutefois, cela ne signifie pas que nous devons cesser toute tentative de protéger nos renseignements personnels contre les pratiques abusives. Plutôt, cela démontre la nécessité de mettre en place un modèle de protection de la vie privée et des renseignements personnels qui permet de distinguer plus adéquatement les pratiques qui portent atteinte à notre attente « véritable » de vie privée, de celles qui sont inoffensives ou nécessaires.

Mais, une telle actualisation du droit canadien en matière de vie privée doit nécessairement passer par une révision des lois sur la protection des renseignements personnels. Comme l'a mentionné le juge LaForest de la Cour suprême du Canada dans l'arrêt *R. c. Wong*, en référence aux atteintes à l'article 8 de la *Charte* par l'utilisation de nouvelles technologies, il n'appartient pas aux tribunaux, mais bien au législateur d'établir les limites d'utilisation des technologies, « de même pour toute nouvelle technologie que les progrès de la science mettront à la disposition de l'État dans les années à venir »[449]. En matière de protection des renseignements personnels dans le secteur privé, le CPVP abonde dans le même sens que le juge LaForest lorsqu'il soutient que :

> […] la LPRPDÉ est neutre sur le plan de la technologie et se fonde sur les pratiques équitables de traitement de l'information; elle a donc su jusqu'à maintenant relever les défis associés à l'évolution de la technologie et des modèles opérationnels. Toutefois, nous sommes d'avis que des mesures supplémentaires pourraient être prises afin d'éviter les problèmes relatifs à la protection de la vie privée ou d'atténuer les effets des nouvelles technologies sur la protection de la vie privée en faisant du cadre de protection de la vie privée actuel une partie intégrante du développement de l'économie

[447] CE, *Directive 95/46/CE*, *supra* note 148 art. 7.
[448] Lessig, *Code 2.0*, *supra* note 24.
[449] *Wong*, *supra* note 132 par. 36.

> numérique. Il s'agit d'une étape essentielle si l'on souhaite respecter les attentes des Canadiennes et des Canadiens en matière de protection de la vie privée et maintenir la confiance envers la technologie. La protection de la vie privée est trop souvent négligée à l'étape de la conception et les réparations après coup peuvent être dispendieuses.[450] [Nous soulignons]

Bien que cette tâche puisse sembler ardue, il faut noter que le droit canadien possède une structure qui est, à plusieurs égards, très adéquate pour assurer la protection des renseignements personnels à plus long terme devant les pratiques de profilage et du suivi sur Internet. Or, l'efficacité à long terme de la LPRPDÉ et des autres lois similaires pour maintenir une protection adéquate envers ces pratiques repose essentiellement sur la capacité des gouvernements de colmater les brèches qui sont actuellement présentes dans ces lois, mais surtout de mettre en place les outils nécessaires pour prévenir celles qui s'ouvriront dans le futur au fur et à mesure qu'apparaissent les nouvelles technologies.

[450] CPVP, « Vie privée, confiance et innovation – Étayer l'avantage numérique du Canada. Observations du Commissariat à la protection de la vie privée du Canada présentées dans le cadre de la consultation sur la Stratégie sur l'économie numérique du Canada » (9 juillet 2010), à la p. 12, en ligne : <http://www.priv.gc.ca/information/pub/sub_de_201007_f.pdf>.

BIBLIOGRAPHIE

LÉGISLATION

Lois fédérales
Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5.
Loi sur la protection des renseignements personnels, L.R.C., 1985, c. P-21.
Loi sur l'accès à l'information et la protection de la vie privée, L.R.O. 1990, c. F.31.

Lois provinciales
Charte des droits et libertés de la personne, L.R.Q., c. C-12.
Code civil du Québec, L.Q., 1991, c. 64.
Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25.
Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.
Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1.
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1.
Personal Information Protection Act, S.A. 2003, c. P-6.5.
Personal Information Protection Act, S.B.C. 2003, c. 63.

Codes et règlements
Alberta Alta. Reg. 366/2003.
Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96.
Colombie-Britannique B.C. Reg. 473/2003.
Règlement précisant les renseignements auxquels le public a accès, DORS/2001-7.

Projets de loi
P.L. C-29, *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, 3e sess., 40e lég., 2010 (première lecture le 25 mai 2010).

