

**La révision de la *Loi sur la protection
des renseignements personnels
et les documents électroniques* :**

Tout vient à point...

Observations présentées par Option consommateurs

**Au Comité permanent de l'accès à l'information, de la protection des
renseignements personnels et de l'éthique
de la Chambre des Communes**

11 mai 2017

Dépôt légal
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISBN : 978-2-89716-036-4

Option consommateurs
50, rue Ste-Catherine Ouest, Bureau 440
Montréal (Québec)
H2X 3V4
Téléphone : 514 598-7288
Télécopieur : 514 598-8511

Adresse électronique : info@option-consommateurs.org
Site Internet : www.option-consommateurs.org

Table des matières

Option consommateurs	iv
Résumé.....	v
1. Le propos	1
1.1 Le contexte	1
1.2 L'intervenante	2
1.3 Nos commentaires	2
2. Nos préoccupations	2
2.1 Des problématiques qui se compliquent	2
2.1.1 La diversification des pratiques	2
2.1.2 La valeur changeante des renseignements personnels	5
2.2 L'évolution des règles.....	6
2.2.1 La prévention	6
2.2.2 L'information	7
2.2.3 Le consentement	9
2.2.4 L'oubli	10
2.2.5 D'autres préoccupations	11
2.2.6 Les pouvoirs du Commissaire	11
3. Conclusions et recommandations	12
3.1 Envisager l'avenir	12
3.2 En attendant.....	14

Option consommateurs

MISSION

Option consommateurs est une association à but non lucratif qui a pour mission de promouvoir et de défendre les droits et les intérêts des consommateurs et de veiller à ce qu'ils soient respectés.

HISTORIQUE

Issue du mouvement des associations coopératives d'économie familiale (ACEF), et plus particulièrement de l'ACEF de Montréal, Option consommateurs existe depuis 1983. En 1999, elle a regroupé ses activités avec l'Association des consommateurs du Québec (ACQ) qui existait depuis plus de 50 ans et accomplissait la même mission qu'elle.

PRINCIPALES ACTIVITÉS

Option consommateurs aide les consommateurs qui vivent des difficultés, les reçoit en consultation budgétaire et donne des séances d'information sur le budget, l'endettement, le droit de la consommation et la protection de la vie privée.

Chaque année, nous réalisons des recherches sur des enjeux de consommation d'importance. Nous intervenons également auprès des décideurs et des médias pour dénoncer des situations inacceptables. Lorsque nécessaire, nous intentons des actions collectives (anciennement appelées recours collectifs) contre des commerçants.

Résumé

L'évolution de la société rend impérative la révision de la *Loi sur la protection des renseignements personnels et les documents électroniques* à laquelle procède présentement le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes. Afin de soutenir ce processus, nous brosserons une esquisse de certaines des difficultés qu'éprouvent les citoyens dans ce domaine, nous examinerons l'état et les carences de notre cadre normatif actuel en le comparant notamment, à certains égards, aux règles que s'apprête à mettre en œuvre l'Union européenne et nous formulerons des recommandations visant à la fois des modifications législatives et l'amélioration des programmes de recherche et d'information visant le domaine de la gestion des renseignements personnels.

Option consommateurs a été constituée en 1983. Cette association de consommateurs québécoise a vocation à aider les consommateurs qui éprouvent des difficultés, en leur fournissant de l'information et des conseils, en les représentant auprès des décideurs et en informant la population en général. Elle s'intéresse activement à la problématique de la protection des renseignements personnels depuis 1990.

Tant les types de renseignements personnels en circulation que les modes de traitement ou la nature des organisations qui utilisent ces renseignements sont présentement en mutation, dessinant de ce fait les contours d'un univers de plus en plus complexe, et que les citoyens comprennent de moins en moins. D'autre part, des renseignements personnels servent de plus en plus souvent de monnaie d'échange: on paie, en quelque sorte, en s'identifiant, et de plus en plus de modes de paiement requièrent qu'on s'identifie pour pouvoir les utiliser. Cette tendance soulève à terme un risque d'exclusion socio-économique qu'il faut dès maintenant appréhender.

Diverses mesures normatives peuvent minimiser les risques encourus par les citoyens. Au plan de la prévention, il faut intégrer les principes de protection des renseignements personnels dans la conception des dispositifs de gestion. Il faut informer mieux, et plus clairement. Il faut accorder plus de souplesse aux citoyens en matière de consentement, et contrer l'effet des clauses abusives qu'imposent trop d'organisations. Il faut s'attarder à des situations particulièrement délicates, comme les droits des enfants et le traitement des renseignements visant des personnes décédées. Le régime canadien pourrait d'autre part être amélioré en étendant son champ d'application et en accroissant sensiblement les attributions et les pouvoirs du Commissaire à la protection de la vie privée, qui devrait notamment pouvoir imposer des sanctions administratives pécuniaires dissuasives.

À plus long terme, il faudra aussi se pencher sur les fondements même de notre régime de gestion des renseignements personnels, établis en 1980 et qui ne correspondent peut-être plus tout à fait aux besoins du vingt-et-unième siècle.

Tout vient à point à qui peut attendre.
F. Rabelais, *Pantagruel*, livre 4, chapitre 48
(version originale)

1. Le propos

1.1 Le contexte

Sommes-nous encore autre chose qu'un assemblage de renseignements personnels plus ou moins cohérents? On se prend parfois à en douter, engoncés que nous sommes de plus en plus dans les traitements automatisés de codes auxquels entreprises et gouvernements nous réduisent afin de nous «mieux» gérer.

Le philosophe Giorgio Agamben le notait en 2009: notre identité ne s'établit désormais plus par notre «personne» sociale et sa reconnaissance, mais par des données (et notamment des données biométriques)¹. Qu'on s'y résigne ou non, force est de composer dans l'immédiat avec des pratiques informationnelles susceptibles de bouleverser nos vies; on tente du moins de les encadrer grâce à des règles fondées sur ce principe tout simple que la personne devrait pouvoir préserver un certain contrôle sur les renseignements qui la concernent et qui composent le «jumeau virtuel» que s'ingénient à régir les décideurs, faute d'avoir sur les personnes elles-mêmes l'emprise qu'ils souhaiteraient exercer.

Au Canada, ces règles s'incarnent notamment dans la *Loi sur la protection des renseignements personnels et les documents électroniques*, adoptée par le Parlement en 2000² et légèrement retouchée depuis lors. Le hic, c'est que la technologie et les pratiques sociales ont au cours des deux dernières décennies muté démesurément plus vite que le cadre législatif, qui se trouve par conséquent de plus en plus désuet. Pour aggraver les choses, les règles établies dans d'autres juridictions, et notamment au sein de l'Union européenne, évoluent également; or, globalisation oblige, les flux de données transfrontaliers se multiplient et il nous faut composer avec les droits et les obligations que déterminent d'autres États ou regroupements d'États.

