Technologies et vie privée, à l'heure des choix de société
5e Rappport quinquennal de la Commission d'accès à l'information du Québec
Résumé

Mot du président

En 2002, au moment de la publication du dernier rapport quinquennal de la Commission, *Facebook, YouTube, Twitter, Google Street View* et *WikiLeaks* n'existaient pas encore ! Le temps écoulé depuis fait en sorte que notre réflexion sur la législation actuelle doit tenir compte de la réalité d'un espace qui ne cesse de se modifier au gré des technologies de l'information.

Ainsi, plusieurs catégories de renseignements personnels peuvent être diffusées plus rapidement et plus largement que jamais par les individus eux-mêmes dans le cadre de leurs activités. En même temps, tant le secteur public que le secteur privé demeurent avides de telles informations. La puissance du traitement informatique permet de les coupler, les regrouper, les lier entre elles et les stocker de façon illimitée pour générer des analyses de comportement, des fiches de crédit, des habitudes de consommation, des historiques de consultations du Web et ainsi de suite.

C'est pourquoi le présent rapport de la Commission porte une attention particulière à la protection de la vie privée. Il devient de plus en plus pressant, à l'ère numérique, de mettre en place des mesures de protection tenant compte des défis posés par les technologies de l'information sur la vie privée.

Il faut faire face à la réalité puisque les moyens technologiques vont continuer à se développer et à se raffiner. L'information fournie aux utilisateurs en ce qui concerne la divulgation de leurs renseignements personnels et les conséquences qui peuvent en découler doit être simple et transparente.

La Commission est préoccupée par ce qui semble être une certaine insouciance à cet égard. Elle s'inquiète de l'inexistence ou du manque de convivialité des formules d'adhésion ou de consentement à la collecte et à l'utilisation de renseignements personnels proposées ici et là pour accéder à un bien ou à un service. Dans le même ordre d'idées, il y a place à la simplification des politiques de confidentialité affichées par les organismes publics et les entreprises. De plus, si les renseignements devaient être perdus ou piratés, que penser du fait que nos législations actuelles ne prévoient aucune obligation d'en informer les autorités et les personnes concernées ? La protection des renseignements personnels a besoin d'une mise à jour importante à l'ère numérique.

Dans une société où l'information prend de plus en plus d'importance, on constate que les citoyens recherchent désormais une information facilement accessible, selon des besoins qu'ils déterminent eux-mêmes. L'information gouvernementale dont l'État est le dépositaire ne peut échapper à cette évolution. Le droit de savoir, le droit d'être informé, ainsi que la nécessaire transparence des pouvoirs publics sont les fondements préalables à la vie démocratique moderne.

Chacune des recommandations contenues dans ce rapport s'inscrit dans la continuité de l'action de la Commission depuis bientôt 30 ans. Si l'accès à l'information gouvernementale a été le « fer de lance » de l'adoption de la *Loi sur l'accès*, il importe maintenant d'augmenter de façon substantielle la quantité des informations accessibles aux citoyens et de faciliter, dans le respect des droits de chacun, l'accès à cette information.

Aussi, la Commission propose d'adapter le régime d'accès à l'information à la réalité actuelle en ouvrant, sauf exceptions, l'ensemble des données gouvernementales à la consultation et à l'utilisation. Sans pour autant gouverner dans une maison de verre, l'État doit répondre aux préoccupations citoyennes par une transparence accrue et une simplification de l'accès à l'information.

D'autres recommandations contribuent à renforcer le régime d'accès à l'information, notamment celles qui abordent l'assujettissement de certains organismes à la *Loi sur l'accès* et la nécessité pour ceux-ci de respecter les délais prescrits pour justifier un refus d'accès, ce qui serait de nature à faciliter le cheminement du justiciable dans un processus qui doit être simple et rapide pour produire ses effets.

De même, si la protection des renseignements personnels a été la « pierre d'assise » de l'adoption de la *Loi sur la protection dans le secteur privé*, il est essentiel de s'assurer que les recours mis à la disposition des citoyens peuvent être exercés adéquatement et que les entreprises sont représentées par un interlocuteur.

Enfin, l'évolution fulgurante des technologies de l'information préoccupe la Commission et l'amène à interpeller le gouvernement sur les nécessaires moyens dont elle devrait disposer pour remplir adéquatement son mandat de voir à la promotion de la protection des renseignements personnels de nos concitoyens. La constitution de mégabases de données, le vol d'identité, l'utilisation insouciante d'Internet, le profilage des individus, dont les enfants, ne peuvent pas demeurer uniquement les manifestations d'un progrès qui nous dépasse. Il faudra bien un jour ou l'autre s'en préoccuper.

En terminant sur une note plus personnelle, je tiens à souligner que mon arrivée à la présidence de la Commission m'a permis de prendre la mesure de l'engagement indéfectible de mon prédécesseur, Me Jacques Saint-Laurent, qui avait lancé la préparation de ce rapport. Nous nous sommes engagés dans les sillons qu'il avait définis et sa contribution mérite notre reconnaissance.