Lois constitutionnelles
Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, c. 11.

JURISPRUDENCE

Cour suprême du Canada
Canada (Commissaire à l'information) c. Canada (GRC), 2003 CSC 8, [2003] 1 R.C.S. 66.
Compagnie H. J. Heinz du Canada Ltée c. Canada (Procureur général), 2006 CSC 13.
Dagg c. Canada (Ministre des Finances), [1997] 2 R.C.S. 403.
Hunter c. Southam, [1984] 2 R.C.S. 145.
Lavigne c. Canada (Commissariat aux langues officielles), [2002] A.C.S. no 55, 2002 CSC 53.
R. c. Dyment, [1988] 2 R.C.S. 417.
R. c. Gomboc, [2010] 3 R.C.S. 211, 2010 CSC 55.
R. c. Plant, [1993] 3 R.C.S. 281.
R. c. Tessling, [2004] 3 R.C.S. 432, 2004 CSC 67.
R. c. Wong, [1990] 3 R.C.S. 36, [1990] A.C.S. no 118.

Cours fédérales
Canada (Commissaire à l'information) c. Canada (Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports), [2006] A.C.F. no 704, 2006 CAF 157.
Eastmond c. Canadien Pacifique Ltée, [2004] A.C.F. no 1043, 2004 CF 852.
Englander c. Telus Communications Inc. [2005] 2 R.C.F. 572.
Gordon c. Canada (Ministre de la Santé), [2008] A.C.F. no 331, 2008 CF 258.

Johnson c. Bell Canada, [2009] 3 R.C.F. 67, 2008 CF 1086
Morgan c. Alta Flights (Charters) Inc., [2006] A.C.F. no 447, 2006 CAF 121.
Morgan c. Alta Flights (Charters) Inc., [2005] A.C.F. no 523, 2005 CF 421.
Nammo c. TransUnion of Canada Inc., [2010] A.C.F. no 1510, 2010 CF 1284.
Randall c. Nubodys Fitness Centres, [2010] A.C.F. no 823.
Rousseau c. Wyndowe, [2008] A.C.F. no 151, 2008 CAF 39.
Rousseau c. Wyndowe, [2006] A.C.F. no 1631, [2006] F.C.J. No. 1631.
Turner c. Telus Communications Inc., [2005] A.C.F. no 1981, 2005 CF 1601.
Wansink c. Telus Communications Inc., [2007] A.C.F. no 122, 2007 CAF 21.

Provinces
Cheskes v. Ontario (Attorney General), [2007] O.J. No. 3515, 87 O.R. (3d) 581, 159 C.R.R. (2d) 191.
Kanitz v. Rogers Cable Inc., (2002) 58 O.R. (3e) 299.
Leon's Furniture Ltd. v. Alberta (Information and Privacy Commissioner), [2011] A.J. No. 338, 2011 ABCA 94.
Ontario (Attorney General) v. Pascoe, [2002] O.J. No. 4300, 166 O.A.C. 88.
Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner), [2001] O.J. No. 4987, 154 O.A.C. 97, (*sub nom. Ontario (Attorney General) v. Pascoe*) 2001 CanLII 32755.
St-Arnaud v. Facebook inc., [2011] Q.J. No. 3161, 2011 QCCS 1506.
X. v. Le Groupe Jean-Coutu (PJC) inc., J.E. 2000AC-63 (C.Q.).

États-Unis
Boyd v. United States, (1886) 116 US 616.
Katz v. United States, (1967) 389 US 347.
Olmstead v. United States, (1928) 277 U.S. 438.