La révision de la LPRPDÉ qu'opère présentement le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes (le «Comité») vient donc fort à point. Il est devenu urgent de revoir le cadre normatif entourant la protection des renseignements personnels des Canadiens. Il nous paraît toutefois, comme nous le noterons dans la section 3, que le processus actuel, si nécessaire-soit-il aux fins d'une mise à jour de ce cadre, ne suffira pas: à terme, il faudra vraisemblablement envisager une réforme beaucoup substantielle. Mais sans doute, à cet égard, devons-nous savoir attendre un peu...

¹ Agamben, Giorgio. *Nudités*. Bibliothèque Rivages. Paris, Payot, 2009. 192 p. Pp. 87-88.

² L.R.C., c. P-8.6, ci-après la «LPRPDÉ».

1.2 L'intervenante

Option consommateurs a été constituée en 1983. Cette association de consommateurs québécoise a vocation à aider les consommateurs qui éprouvent des difficultés, en leur fournissant de l'information et des conseils, en les représentant auprès des décideurs et en informant la population en général.

Option consommateurs s'intéresse activement à la problématique des renseignements personnels depuis 1990. Elle a, entre autres, contribué à l'adoption de la LPRPDÉ et à celle de la législation québécoise en matière de protection des renseignements personnels dans le secteur privé. Au cours des dernières années, elle a également réalisé un certain nombre de recherches soutenues financièrement par le Bureau de la consommation d'Innovation, Sciences et Développement économique Canada ou par le Commissariat à la protection de la vie privée du Canada.

1.3 Nos commentaires

Nous aborderons sommairement dans les prochaines pages deux ordres de questions. D'abord, dans la section 2.1, nous évoquerons certaines des tendances sociales et technologiques qui rendent nécessaire une révision du cadre normatif canadien en matière de protection des renseignements personnels détenus par des entreprises. Ensuite, dans la section 2.2, nous passerons brièvement en revue un certain nombre de problématiques spécifiques, qui ont trait notamment à la prévention, à l'information, au consentement, à l'oubli, au champ d'application et à la mise en œuvre des règles, et qui nous paraissent requérir à tout le moins des ajustements à notre régime juridique. Dans la section 3, en plus de formuler quelques recommandations spécifiques découlant de ces observations, nous soulèverons une question beaucoup plus fondamentale, à laquelle la présente révision législative ne répondra sans doute pas: le temps serait-il venu de repenser les fondements mêmes de nos régimes de protection des renseignements personnels? Pourrions-nous attendre vingt années de plus avant de réajuster le droit à nos besoins?

2. Nos préoccupations

2.1 Des problématiques qui se compliquent

2.1.1 La diversification des pratiques

La gestion des renseignements personnels devient de plus en plus délicate, en raison notamment d'un phénomène de diversification qu'on observe dans pratiquement toutes les sphères de la protection de ces renseignements. On le constate à maints égards.

D'abord, les types de renseignements qui font l'objet de collectes et de traitements se multiplient. Naguère, il s'agissait surtout de quelques identifiants (nom, adresse, numéro de carte de crédit...), associés à une donnée spécifique, comme le droit à une prestation ou l'exigibilité d'une dette, par exemple. Désormais, on recueille des données génétiques, des images, des données de géolocalisation, les déplacements du curseur de votre souris

sur une page web³, l'expression d'émotions, des données métaboliques⁴, la nature «amicale» de nos relations avec autrui, des opinions...; tout cela peut être archivé, recherché, analysé, utilisé pour prendre des décisions.

Pour tout compliquer, beaucoup partagent des dispositifs permettant l'accès à divers réseaux. L'ordinateur familial peut être utilisé par plusieurs; d'autres empruntent régulièrement le téléphone intelligent d'un ami ou d'un membre de la famille, par exemple⁵. Évidemment, rares sont ceux qui s'assurent de créer des profils distincts sur ces appareils; dans la mesure où des entreprises identifient régulièrement des appareils à des fins de profilage, plutôt que les usagers eux-mêmes, un utilisateur peut évidemment compromettre non seulement la protection de ses propres renseignements personnels, mais celle de tiers. Pensons par exemple à une jeune fille qui emprunte le téléphone intelligent de son aînée pour effectuer une recherche sur le web concernant l'avortement, en raison de la situation d'une amie; l'aînée, voyant que des sites lui proposent désormais certains liens, se doutera de la recherche faite par sa cadette, mais le père des deux sœurs, s'il effectue une inspection du téléphone, pourrait poursuivre de son courroux l'aînée, qui n'y est pourtant pour rien.

Les modes de pistage se diversifient également. On fournit souvent nos renseignements volontairement, mais il nous faut aussi composer avec des *cookies* et divers types de témoins qui s'établissent discrètement dans nos machines, avec des pixels invisibles sur les sites web que nous consultons⁶, avec les métadonnées que nous produisons inévitablement⁷... Les Canadiens comprennent en général assez mal comment tout cela fonctionne, et quel impact ces renseignements peuvent avoir⁸.

D'autre part, les traitements de renseignements personnels deviennent d'autant plus opaques que leurs utilisateurs recourent à des mégadonnées (le *Big data*) pour procéder à des analyses dont la portée excède largement ce à quoi l'individu qui a fourni un

³ On verra par exemple un document de la société Amazon cité par Plourde, Alexandre. *Le prix de la gratuité – Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne?* Montréal, Option consommateurs, juin 2015. 72 p. P. 21. Disponible au http://www.option-consommateurs.org/documents/principal/fr/File/option_consommateurs_2014_2015_gratuite_rapport.pdf. Ci-après «Plourde-prix».

⁴ Songeons notamment aux montres ou aux bracelets qui captent votre rythme cardiaque, le nombre de pas que vous effectuez... et qui permettent d'emmagasiner ces informations, d'en tirer des profils, de les comparer avec les résultats d'autres personnes.

⁵ On en trouvera une illustration dans Green, Eileen; Singleton, Carrie. *Mobile connections: an exploration of the place of mobile phones in friendship relations*. (2009) 57:1 *The Sociological Review* 125-144, où les auteures explorent entre autres le partage de téléphones intelligents dans la fratrie (ou entre amis) lorsque les parents s'opposent à ce que les enfants plus jeunes disposent de leur propre téléphone.

⁶ Plourde-prix, *op. cit.*, pp. 12-14.

⁷ On notera à ce dernier égard que l'Union européenne procède actuellement à l'étude d'un projet de règlement qui les viserait particulièrement: Commission européenne. *Proposition de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»)*. 2017/0003 (COD). Bruxelles, Commission européenne, 10 janvier 2017. 39 p. La version française est accessible par l'entremise de la page <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>.