Depuis ma nomination à la Commission en 2006, j'ai eu l'occasion de tisser des liens privilégiés avec les membres du personnel de l'institution. Au cours des derniers mois, j'ai eu la chance de pouvoir apprécier leur compétence et leur dévouement remarquable. Tous ont su conjuguer leurs efforts et leurs expertises pour produire ce rapport. Au nom de tous mes collègues commissaires, je tiens à les remercier et à leur exprimer ma considération.

JEAN CHARTIER

Technologies et vie privée, à l'heure des choix de société est le cinquième Rapport quinquennal de la Commission d'accès à l'information du Québec (« la Commission »). Ce rapport répond aux exigences de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1] et de la *Loi sur la protection des renseignements personnels dans le secteur privé*[2] puisqu'il contient des constats relatifs à l'application de ces deux législations et propose des recommandations.

La première partie de ce rapport a trait à **la protection des renseignements personnels**.

La Commission estime qu'il est nécessaire de simplifier, à l'ère numérique, l'information préalable à l'expression du consentement des personnes concernées et par le fait même l'expression de leur consentement. L'action de cocher une case de type « j'ai lu et j'accepte » ou « j'atteste avoir pris connaissance » signifie que les personnes concernées ont lu et compris les conditions d'utilisation ou la politique de confidentialité associées à un site Web, à un réseau social. Nombreux sont les utilisateurs qui cochent une telle case sans avoir consulté ces informations, ils ne savent donc pas toujours à quoi ils consentent. La Commission considère que des actions doivent être prises afin que les organismes publics et les entreprises adoptent différents mécanismes susceptibles de répondre à ces objectifs. Pour ce faire, elle recommande, d'une part, l'adoption de politiques de confidentialité simplifiées. Ainsi, au lieu de publier une telle politique sous forme linéaire, les organismes publics et les entreprises doivent proposer une politique condensée présentant, en quelques paragraphes, leurs engagements en matière de protection des renseignements personnels et à partir de laquelle il est possible d'accéder à une politique détaillée contenant plus d'informations sur ceux-ci. Cette approche permet de présenter les politiques de confidentialité dans un format adapté au support. En effet, la lecture d'un document ne s'appréhende pas de la même manière selon qu'il est sur support papier ou informatique. De plus, l'attention du lecteur n'étant pas la même face à un support électronique, il est important de présenter des textes ne nécessitant pas ou peu de défilement. D'autre part, elle recommande la mise en place de pictogrammes de protection et une meilleure information des personnes physiques utilisant des objets susceptibles de les localiser et de les identifier (vidéosurveillance, biométrie, géolocalisation, identification par radiofréquence, par exemple).

Cet encadrement de l'information transmise aux personnes concernées pour s'assurer qu'elles expriment un consentement libre et éclairé doit profiter à tous, adultes et jeunes.

Ces derniers – les natifs du numérique – recourent aux blogues, à *Twitter*, à *MySpace* ou encore à *Facebook* pour communiquer avec leurs amis d'ici et d'ailleurs, pour publier des photos et des vidéos, pour savoir où sont leurs amis. Ils naviguent sur Internet pour leurs devoirs, pour se divertir en jouant en ligne, pour télécharger de la musique ou pour se procurer des biens et des services. Ils divulguent ainsi un certain nombre de renseignements permettant de les identifier et de les suivre à la trace. Certes ils les communiquent volontairement. Mais connaissent-ils l'usage que font de leurs renseignements personnels les responsables de sites Web commerciaux ou de réseaux sociaux? Ont-ils consenti à ce que ceux-ci se servent de leurs données à des fins de vente ou de profilage? Savent-ils dans quel pays leurs informations sont conservées et qui y aura accès? En un mot, sont-ils conscients des possibles incidents et préjudices engendrés par le dévoilement de leurs renseignements personnels, pour aujourd'hui mais aussi pour demain? En effet, dès l'instant où elle est publiée en ligne, une information devient permanente.

1 L.R.Q., c. A.2-1, ci-après « Loi sur l'accès ».
2 L.R.Q., c. P.39-1, ci après « Loi sur la protection dans le secteur privé ».

Ce constat ne vise pas uniquement les natifs du numérique. Toutefois, leur présence de plus en plus nombreuse et leur comportement face aux enjeux des technologies de l'information et du Web 2.0 quant à leurs renseignements personnels inquiètent plusieurs acteurs concernés, dont la Commission. Pour ce faire, elle recommande différentes avenues. Une première concerne la sensibilisation et l'éducation des natifs du numérique. Une seconde a trait à l'implication des entreprises face à cette problématique. Néanmoins, pour que ces avenues ne demeurent pas lettre morte, elles doivent s'accompagner d'une prise de conscience collective. En effet, la protection des renseignements personnels des jeunes est l'affaire de tous.