DOCTRINE : MONOGRAPHIES

Foucault, Michel. *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975.
Gandy, Oscar H. Jr. *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, Westview, 1993.
Garner, Bryan A., dir. *Black's Law Dictionary*, 8e éd., St. Paul, Thomson West, 2004.
Kerr, Ian, Steeves, Valerie, Lucock, Carole, dir. *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, New York, Oxford University Press, 2009.
Leenes, Ronald E., dir. *Constitutional Rights and New Technologies: A Comparative Study*, La Haye, T.M.C. Asser, 2008.
Lessig, Lawrence. *Code 2.0*, New York, Basic Books, 2006.
Lyon, David. *Surveillance Studies: An Overview*, Cambridge, Polity, 2007.
McIsaac, Barbara. Shields, Rick. Klein, Kris. *The Law of Privacy in Canada*, Toronto, Carswell, 2010.
Moore, Adam D. *Privacy Rights: Moral and Legal Foundations*, University Park, Pennsylvania University Press, 2010.
Murray, Andrew. *Information Technology Law*, Oxford, Oxford University Press, 2010.
Nissenbaum, Helen. *Privacy in Context.Technology, Policy, and the Integrity of Social Life*, Stanford, Stanford Univeristy Press, 2010.
Orwell, George. Nineteen Eighty-Four, London, Secker & Warburg, 1949
Pellemans, Paul. *Le marketing qualitatif : perspective psychoscopique*, Paris-Bruxelles, De Boeck & Larcier, 1998.
Rubin, Paul H. Lenard, Thomas M. *Privacy and the Commercial Use of Personal Information*, Boston, Kluwer, 2002.
Solove, Daniel J. *Understanding Privacy,* Cambridge, Harvard University Press, 2008.
——. *The Future of Reputation*, New Haven, Yale University Press, 2007.
——. *The Digital Person. Technology and Privacy in the Information Age*, New York et Londres, . New York University Press, 2004.
Solove, Daniel J., Rotenberg, Marc et Schwartz, Paul M. *Information Privacy Law*, 2e éd., New York, Aspen, 2006.

DOCTRINE : ARTICLES

Austin, Lisa M. « Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices » (2006-2007) 44 Can. Bus. L.J. 21.

——. « Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA », (2006) 56 Univ. of Toronto L.J. 181.

Balaban, Tanith L. « Comprehensive Data Privacy Legislation: Why Now is the Time », (2009) 1 Case W. Res. J.L. Tech. & Internet 1.

Barnhizer, Daniel D. « Propertization Metaphors for Bargaining Power and Control of the Self in the Information Age », (2006) Clev. St. L. Rev. 69.

Bergert, Dustin D. « Balancing Consumer Privacy with Behavioral Targeting », (2010-2011) 27 Santa Clara Computer & High Tech. L.J. 3.

Berzins, Christopher, « Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building », (2002) 27 Queen's L.J. 609.

Burdon, Mark. « Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws », [2010] J.L. Tech. & Pol'y 1.

Chivvis, Matthew A. « Consent to Monitoring of Electronic Communications of Employees as an Aspect of Liberty and Dignity: Looking to Europe », (2009) 19 Fordham Intell. Prop. Media & Ent. L.J. 799.

Cockfield, Arthur J. « The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government », (2003-2004) 1 U. Ottawa L. & Tech. J. 325.

——. « Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance », (2003) 29 Queen's L.J. 364.

Ciocchetti, Corey. « Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information », (2007-2008)10 Vand. J. Ent. & Tech. L. 553.

Ciocchetti, Corey et Sprague, Robert. « Preserving Identities: Protecting Personal Identifying Information through Enhanced Privacy Policies and Laws », (2009) 19 Alb. L.J. Sci. & Tech. 91.

Debusseré, Frederic. « The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? », (2005) 13 Int'l J.L. & Info. Tech. 70.

Doré, Lyette. « La législation canadienne sur la protection des renseignements personnels dans le secteur privé », dans Barreau du Québec, *Développement récents en droit de l'accès à l'information 2003*, Cowansville (Qc), Yvons Blais, 2003, 233.

Fairfield, Joshua A.T. « Anti-social Contracts: The Contractual Governance of Virtual Worlds », (2008) 53 R.D. McGill 427.

Garrie, Daniel B. et Wong, Rebecca. « The Future of Consumer Web Data: A European/US Perspective », (2006) 15:2 Int'l J.L. & I.T. 129.

Gautrais, Vincent. « The Colour of E-consent », (2003-2004) 1 UOLTJ 189.

Graham-Collins, Robert Todd. « The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat », (2009-2010) 44 Ga. L. Rev. 545.

Grimmelmann, James. « Privacy as Product Safety », (2009-2010) 19 Widener L.J. 793.

——. « Saving Facebook », (2009) 94 Iowa L. Rev. 1137.

Gandy, Oscar H. Jr. « Exploring Identity and Identification in Cyberspace », (2000) 14 Notre Dame J.L. Ethics & Pub. Pol'y 1085.