⁸ Plourde-prix, *op. cit.*, pp. 31-37.

renseignement tout banal peut s'attendre⁹. Le maillage d'un vaste spectre de fournisseurs, d'analystes, de sous-traitants... ne simplifie pas les choses. L'utilisatrice d'une carte de crédit émise par une institution financière canadienne saisit-elle bien dans quelle mesure les renseignements relatifs aux achats qu'elle effectue grâce à sa carte transitent presque inévitablement par les États-Unis, compte tenu de la configuration des réseaux électroniques des MasterCard et Visa de ce monde?

Non seulement nous faut-il composer avec le traitement des renseignements qui nous concernent durant notre vie, mais il faut de plus en plus fréquemment gérer des situations où un même renseignement concerne plusieurs personnes, dont les intérêts ou les volontés peuvent diverger; les médias sociaux en fournissent d'innombrables exemples, qu'il s'agisse de déclarations d'appui (les *like*, par exemple), de liens, de photos retransmises d'usager en usager et relatives à plusieurs personnes... Nos jumeaux virtuels sont entrelacés avec ceux de dizaines d'autres personnes. Chose encore plus délicate, ils nous survivent et nos proches doivent en gérer l'existence sans pouvoir toujours compter sur l'expression de notre consentement¹⁰.

Ajoutons l'essor de l'Internet des objets. Non seulement fournissons-nous nous-mêmes des renseignements qui nous concernent, plus ou moins volontairement mais, de plus en plus, nos objets généreront également des données. La voiture intelligente en fournit le meilleur exemple, mais ce ne sera pas le seul. Songeons par exemple à la consommation d'électricité de notre domicile, dorénavant transmise électroniquement au fournisseur (et donc susceptible d'interception), qui peut révéler – même en notre absence, sans notre consentement et sans intervention délibérée de notre part – des informations significatives quant à notre mode de vie. Bientôt, notre réfrigérateur passera peut-être de manière autonome une commande chez l'épicier parce que notre stock de

⁹ Vous vous arrêtez à un comptoir de restauration rapide; des caméras captent la scène, le système constate que la file d'attente s'allonge et il modifie par conséquent l'affichage des mets proposés sur les menus numériques, de manière à mettre l'accent sur les produits qui peuvent être fournis le plus rapidement: Laskowski, Nicole. *Ten Big data case studies in a nutshell*. CIO Decisions, December 2013-January 2014, consulté au <http://searchcio.techtarget.com/opinion/Ten-big-data-case-studies-in-a-nutshell>. On pourrait tout aussi bien modifier les prix à la hausse en fonction de l'augmentation ponctuelle de la demande, comme le font les transporteurs aériens sur leur site web, en tenant là encore compte en temps réel de l'achalandage. On connaît aussi, bien sûr, le cas d'Uber. Votre présence, ou votre recherche, altère l'offre et les prix, sans qu'on puisse déterminer quels renseignements sont recueillis à notre égard ou soupçonner l'usage qu'on en fait – et dont le résultat sera à vrai dire le plus souvent imprévisible.

¹⁰ Option consommateurs publiera sous peu les résultats d'une recherche relative à certains aspects de la mort numérique, qui a bénéficié du soutien financier du Commissariat à la protection de la vie privée. Notons à cet égard que l'Union européenne a expressément noté, au considérant 27, que le *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*. J.O. 4.5.2016, p. L119/1 (ci-après le «Règlement») ne s'applique pas aux renseignements concernant les personnes décédées; nous en prenons acte, mais la problématique demeure entière pour autant et les autorités européennes, tout comme les autorités canadiennes, devront tôt ou tard se pencher sur ces questions fort délicates et assez complexes. Tout simplement, nos renseignements nous survivent, ce n'est pas toujours la meilleure solution que de les supprimer automatiquement, mais nous ne pouvons plus exprimer de consentement à l'égard de leur sort: c'est le paradigme fondamental du régime de gestion des renseignements personnels qui se trouve ainsi mis en cause, comme on le relèvera dans la section 3.

yogourt est presque épuisé¹¹. Mais ces renseignements, qui n'émaneront pas directement de nous, nous concerneront aussi; comment les traitera-t-on? Et comment garantira-t-on leur sécurité, alors que des sites comme Shodan¹² permettent au premier venu de consulter une myriade de renseignements recueillis par des objets de toutes sortes, ou que les images de milliers de caméras de surveillance dans le monde sont mises à la disposition de quiconque souhaite jouer au voyeur¹³?

2.1.2 La valeur changeante des renseignements personnels

Nos renseignements personnels permettent depuis toujours que l'on prenne des décisions à notre égard: ils valent traditionnellement comme des éléments de processus décisionnels. Mais, dorénavant, il y a plus: ils servent aussi de monnaie d'échange.

On trouve, notamment sur le web, un nombre croissant d'entreprises dont le modèle d'affaires relève au plan économique de marchés bifaces¹⁴ et qui n'exigent des personnes physiques qui les utilisent aucune autre contribution que le partage de renseignements personnels. Songeons par exemple à Google, à Facebook... qui peuvent ensuite monnayer ces renseignements personnels de diverses manières pour en tirer des revenus¹⁵. C'est en quelque sorte en fournissant nos renseignements personnels à ces entreprises que nous les payons, et que nous pouvons par conséquent avoir accès à leurs services.

Il en résulte un risque d'exclusion: si on ne consent pas à partager nos renseignements, on ne pourra pas participer à des réseaux dont l'importance sociale est grandissante. On pourrait même se trouver à terme exclus de certains circuits économiques, puisqu'anonymat et paiement se trouvent de plus en plus souvent découplés: on paie

¹¹ Pegoraro, Rob. *Samsung's Family Hub Smart Fridge: Would You Believe It Keeps Beer Cold, Too?*. Yahoo Tech, 7 janvier 2016. Consulté au <https://www.yahoo.com/tech/samsung-updates-the-smart-fridge-but-will-it-230148026.html>.

¹² On verra le <https://www.shodan.io/>. À l'égard de pratiques comme la surveillance par caméra, on verra Osborne, Charlie. *Shodan : The IoT search engine for watching sleeping kids and bedroom antics*. Zero Day, 26 janvier 2016. Consulté au <http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/>. Mais on a aussi eu accès grâce à Shodan à des moniteurs de rythme cardiaque utilisés dans des hôpitaux états-uniens ou à la gestion de centrales hydro-électriques françaises, notamment: Goldman, David. *The Internet's most dangerous sites*. CNN, 2 mai 2013. Consulté au <http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html>.

¹³ On verra par exemple, à l'égard d'un cas récent dans une école de Nouvelle-Écosse, Bradley, Susan. *N.S. privacy watchdog investigating after Russian site shows surveillance video of school*. CBC, 4 mai 2017. Consulté au <http://www.cbc.ca/news/canada/nova-scotia/privacy-commissioner-investigation-school-webcam-broadcast-1.4099658>.

¹⁴ On entend par « marchés bifaces » (ou, en anglais, *two-sided markets*) des marchés où un fournisseur dépend simultanément de deux marchés: l'éditeur d'un journal, par exemple, doit à la fois convaincre des lecteurs et des publicitaires de recourir à ses services, à des prix qui peuvent différer – ou même être nuls, dans le cas d'une des deux faces. On pourra lire l'étude classique en économie dans ce domaine: Rochet, Jean-Charles; Tirole, Jean. *Two-Sided Markets: A Progress Report*. (2006) *The Rand Journal of Economics* 37:3, 645-667. Disponible au <https://www.jstor.org/stable/pdf/25046265.pdf>. Le professeur Tirole a reçu le Prix en sciences économiques de la Sverige Riksbank en mémoire d'Alfred Nobel en 2014. On verra également Hoofnagle, Chris Jay; Whittington, Jan. *Free: Accounting for the Costs of the Internet's Most Popular Prize*. (2014) *UCLA Law Rev.* 606-670.

¹⁵ Plourde-prix, *op. cit.*, pp. 38-44.

parfois par l'échange même d'identifiants, et de plus en plus en fournissant du moins certains renseignements pour authentifier l'opération. Cette relation insidieuse entre paiement et captation de renseignements personnels mériterait d'être étudiée de beaucoup plus près. Elle a aussi pour effet que, trop souvent, les organisations exigent la communication de renseignements personnels qui ne sont pourtant pas nécessaires à l'opération qu'elles envisagent d'effectuer avec une personne; trop peu savent ou se souviennent qu'il est pourtant interdit d'exiger la cueillette de renseignements non nécessaires, en vertu notamment de l'alinéa 5 (1) de la LPRPDÉ et de l'article 4.2.2 de son annexe 1.

Nos renseignements personnels ne valent donc plus seulement pour eux-mêmes: ils deviennent le sésame qui nous permet de nous intégrer à une société de plus en plus réseautée. Il ne s'agira plus simplement de savoir si je veux fournir tel ou tel renseignement, nécessaire à la prise d'une décision donnée; à défaut de consentement, c'est de systèmes entiers qu'on se trouvera exclu, non pas parce que nos renseignements seraient nécessaires, mais parce qu'ils seront exigés à l'égard de services «facultatifs», mais socio-économiquement quasi-essentiels.

2.2 L'évolution des règles

Si notre univers informationnel se transforme, sa charpente normative doit aussi évoluer, sans quoi l'écart croissant entre les pratiques et les règles engendrera la prolifération de problèmes qui, tôt ou tard, deviendront des crises qui nuiront au plus grand nombre. Les travaux menés au sein de l'Union européenne au cours des dernières années, notamment, indiquent toutefois qu'on peut réformer l'appareil réglementaire soutenant la gestion des renseignements personnels. Si les solutions proposées par le Règlement ne sauraient être transposées intégralement dans le contexte canadien, elles peuvent du moins alimenter notre réflexion et nous inspirer. Certains des principes qui la sous-tendent, comme l'accent sur des mesures préventives, l'amélioration des pratiques liées à l'information et au consentement ainsi que la mise à jour des pouvoirs des autorités réglementaires, se prêtent admirablement à une transposition dans le régime canadien.

2.2.1 La prévention

Plus que jamais, il vaudra mieux prévenir que guérir en matière de gestion des renseignements personnels. C'est d'ailleurs la philosophie que retient le Règlement lorsqu'il requiert, à son article 25, que l'on conçoive les dispositifs de cueillette et de traitement des renseignements personnels de manière à favoriser la mise en œuvre des principes de gestion de ces renseignements que le Règlement formule par ailleurs. On notera au passage que ce concept de «protection intégrée», dès la conception d'un service, a d'abord été élaboré au Canada il y a une vingtaine d'années sous le nom de

*privacy by design*¹⁶; sans doute serait-il temps que nous le formulions à notre tour formellement dans notre régime normatif.

La perspective de la protection intégrée mérite d'autant plus d'être retenue qu'elle repose sur un principe économique d'attribution des coûts dont la logique paraît implacable: c'est l'acteur économique qui peut éviter d'imposer des coûts le plus facilement qui devrait être requis de le faire; on évoquera en anglais le *least cost avoider*. Puisque les pratiques de gestion des renseignements personnels dérogeant aux règles imposent des désavantages – et donc des coûts – à leurs victimes, elles doivent être évitées. Or ce sont généralement les concepteurs et les fournisseurs de services qui peuvent le plus facilement éviter ces inconvénients imposés au plus grand nombre, en concevant mieux leurs produits. Il est beaucoup plus facile – et moins coûteux – pour Facebook, par exemple, de mettre en service un produit conforme aux règles de protection des renseignements personnels que de demander à près de deux milliards d'utilisateurs¹⁷ de modifier après coup leurs paramètres d'utilisation ou de logger des requêtes de rectification ou de retrait de certains renseignements.

Pour prévenir les risques, bien sûr, il faut d'abord les déceler, puis les évaluer. Le Règlement requerra donc dans certains cas au sein de l'Union européenne la réalisation préalable d'analyses d'impact, gouvernées par ses articles 35 et 36. Sans doute faudrait-il adapter quelque peu ce régime avant de l'imposer au Canada, mais il nous paraît qu'il s'agit là d'un accessoire parfois indispensable à la mise en place d'un régime efficace de protection intégrée des renseignements personnels dès la conception des dispositifs chargés de les recueillir et de les traiter.

Au plan individuel, la mise à disposition d'options permettant de s'opposer à ce qu'on soit pisté (*do not track*) s'avérerait également utile, en permettant d'éviter d'emblée la cueillette et l'accumulation de renseignements personnels¹⁸.

Un vigoureux effort s'impose donc au plan de l'amélioration de notre régime au plan de la prévention; cela ne saurait toutefois suffire.

2.2.2 L'information

Pour consentir adéquatement, il faut comprendre; et pour comprendre, il faut être informé. Les règles canadiennes actuelles, telles qu'elles ont été formulées par le législateur, puis interprétées par les tribunaux ou les organismes administratifs, ne garantissent toutefois pas aux citoyens qu'ils pourront obtenir toute l'information dont ils ont besoin pour comprendre, ni que cette information sera compréhensible.

D'abord, l'information fournie par les prestataires de services prend souvent la forme de «politiques», plus ou moins faciles à trouver sur leurs sites web ou ailleurs, ou de

¹⁶ On trouvera entre autres un sommaire de la petite histoire de ce concept dans Bélanger-Krams, Annik. *Enquête sur les paiements mobiles au point de vente: qu'en est-il de la vie privée des consommateurs?* Montréal, Option consommateurs, juin 2016. 87 p. Pp. 42-44.