Gandy, Oscar H. Jr. « Toward a Political Economy of Personal Information », (1993) 10 CSMC 70.

Hilbert, Martin et López, Priscila . « The World's Technological Capacity to Store, Communicate, and Compute Information », (2011) 332:6025 Science 60.

Hillman, Robert A. et Rachlinski, Jeffrey J. « Standard-Form Contracting in the Electronic Age », (2002) 77 N.Y.U. L. Rev. 429.

Hirsch, Dennis D. « The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? », (2010-2011) 34 Seattle U. L. Rev. 439.

Holland, H. Brian. « Privacy Paradox 2.0 », (2009-2010) 19 Widener L.J. 893.

Hoofnagle, Chris Jay. « Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement », (2003-2004) 29 N.C. J. Int'l L. & Com. Reg. 595.

Hotaling, Andrew. « Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting », (2008) 16 CommLaw Conspectus 529.
Kang, Jerry. « Information Privacy in Cyberspace Transactions », (1997-1998) 50 Stan. L. Rev. 1193.
Kerr, Ian et al. «Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent », dans Ian Kerr, Valerie Steeves et Carole Lucock, dir., *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, New York, Oxford University Press, 2009, 5.
Kightlinger, Mark F. « Twilight of the Idols? EU Internet Privacy and the Post Enlightenment Paradigm », (2007-2008) 14 Colum. J. Eur. L. 1.
Lawson, Philippa et O'Donoghue, Mary. « Approaches to Consent in Canadian Data Protection Law » dans Ian Kerr, Valerie Steeves et Carole Lucock, dir., *Lessons From the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, New York, Oxford University Press, 2009, 23.
Levin, Avner et Nicholson, Mary Jo. « Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground », (2005) 2 U. Ottawa L. & Tech. J. 357.
Mackinnon, William. « Discarding Reasonable Expectations of Privacy: A Critique of R. V. Patrick », (2010) 47 Alta. L. Rev. 1037.
Marx, Gary. « Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information », dans T. Monahan, *Surveillance and Security: Technological Politics and Power in Everyday Life*, London, Routledge, 2006.
Matwyshyn, Andrea M. « Resilience: Building Better Users and Fair Trade Practices in Information », (2010-2011) 63 Fed. Comm. L.J. 391, à la p. 403.
McGeveran, William. « Disclosure, Endorsement, and Identity in Social Marketing », [2009] U. Ill. L. Rev. 1105.
Moffat, Viva R. « Regulating Search », (2008-2009) 22 Harv. J.L. & Tech. 475.
Ohm, Paul. « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », (2009-2010) 57 UCLA L. Rev. 1701.
——. « The Rise and Fall of Invasive ISP Surveillance », [2009] U. Ill. L. Rev. 1417.
Peek, Marcy. « The Observer and the Observed: Re-imagining Privacy Dichotomies in Information Privacy Law », (2009) 8 Nw. J. Tech. & Intell. Prop. 51.
Rubinstein, Ira S., Lee, Ronald D. et Schwartz, Paul M. « Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches », (2008) 75 U. Chi. L. Rev. 261.
Scassa, Teresa. « Geographical Information as "Personal Information" », (2011) 10:2 OUCLJ 183.
——. « Text and Context: Making Sense of Canada's New Personal Information Protection Legislation », (2000-2001) 32 Ottawa L. Rev. 1.
Schartum, Dag Wiese. « Designing and Formulating Data Protection Laws », (2008) 18:1 Int'l J.L. & I.T. 1.
Soma, John T., Courson, J. Zachary et Cadkin, John. « Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets », (2008-2009) 15 Rich. J.L. & Tech. 1.
Stallworth, Brian. « Future Imperfect: Googling for Principles in Online Behavioral Advertising », (2010) 62 Fed. Comm. L.J. 465.
Steeves, Valerie. « Reclaiming the Social Value of Privacy », dans Ian Kerr, Valerie Steeves et Carole Lucock, dir., *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, New York, Oxford University Press, 2009, 191,
Tene, Omer. « What Google Knows: Privacy and Internet Search Engines », [2008] Utah L. Rev. 1433.
Tindall, Craig D. « Argus Rules: The Commercialization of Personal Information », [2003] J.L Tech. & Pol'y 181.
Tzanou, Maria. « Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection », (2010) 6 Croatian Y.B. Eur. L. & Pol'y 53.
Warner, Jeremy. « The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps », (2005) 2:1 UOLTJ 75.
Warren, Samuel et Brandeis, Louis. « The Right to Privacy », (1890) 4 Harv. L. Rev. 193.
Whitman, James Q. « The Two Cultures of Privacy: Dignity Versus Liberty », (2004)113 Yale L.J. 1151.
Zimmer, Michael. « Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search », (2008) 3 J. Bus. & Tech. L. 109.