¹⁷ Facebook aurait compté en mars 2017 1,94 milliard d'utilisateurs: Zephoria Digital Marketing. *The Top 20 Valuable Facebook Statistics – Updated May 2017*. Consulté au <https://zephoria.com/top-15-valuable-facebook-statistics/>.

¹⁸ On verra à cet égard Plourde, Alexandre. *Payer pour disparaître – Aspects juridiques et commerciaux du droit à l'oubli au Canada*. Montréal, Option consommateurs, juin 2016. 61 p. Ci-après «Plourde-Payer». P. 60.

dispositions dans des modalités de service. Trop souvent, ces textes sont illisibles et incompréhensibles: on recourt à de petits caractères et à des mises en page qui rebutent le lecteur le plus aguerris, tandis que le contenu est abstrus à cause de l'usage d'un jargon inintelligible, d'une syntaxe démesurément complexe et du recours – exprès ou implicite – à des concepts juridiques que l'usager moyen ne connaît pas. On oublie par ailleurs trop souvent que la moitié des Canadiens sont fonctionnellement analphabètes¹⁹, et que toute cette documentation ne peut par conséquent leur être d'aucune utilité.

Bref, l'information se trouve formellement mise à notre disposition, mais elle ne sert pratiquement à rien²⁰.

Sans doute serait-il plus exact d'écrire plutôt qu'une partie de l'information est disponible; dans certains cas, c'est plutôt l'opacité qui règne. Trop souvent, des décisions sont prises sur notre compte à l'aide d'algorithmes dont on ne sait rien, et dont on présume apparemment de la fiabilité. Il y a pourtant tout lieu de croire que les mécanismes automatisés de prise de décision comportent des lacunes appréciables²¹. Nous partageons par conséquent pleinement les appréhensions que manifestait à cet égard le professeur Michael Geist lors de sa comparution devant le Comité, le 21 mars dernier²².

Dans cette perspective, il nous paraît essentiel que les autorités canadiennes s'inspirent de l'article 22 du Règlement afin d'encadrer au plus tôt les mécanismes automatisés de prise de décision et s'assurent que les données nécessaires à l'évaluation de leur efficacité se trouvent dans le domaine public ou, à tout le moins, puissent être jaugées rigoureusement par des organismes de contrôle tels que le Commissariat à la protection de la vie privée.

Quant aux informations qui nous sont transmises, et en présumant qu'elles puissent comporter une certaine utilité, on devrait du moins s'inspirer des articles 12 à 14 du Règlement pour accentuer l'exigence qu'elles soient fournies «de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et précis.»

¹⁹ Plus précisément, quarante-neuf pour cent (49%) de la population canadienne se trouve au mieux au niveau 2 en matière de «littéracie» sur une échelle de 5. Statistique Canada; Emploi et Développement social Canada; Conseil des ministres de l'Éducation (Canada). *Les compétences au Canada: Premiers résultats du Programme pour l'évaluation internationale des compétences des adultes (PEICA)*. Ottawa, Ministère de l'Industrie, 2013. Catalogue no. 89-555-X. 109 p. Pp. 16, 17. Consulté au <http://www.statcan.gc.ca/pub/89-555-x/89-555-x2013001-fra.pdf>.

²⁰ On verra entre autres Plourde-prix, *op. cit.*, pp. 16-37 et Bélanger-Krams, *op. cit.*, pp. 50-67.

²¹ À l'égard de l'efficacité toute relative des mécanismes automatisés d'évaluation de l'attribution de crédit utilisés par des institutions financières canadiennes, on verra Allen, Jason; Damar, Evren; Martinez-Miera, David. *Consumer Bankruptcy and Information*. Bank of Canada Working Paper 2012-18. Ottawa, Banque du Canada, juillet 2012. 34 p. Consulté au <http://www.bankofcanada.ca/wp-content/uploads/2012/07/wp2012-18.pdf>. Les auteurs ont affiné leur analyse dans Allen, Jason; Damar, Evren; Martinez-Miera, David. *Consumer Bankruptcy, Bank Mergers and Information*. (2016) Review of Finance 1289-1320 On verra également Drozd, Lukasz A.; Ricardo Serrano-Padial. *Modeling the Revolving Revolution: The Debt Collection Channel*. (2017) *American Economic Review*, 107(3): 897-930.

²² On verra aussi Plourde-prix, *op. cit.*, pp. 50-51.

2.2.3 Le consentement

Pierre d'assise du cadre normatif de protection des renseignements personnels, la notion de consentement a été vidée de toute substance. Comme le notait le professeur Vincent Gautrais lors de son témoignage devant le Comité, le 4 avril dernier, les mécanismes d'échanges de consentement proposés sous forme contractuelle par les organisations protègent d'abord et avant tout les entreprises qui rédigent ces formulaires, et non les usagers. La LPRPDÉ ne contient d'autre part pratiquement aucune règle qui vienne encadrer ces contrats d'adhésion afin de rendre invalides les clauses abusives qu'ils contiennent le plus souvent²³.

Le plus souvent, les citoyens n'ont pas le choix: ils doivent consentir en bloc à l'ensemble des exigences imposées par des prestataires, ou se passer de leurs services. Comme la plupart des fournisseurs formulent des règles similaires dans ce domaine, la concurrence ne joue non plus aucun rôle effectif dans l'encadrement des pratiques. Nous partageons par conséquent le souhait, formulé par le professeur Geist lors de sa comparution devant le Comité, qu'on instaure plutôt un régime de consentement «à la carte», qui permette véritablement aux consommateurs de déterminer librement dans quelle mesure il consent, ou non, à la cueillette et à l'utilisation de renseignements personnels qui ne sont pas absolument nécessaires à la prestation des produits ou des services qu'ils souhaite obtenir²⁴.

Les difficultés soulevées par la mise en œuvre de la notion de consentement se trouvent évidemment exacerbées lorsqu'on s'adresse à des enfants, qui ne disposent pas de l'information ou, dans bien des cas, de la faculté de jugement, auxquelles les adultes sont présumés pouvoir faire appel.

Quel enfant, quel parent même soupçonnerait qu'un ourson en peluche interactif capte les propos du tout-petit et les stocke dans le «nuage» informatique, où ils peuvent être analysés et piratés²⁵? Qui pourrait imaginer que le fabricant, connu sous la marque *CloudPets* et informé à plusieurs reprises par des spécialistes que ses mesures de sécurité comportaient des failles colossales, n'ait absolument rien fait afin d'y remédier? Et comment peut-on mettre en marché une poupée qui permet à des enfants de faire des recherches sur le web ou de communiquer avec des tiers sans s'assurer de l'assortir de mesures de sécurité qui empêcheraient des tiers malveillants de communiquer avec ces enfants²⁶?

Nous partageons par conséquent la préoccupation évoquée notamment au considérant 38 du Règlement, et qui se concrétise entre autres aux paragraphes 6 f), 8, et 12 (1) en matière de nécessité de la cueillette et du traitement, d'obtention du consentement et de

²³ On verra notamment, en matière du contenu des contrats et des politiques, Plourde-prix, *op. cit.*, pp. 25-30 et Bélanger-Krams, *op. cit.*, pp. 53-63.

²⁴ On verra aussi à cet égard, Plourde-prix, *op. cit.*, p. 46.

²⁵ Hunt, Troy. *Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages*. 28 février 2017. Consulté au <https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/>.

²⁶ Huggler, Justin. *Germany bans internet-connected dolls over fears hackers could target children*. Londres, The Telegraph, 17 février 2017. Consulté au <http://www.telegraph.co.uk/news/2017/02/17/germany-bans-internet-connected-dolls-fears-hackers-could-target/>.

transparence en ce qui a trait à l'obtention et à l'usage des renseignements personnels relatifs aux enfants, ou fournis par eux. Nous appuyons aussi la substance des recommandations formulées à cet égard par le Centre pour la défense de l'intérêt public dans les observations écrites qu'il a communiquées au Comité le 20 février dernier²⁷.

Nous notons d'autre part que le régime canadien effectue assez peu de distinctions en rapport avec le type de renseignement personnel qui fait l'objet d'un traitement, contrairement au régime européen, où l'article 9 du Règlement établit des règles particulières à l'égard de renseignements plus «sensibles». Sans doute ne pourrait-on pas importer entièrement ce régime au Canada, mais il nous paraît qu'on devrait envisager d'accorder une attention particulière aux renseignements de nature «biologique» (génétique, biométrie, métabolisme, pathologies...), en exigeant notamment des consentements particulièrement bien éclairés, et qu'on devrait se pencher plus attentivement sur les questions entourant le consentement à l'égard des renseignements, de plus en plus nombreux, qui concernent simultanément deux ou plusieurs personnes susceptibles d'avoir des intérêts différents ou d'exprimer des volontés différentes quant au traitement de ces renseignements.

2.2.4 L'oubli

Notre jumeau virtuel doit-il être éternel, même lorsque la conservation des renseignements qui le concernent ne relève pas de l'intérêt public? Nous ne le croyons pas. Il ne nous semble pas pour autant qu'un seul remède puisse régler toutes les difficultés que peut soulever la préservation pour une période indéterminée de renseignements que la personne concernée a pu juger pertinents à une époque, mais qui lui paraissent désormais inutiles, périmés ou équivoques. Nous ne croyons pas davantage qu'une personne ne devrait pouvoir exiger le retrait de renseignements que lorsqu'ils sont inexacts ou comportent, par exemple, un aspect attentatoire à leur réputation. C'est le contrôle de la personne concernée à l'égard des renseignements qui la concernent qui caractérise notre régime de gestion des renseignements personnels, et ce contrôle devrait pouvoir s'exercer soupagement et facilement, sous réserve de l'existence d'intérêts supérieurs bénéficiant à d'autres personnes ou à la collectivité.

Il nous paraît par conséquent qu'on devrait mettre en place une panoplie de moyens simples et efficaces permettant à une personne d'obtenir le retrait de renseignements, et notamment de contenus en ligne, qui peuvent diversement porter atteinte à ses intérêts ou à ses droits, y compris le droit à la dignité²⁸. Le droit à l'oubli, tel que le constitue l'article 17 du Règlement, devrait faire partie de cet arsenal fourni aux individus. Nous partageons à cet égard les recommandations formulées par le Centre pour la défense de l'intérêt public dans ses observations précitées.

²⁷ Lawford, John; Lau, Alysia. *Final written submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics – Review of PIPEDA*. Ottawa, PIAC, 20 février 2017. 6 p.

²⁸ Plourde-payer, *op. cit.*

2.2.5 D'autres préoccupations

Certaines problématiques font l'objet de dispositions spécifiques dans le Règlement, alors que le droit canadien demeure muet ou insatisfaisant à leur égard. Il nous paraît que, non seulement pour garantir l'adéquation de notre régime aux fins de l'article 45 du Règlement, mais tout simplement pour l'améliorer, il conviendrait de s'inspirer à ces égards des règles européennes.

Nous songeons d'abord ici au statut et aux obligations des sous-traitants et de ceux qui leur confient diverses tâches, qui font l'objet d'un encadrement assez complet aux articles 24, 26 et 28 du Règlement.

Notons ensuite le droit à la portabilité des données, visé par l'article 20 du Règlement. L'implantation d'un régime analogue comporterait des avantages notables pour les individus, en plus de favoriser la mobilité et la concurrence dans divers marchés.

D'autre part, il y aurait lieu de se pencher sur le champ d'application territorial de la LPRPDÉ. Compte tenu du libellé de son article 4, la Loi s'applique d'abord et avant tout aux organisations situées au Canada, et donc aux opérations qui y sont effectuées. En vertu du paragraphe 3 (2) du Règlement, toutefois, celui-ci s'applique non seulement aux opérations effectuées sur le territoire «national», mais aussi à certaines opérations visant des personnes qui se trouvent sur le territoire de l'Union européenne, même si l'organisation responsable du traitement des données se trouve à l'extérieur de ce territoire. Il nous paraît que ce concept de juridiction en fonction de la localisation de la personne, qui est d'ailleurs analogue à ce qu'on connaît en droit international privé en matière de protection des consommateurs, devrait être retenu dans la LPRPDÉ²⁹.

Toujours en matière de flux transfrontaliers de données, nous notons que le paragraphe 45 (2) a) du Règlement établit parmi les critères pris en compte dans le cadre d'une décision d'adéquation les règles établies par le pays tiers (en l'occurrence le Canada) à l'égard du transfert ultérieur de renseignements personnels en provenance de l'Union européenne vers un autre pays. Il nous semble que la LPRPDÉ pourrait à cet égard faire preuve de plus de précision.

2.2.6 Les pouvoirs du Commissaire

Pour que le régime mis en place par la LPRPDÉ soit efficace, il faut qu'on puisse en assurer la mise en œuvre. Dès l'adoption de la Loi, nous étions d'avis qu'elle ne conférerait pas au Commissaire à la protection de la vie privée les attributions et les pouvoirs dont il aurait besoin pour la faire appliquer. Malgré les efforts qu'a déployés le Commissariat depuis cette époque, nous estimons toujours qu'il devrait disposer de pouvoirs plus

²⁹ La qualification juridique des questions relatives à la gestion des renseignements personnels est aussi complexe que délicate; il est toutefois généralement reconnu que les questions liées à l'état d'une personne sont régies par le droit de son domicile, tandis qu'en vertu notamment de l'article 5 de la *Convention de Rome de 1980 sur la loi applicable aux obligations contractuelles*, on ne peut priver un consommateur du bénéfice des règles impératives de la loi du lieu où il a sa résidence habituelle lorsqu'elles sont plus avantageuses que les règles s'appliquant par ailleurs au contrat; la situation de vulnérabilité des personnes dont on traite les renseignements personnels étant fréquemment analogue à celle des consommateurs, il y aurait lieu d'insérer dans la LPRPDÉ une règle similaire afin de protéger les Canadiens qui font affaire avec des entreprises situées à l'étranger. On trouvera le texte de la Convention au [http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:41998A0126\(02\)&from=FR](http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:41998A0126(02)&from=FR).