DOCUMENTS GOUVERNEMENTAUX

Alberta Information and Privacy Commissioner, « Report on the Investigation into Collection, Use and Disclosure of Customer Information, Re: EPCOR » (26 juillet 2004), P2004-IR-001, en ligne : <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2310>.

Bibliothèque du Parlement, *Les lois fédérales du Canada sur la protection de la vie privée* par Nancy Holmes, PRB 07-44F, révisé le 25 septembre 2008.

Commissariat à la protection de la vie privée du Canada, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2009-014, « La détection de la fraude n'est pas un motif acceptable pour recueillir des numéros de permis de conduire aux fins d'une adhésion à un magasin », <http://www.priv.gc.ca/cf-dc/2009/2009_014_0529_f.cfm>.

——, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2009-011, « Le conducteur d'un véhicule de transports en commun s'oppose à l'utilisation de technologies (MDT et GPS) à bord des véhicules d'entreprise », <http://www.priv.gc.ca/cf-dc/2009/2009_011_0527_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2009-009, « Plainte en vertu de la LPRPDÉ à l'égard d'Accuserach Inc. s/n Abika.com », en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009_009_rep_0731_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2009-008, « Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* », en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2009-004, « Aucun consentement n'est requis pour l'utilisation de renseignements personnels accessibles au public combinés à des statistiques démographiques propres à un lieu géographique », en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009_004_0109_f.cfm>.

——, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2009-001, « Contestation de la vidéosurveillance dans une station d'autobus par un employé de l'entreprise », <http://www.priv.gc.ca/cf-dc/2009/2009_001_0219_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2008-388, « Ticketmaster Canada Limited a révisé ses politiques et pratiques relativement à la LPRPDÉ en vue de protéger les renseignements personnels de ses clients », en ligne : <http://www.priv.gc.ca/cf-dc/2008/388_20080212_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2007-372, « Les communications aux courtiers en données exposent les faiblesses des mesures de sécurité en télécommunications », en ligne : <http://www.priv.gc.ca/cf-dc/2007/372_20070709_f.cfm>.

——, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2006-349, « Prise de photographies d'appartements de locataires sans leur consentement pour fins d'assurance », en ligne : <http://www.priv.gc.ca/cf-dc/2006/349_20060824_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2006-324, « Un consommateur se plaint de devoir fournir des pièces d'identité afin d'obtenir son rapport de solvabilité », en ligne : <http://www.priv.gc.ca/cf-dc/2006/324_20060109_f.cfm>.

——, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2005-296, « Remise en question du libellé du consentement et de l'activité de surveillance » en ligne : <http://www.priv.gc.ca/cf-dc/2005/296_050314_02_f.cfm>.

——, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2003-244, « Communication présumée de renseignements personnels sans consentement, à des fins commerciales secondaires, par la société de télécommunications « A » », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031107_02_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2003-242, « Un homme s'oppose à ce que des travailleurs assignés temporairement traitent les renseignements liés à la paye », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031204_06_f.cfm>.

——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2003-226, « L'entreprise recueille sans raison valable des renseignements médicaux; les mesures de sécurité sont insuffisantes », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031031_f.cfm>.

——, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2003-203, « Un particulier laisse percer ses inquiétudes quant aux clauses de consentement sur un formulaire de demande de carte de crédit » en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030805_01_f.cfm>.
——. Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2003-207, « Une entreprise de téléphones cellulaires satisfait aux conditions rattachées au consentement négatif », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030806_02_f.cfm>.
——. Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2003-162, « Un client se plaint de la présence de « témoins » sur le site Web d'une compagnie aérienne », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_7_f.cfm>.
——, Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ nº 2003-152, « Un câblodistributeur accusé de recueillir trop de renseignements personnels comme condition de service », en ligne : <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030414_2_f.cfm>.
——, Résumé de conclusions d'enquête en vertu de la LPRPDÉ nº 2002-83, « Communication alléguée sans consentement de renseignements personnels pour des fins secondaires de marketing par une banque », <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_1_f.cfm>.
——, Résumé de conclusion d'enquête en vertu de la LPRPDÉ n° 2002-42, « Air Canada permet à 1 % des membres Aéroplan de se « désister » des pratiques de partage d'information », en ligne : <http://www.priv.gc.ca/cf-dc/2002/cf-dc_020320_f.cfm>.
——, « Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique » (mai 2011), en ligne : <http://www.priv.gc.ca/resource/consultations/report_201105_f.pdf>.
——, « Vie privée, confiance et innovation – Étayer l'avantage numérique du Canada. Observations du Commissariat à la protection de la vie privée du Canada présentées dans le cadre de la consultation sur la Stratégie sur l'économie numérique du Canada » (9 juillet 2010), en ligne : <http://www.priv.gc.ca/information/pub/sub_de_201007_f.pdf>.
——, « Lignes directrices sur le traitement transfrontalier des données personnelles » (janvier 2009), en ligne : <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.cfm>.
——, « Outil d'autoévaluation – LPRPDÉ », en ligne : <http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_f.cfm>.
——, « Document d'information : La *Loi sur la protection des renseignements personnels et les documents électroniques* », en ligne : <http://www.priv.gc.ca/legislation/02_06_07_f.cfm>.
——, « Examen, prévu par la loi, de la Loi sur les renseignements personnels et les documents électroniques. Aperçu de la consultation du CPVP » (27 novembre 2006), en ligne : <http://www.priv.gc.ca/parl/2006/sub_061127_f.cfm#003>.

DOCUMENTATION INTERNATIONALE

Traités

Charte des droits fondamentaux de l'Union européenne, 7 décembre 2000, C 364/01.
Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950, 213 R.T.N.U. 221, S.T.E. 5.
Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, S.T.C.E. nº 108.

Directives et recommandations

CE, *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, [2002] J.O. L 201/37.
CE, *Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications*, [1998] J.O. L 24/1.
CE, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [1995] J.O. L 281/31.

Organisation de Coopération et de Développement Économiques (OCDE), *Annexe à la Recommandation du Conseil du 23 Septembre 1980 : Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, en ligne : ocde.org <http://www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html>.

——, *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée* (2007), en ligne : ocde.org <http://www.oecd.org/dataoecd/12/48/38876531.pdf>.

Autres

CE, Groupe de travail « Article 29 » sur la protection des données, « Opinion 15/2011 on the definition of consent », 01197/11/EN, WP 187, à la p. 10, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>.

——, « Avis 2/2010 sur la publicité comportementale en ligne », 00909/10/FR, WP 171, à la p. 23, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf>.

——, « Avis 4/2007 sur le concept de données à caractère personnel », 01248/07/FR, WP 136, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf>.

——, « Recommandation 1/99 sur le traitement invisible et automatique des données à caractère personnel sur l'Internet effectué par des moyens logiciels et matériels », 5093/98/FR, WP 17, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp17fr.pdf>.

CE, Groupe de travail « Article 29 » sur la protection des données et Groupe de travail « Police et justice », *L'avenir de la protection de la vie privée – Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel*, 02356/09/FR, WP 168, en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_fr.pdf>.

CE, « Groupe de travail « Article 29 » », en ligne : < http://ec.europa.eu/justice/data-protection/article-29/index_fr.htm>.

É.-U., Federal Trade Commission, Preliminary FTC Staff Report, « Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers » (1er décembre 2010), en ligne: <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

——, *Statement of Federal Trade Commission Concerning Google/DoubleClick* (FTC no 071-0170) 20 décembre 2007, en ligne : <http://www.ftc.gov/os/caselist/0710170/071220statement.pdf>.

——, « Summary of the US SAFE WEB Act », en ligne : ftc.gov <http://www.ftc.gov/reports/ussafeweb/Summary%20of%20US%20SAFE%20WEB%20Act.pdf>.