étendus (et de ressources plus considérables, mais il s'agit là d'un autre débat). Nous partageons par conséquent les avis exprimés notamment par le professeur Gautrais et le Centre pour la défense de l'intérêt public à cet égard.

Il suffit d'examiner les articles 57 et 58 du Règlement pour constater à quel point les autorités de contrôle nationales au sein de l'Union européenne seront dotées d'un vaste éventail de mécanismes, qui leur permettent de moduler une intervention en passant au besoin de l'enquête à l'avertissement, puis à l'ordonnance et à la sanction. Et cette sanction, sous la forme d'une amende administrative, peut dans les cas les plus graves atteindre 4% du chiffre d'affaires annuel mondial d'un contrevenant (par. 84 (6)); dans le cas de Facebook, par exemple, cette pénalité pourrait s'élever à plus d'un milliard de dollars canadiens³⁰. Il y a là de quoi dissuader toute entreprise...

Il nous paraît d'autre part que l'accroissement des pouvoirs du Commissaire, loin de restreindre sa capacité d'intervention, accentuerait sa crédibilité. Si la diversification de ces pouvoirs, y compris l'établissement de sanctions administratives pécuniaires, peut requérir certains aménagements administratifs pour assurer l'entier respect des droits des organisations assujetties à la LPRPDÉ, il nous paraît que la qualification juridique que la Cour suprême du Canada a récemment donnée à l'égard de telles sanctions³¹ fait en sorte qu'il est parfaitement possible de concilier au sein d'un organisme comme le Commissariat un vaste éventail de pouvoirs.

Il conviendrait par ailleurs de préciser les obligations imparties aux organisations lorsqu'elles sont alertées à l'égard de failles concernant leurs mesures de sécurité, ou lorsqu'elles les constatent. Elles devraient être légalement tenues de procéder avec diligence à la mise en place de mesures remédiatrices adéquates, et elles devraient informer les personnes concernées dans les cas où des renseignements personnels pourraient avoir été compromis. Le Règlement comporte d'ailleurs des obligations à ce dernier égard à ses articles 33 et 34.

3. Conclusions et recommandations

3.1 Envisager l'avenir

L'émergence de préoccupations à l'égard des traitements automatisés de renseignements personnels a conduit l'Organisation de coopération et de développement économiques à adopter en 1980 des lignes directrices visant l'encadrement de pratiques qui se multipliaient tout en générant une confusion croissante, du fait notamment de la diversité croissante de solutions normatives improvisées par des autorités plus déconcertées les unes que les autres par l'évolution des problématiques³². Ces lignes

³⁰ La société Facebook a réalisé en 2016 un chiffre d'affaires de 26,885 G USD, selon le sommaire financier de la société (consulté au <https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx>); 4%, c'est le vingt-cinquième de cette somme, soit plus d'un milliard de dollars des États-Unis.

³¹ *Guindon c. Canada*, 2015 CSC 41, [2015] 3 R.C.S. 3.

³² Organisation de coopération et de développement économiques. *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*. Paris, Organisation de coopération et de développement économiques, 1980. Elles ont été adoptées le 23 septembre 1980 sous forme d'une

directrices, axées sur le respect du contrôle de la personne à l'égard des renseignements qui la concernent, visaient notamment à favoriser une certaine harmonie normative, tout en restaurant la confiance de la population à l'égard du sort réservé aux renseignements personnels; ces deux objectifs demeurent tout à fait louables. D'autre part, les lignes directrices constituent encore l'ossature de pratiquement tous les régimes juridiques de gestion des renseignements personnels, y compris ceux de l'Union européenne et du Canada. Mais tout a changé depuis.

En 1980, on envisageait des traitements de renseignements personnels par des organismes publics et de grandes entreprises, seuls capables à l'époque de se doter des infrastructures informatiques nécessaires. La micro-informatique, balbutiante, ne prendrait son essor que quelques années plus tard³³. Le réseau Internet existait, sous le nom d'ARPANET, mais il ne reliait guère que quelques institutions universitaires ou étatiques³⁴; le web ne serait inventé qu'en 1989, et ne deviendrait véritablement accessible au public qu'en 1991. Pour mémoire, Google a été fondée en 1996 et Facebook, en 2004; Twitter? En 2006.

À l'époque de l'adoption des lignes directrices, on n'avait donc affaire qu'à des rapports relativement simples: une grande organisation saisissait des renseignements auprès des individus, le plus souvent directement et pour des fins qu'elle pouvait clairement déterminer; cette organisation disposait d'autre part des ressources requises afin d'informer adéquatement les personnes touchées. Il s'agissait par conséquent de relations bilatérales dont les individus pouvaient comprendre les tenants et les aboutissants, pour peu qu'on leur fournisse des explications adéquates.

Comme on l'a noté dans la section 2, le portrait s'est depuis considérablement compliqué. Des millions d'organisations de toutes tailles recueillent et s'échangent des renseignements dont la nature s'est beaucoup diversifiée, pour des fins qui peuvent se multiplier comme des champignons après la pluie, au hasard des nouvelles inventions des prodiges du marketing, dans le cadre de réseaux remarquablement complexes et en utilisant des dispositifs souvent indétectables par l'utilisateur moyen, et qui leur sont difficilement intelligibles. Ne pas plonger dans ce torrent de données, toutefois, c'est parfois s'isoler socialement, et même économiquement.

Cela soulève par conséquent une question. Le cadre formulé en 1980, calqué sur le modèle contractuel entre individu et organisation et fondé sur un échange de consentements éclairés, est-il adapté à ce nouvel univers, beaucoup plus complexe et de moins en moins compréhensible? Si la réponse devait s'avérer négative, c'est à une révolution copernicienne que nous serions appelés. Et nous soupçonnons que ce soit le cas.

recommandation du Conseil de l'Organisation. On en trouve le texte sur son site web, au <http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm>.

³³ Le tout premier ordinateur personnel d'IBM, qui fut le premier chef de file dans ce marché, a été commercialisé en 1981; le Macintosh, bien sûr, date pour sa part de 1984. Si divers modèles de micro-ordinateurs ont commencé à se développer dès les années 1970, ce n'est qu'une décennie plus tard que le phénomène est devenu véritablement significatif.