DOCUMENTS ÉLECTRONIQUES

Articles de journaux

Angwin, Julia et McGinty, Tom. « Sites Feed Personal Details to New Tracking Industry » *Wall Street Journal* (30 juillet 2010), en ligne : wsj.com <http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html>.

Bilton, Nick et Stelter, Brian. « Sony Says PlayStation Hacker Got Personal Data » (26 avril 2011), *New York Times*, en ligne : nytimes.com <http://www.nytimes.com/2011/04/27/technology/27playstation.html>.

Carlson, Nicholas. « Facebook Has More Than 600 Million Users, Goldman Tells Clients » (5 janvier 2011), *Business Insider*, en ligne : Businessinsider.com <http://www.businessinsider.com/facebook-has-more-than-600-million-users-goldman-tells-clients-2011-1>.

Womack, Brian. « Facebook 2010 Sales Said Likely to Reach $2 Billion, More Than Estimated » (16 décembre 2010), *Bloomberg*, en ligne : Bloomberg.com <http://www.bloomberg.com/news/2010-12-16/facebook-sales-said-likely-to-reach-2-billion-this-year-beating-target.html>.

Études et références

Bureau de la publicité interactive du Canada, « En 2010, les revenus de la publicité en ligne au Canada se sont élevés à 2,23 milliards de dollars, dépassant ceux de la publicité dans les quotidiens », en ligne : <http://www.iabcanada.com/fr/blogue/la-publicite-en-ligne-2010>.

Electronic Privacy Information Center, « ChoicePoint », en ligne : Epic.org <http://epic.org/privacy/choicepoint/>.

Les associés de recherche EKOS, Inc.**,** « les Canadiens et la vie privée » (mars 2009), en ligne : <http://www.priv.gc.ca/information/survey/2009/ekos_2009_01_f.pdf>.
Levin, Avner et al., « The Next Digital Divide: Online Social Network Privacy » (mars 2008), en ligne : <http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf>.
NetMarketShare, « Search Engine Market Share », en ligne : <http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4>.

Sites consultés

Acxiom, « Acxiom Announces Fourth Quarter and Fiscal Year 2010 Results », en ligne : Acxiom.com <http://www.acxiom.com/news/press_releases/2010/Pages/AcxiomAnnouncesFourthQuarterandFiscalYear2010Results.aspx>.
——, « Acxiom Announces New Canadian Data Centre », en ligne : Acxiom.com <http://www.acxiom.com/news/press_releases/2006/Pages/AcxiomAnnouncesNewCanadianDataCentre.aspx>.
Amazon, « Déclaration de confidentialité Amazon.ca », en ligne : Amazon.ca <http://www.amazon.ca/gp/help/customer/display.html?ie=UTF8&nodeId=918814>.
eBay, « Règlement sur le respect de la vie privée d'eBay », en ligne : eBay.ca <http://pages.cafr.ebay.ca/help/policies/privacy-policy.html>.
Equifax, « Industry-Specific », en ligne : Equifax.com <http://www.equifax.com/consumer/industry-specific/en_ca>.
Experian, « BehaviorBank Lifestyle Data », en ligne : experian.com <http://www.experian.com/marketing-services/targeted-consumer-marketing.html?cat1=customer-acquisition&cat2=target-prospects>.
——, « Company Profile », en ligne : Experian.com <http://www.experian.com/corporate/experian-profile.html>.
Facebook, « Statement of Rights and Responsibilities », en ligne : Facebook.com <http://www.facebook.com/terms.php>.
Google, « Terms of Service », en ligne : Google.ca <http://www.google.ca/accounts/TOS>.
——, « Règles de confidentialité », en ligne : Google.com <http://www.google.com/intl/fr/privacy/privacy-policy.html>.
——, « Technologie », en ligne : Google.ca <http://www.google.ca/intl/fr/corporate/tech.html>.
——, « Form 10-K, FY 2010 », en ligne : Google.com <http://investor.google.com/documents/20101231_google_10K.html>.
Infogroup, « Data Services », en ligne : Infogroup.com <http://www.infogroup.com/our-services/data-services.aspx>.
Transunion Canada, « Fast Facts », en ligne : Transunion.ca <http://www.transunion.ca/ca/aboutus/aboutus_en.page>.