³⁴ Ce n'est qu'en 1983 qu'on a implanté les protocoles TCP et IP, et qu'en 1984 qu'on a decouplé la portion militaire du reste du réseau, pour créer ce qu'on connaît maintenant sous le nom d'Internet.

On sait les problèmes, évoqués *supra*, que pose manifestement la notion de consentement. Bientôt, il faudra réfléchir au statut des renseignements reliés à nos objets, qui prendront eux-mêmes des décisions qui pourront altérer les profils informationnels qui nous seront reliés. Dans certains cas, des renseignements concernent simultanément plusieurs personnes: données génétiques, photos de groupe... Quelle est la mesure du droit de chaque personne à leur égard? Déjà, on l'a noté, on demeure perplexe à l'égard du régime relatif aux renseignements concernant ceux qui ne sont plus des personnes et ne peuvent plus consentir, en raison de leur décès. Le lien tout simple personne – consentement – organisation ne peut plus expliquer adéquatement les phénomènes que nous observons. Il faudra un autre paradigme.

«Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité», nous rappelle le considérant 4 du Règlement. Le sort fait à nos jumeaux virtuels ne devrait pas dicter le nôtre, et c'est nous qui, dans toute la mesure du possible, devrions maintenir le contrôle sur ces jumeaux. Mais la tâche se complique sensiblement, et il devient urgent d'y voir.

Si Rabelais nous rappelait dès 1532 que tout vient à point à qui peut attendre, force est de constater que notre société ne pourra guère attendre beaucoup plus longtemps que l'on encadre, de manière fiable et cohérente, l'usage des données qui est devenu essentiel dans notre monde hyper-réseauté.

Nous savons bien que la révision à laquelle procède actuellement le Comité ne réglera pas ce nouvel ordre de difficultés. Mais ce serait, nous semble-t-il, faire œuvre utile que de constater d'ores et déjà qu'il faut amorcer cette réflexion fondamentale, et proposer peut-être un programme de recherche qui permettrait de renforcer la veille technologique qui s'impose et, surtout, qui reposerait sur la participation active de tous les intervenants dans la société, y compris les associations de consommateurs.

3.2 En attendant...

À plus court terme et dans le cadre du mandat actuel du Comité, compte tenu des observations formulées *supra*, nous formulons par conséquent des recommandations qui ont trait, d'une part, à des modifications législatives et, d'autre part, à la poursuite de travaux de recherche et d'information.

- 1- Option consommateurs recommande au Comité qu'il propose de modifier la LPRPDÉ afin d'y intégrer**
 - a) des dispositions précisant que la Loi s'applique en général au traitement de données concernant des personnes résidant habituellement au Canada;**
 - b) des obligations relatives à la protection intégrée des données dès la conception des dispositifs de cueillette et de traitement;**
 - c) des obligations relatives à la réalisation préalable, par les organisations qui conçoivent de tels dispositifs, d'analyses d'impact dans les cas qui le requièrent;**
 - d) des règles précisant le partage des responsabilités entre les organisations et leurs sous-traitants;**

-
- e) des obligations relatives à la forme des informations fournies aux personnes concernées, afin de garantir qu'elles soient concises, transparentes, compréhensibles, facilement accessibles et formulées en termes clairs et précis;
 - f) des mesures permettant de contrôler la validité, dans des contrats d'adhésion, de dispositions visant à obtenir des consentements de la part des personnes concernées, afin d'assurer que ces dispositions ne désavantagent pas ces personnes de manière excessive et déraisonnable et qu'elles puissent être invalidées en tout ou en partie lorsque c'est le cas;
 - g) des mesures permettant à la personne concernée de moduler les consentements qu'elle fournit et, notamment de s'opposer à son pistage lorsqu'il n'est pas nécessaire;
 - h) des mesures permettant un encadrement rigoureux et transparent des mécanismes automatisés de prise de décision, qui devraient pouvoir faire l'objet d'un contrôle spécifique du Commissaire à la protection de la vie privée;
 - i) des mesures visant particulièrement la protection des enfants;
 - j) des mesures visant particulièrement l'encadrement de l'usage des renseignements relatifs à des personnes décédées;
 - k) des mesures facilitant le retrait à la demande d'une personne des renseignements qui la concernent, y compris la mise en œuvre d'une forme de droit à l'oubli et la précision des obligations imparties à un intermédiaire en ligne informé du caractère faux ou diffamatoire d'un renseignement;
 - l) des mesures permettant d'établir un régime de portabilité des données;
 - m) des mesures obligeant les organisations à tenir compte, avec diligence, des informations qui leur sont transmises et qui font état de la vulnérabilité de leurs systèmes, et notamment de leurs mesures de sécurité, et à notifier les personnes concernées par des défaillances dans les cas qui le requièrent;
 - n) des mesures étendant substantiellement les attributions et les pouvoirs du Commissaire à la protection de la vie privée, y compris la mise en place d'un régime dissuasif de sanctions administratives pécuniaires;
- 2- Option consommateurs recommande au Comité qu'il propose au Commissaire à la protection de la vie privée ou à d'autres instances compétentes que soient menées à brève échéance des recherches portant sur
- a) le rôle de plus en plus important que jouent les renseignements personnels en guise de modes de paiement, ou à titre d'accessoires à des modes de paiement, et le risque d'exclusion socio-économique qui peut en découler;
 - b) l'encadrement de l'usage de renseignements de nature biologique, y compris les renseignements génétiques, biométriques et métaboliques, et d'autres types de renseignements dits «sensibles»;
 - c) la mise en œuvre effective du principe de nécessité en matière de cueillette et d'utilisation des renseignements personnels, dans le cadre des pratiques réelles et contemporaines des organisations assujetties à la Loi;

-
- d) le fonctionnement et l'effet des processus automatisés de prise de décision;
 - e) l'encadrement de l'usage de renseignements qui concernent simultanément plusieurs personnes physiques et les problématiques particulières que de telles situations peuvent comporter;
 - f) les impacts économiques et sociaux de l'hypermnésie du web, qui tend à ne rien oublier;
 - g) la révision du cadre conceptuel sous-tendant notre régime de protection des renseignements personnels, afin de l'adapter au besoin à l'évolution fondamentale des pratiques de gestion des renseignements personnels que nous constatons;
- 3- Option consommateurs recommande au Comité qu'il propose au Commissaire à la protection de la vie privée ou à d'autres instances compétentes que soient accentués les efforts d'information visant
- a) la sensibilisation du public, des organisations et des professionnels concernés à l'égard des questions soulevées par la problématique de la mort numérique;
 - b) la sensibilisation du public et des organisations à l'égard des risques particuliers qui sont reliés aux renseignements concernant des enfants;
 - c) la sensibilisation du public et des organisations au fait qu'on ne peut en principe exiger d'une personne la fourniture de renseignements qui ne sont pas nécessaires à la réalisation d'une opération.