Notre vigilance ne doit pas être uniquement concentrée sur ce qui est divulgué sur les environnements électroniques, elle doit également s'appliquer à la sécurité des renseignements personnels. Les organismes publics et les entreprises doivent adopter des mesures de sécurité organisationnelles, humaines et techniques adaptées au contexte. Toutefois, comme nous le rappelle fréquemment l'actualité, en matière de sécurité, le « risque zéro » n'existe pas. Les organismes publics et les entreprises ne sont pas à l'abri d'incidents pouvant conduire, par exemple, à l'oubli de documents contenant des renseignements personnels dans un lieu public, à l'envoi au mauvais destinataire de correspondances d'affaires, à la conservation non sécuritaire de matériel contenant des renseignements personnels par un dépositaire chargé de les détruire ou carrément à la perte et au vol de ces documents.

Une telle faille de sécurité constitue un manquement dans la mise en œuvre et l'application des mesures de sécurité. Elle peut entraîner une perte de renseignements personnels ou encore leur accès, utilisation ou divulgation non autorisés. Elle n'est pas toujours associée aux technologies de l'information et elle peut provenir d'une simple erreur ou négligence humaine.

Une faille de sécurité est donc un phénomène dont les causes multiples appellent divers moyens de prévention. Un des moyens consiste à procéder à une analyse des risques en tenant compte du support et de la sensibilité des données. Un autre consiste à informer le personnel d'un organisme public ou d'une entreprise des mesures de protection retenues et des risques engendrés par leur non-respect. Tester régulièrement les mesures de sécurité en place et, le cas échéant, procéder aux ajustements nécessaires permet aussi aux organismes publics et aux entreprises de maintenir des mesures de sécurité efficaces et efficientes.

Par ailleurs, pour consolider l'obligation d'adopter et de maintenir des mesures de sécurité efficaces et efficientes tout au long du cycle de vie des renseignements personnels, la Commission recommande que celle-ci s'accompagne d'une obligation de lui déclarer les failles de sécurité et, dans certaines circonstances, de déclarer ces failles aux personnes concernées.

En effet, que ce soit à l'égard des organismes publics ou des entreprises, la Commission a, entre autres, pour fonctions de surveiller l'application de la loi et de s'assurer du respect de la protection des renseignements personnels. L'obligation de déclarer les failles de sécurité à la Commission s'inscrit dans cet objectif. Une telle déclaration donnerait à la Commission l’opportunité de conseiller et d’accompagner les organismes publics et les entreprises dans le choix des mesures à prendre et d’effectuer un suivi. Cela lui permettrait également de répondre adéquatement aux demandes des médias et aux éventuelles plaintes du public et de développer des documents d’information adaptés aux situations ayant causé les failles de sécurité. L’obligation de déclarer les failles de sécurité servirait à renforcer la confiance des citoyens envers les organismes publics et les entreprises qui détiennent leurs renseignements personnels et permettrait à la

Commission de mieux jouer son rôle de surveillance quant au respect de l'obligation de sécurité des renseignements personnels.

La Commission, dans son rôle de surveillance, doit pouvoir échanger avec un responsable de la protection des renseignements personnels. Si dans le secteur public, la fonction de personne responsable de l'accès aux documents et de la protection des renseignements personnels a été instaurée et a démontré son utilité au cours des 29 dernières années, pareille responsabilité ne se retrouve pas dans le secteur privé. En effet, si une entreprise est responsable actuellement des renseignements personnels qu'elle a en sa possession ou sous sa garde, rien ne l'oblige toutefois à désigner nommément une personne pour assumer cette responsabilité.

Or, les avantages liés au fait qu'une personne réponde auprès du public et de la Commission de l'application de la *Loi sur la protection dans le secteur privé* et qu'elle contribue à établir dans l'entreprise une culture de protection des renseignements personnels ne doivent pas être mésestimés. Dès lors, la Commission recommande qu'un responsable de l'accès et de la protection des renseignements personnels soit désigné dans le secteur privé. Elle est, néanmoins, consciente que les moyens pour assurer le respect de la loi peuvent varier d'une entreprise à l'autre, selon la taille de l'entreprise, la structure ainsi que la quantité et la sensibilité des renseignements personnels traités. La création de la fonction de responsable de l'accès et de la protection des renseignements personnels pourrait donc être recommandée aux entreprises comportant un seuil minimal d'employés à être déterminé par le législateur.

Toutefois, cet arrimage du secteur privé au secteur public est nécessaire pour assurer le respect des droits des personnes et pour renforcer l'application de la *Loi sur la protection dans le secteur privé*. Également, cette mise à niveau est rendue essentielle pour assurer la sensibilisation et la responsabilisation en matière de protection des renseignements personnels, particulièrement convoités à l'ère numérique.

Après avoir insisté sur l'importance de la protection des renseignements personnels, la Commission aborde, dans la seconde partie de ce rapport, des problématiques inhérentes à **l'accès aux documents des organismes publics**. Il en va ainsi du délai pour motiver un refus d'accès, de la représentation par avocat devant la Commission, de l'assujettissement à la *Loi sur l'accès* des organismes dont le fonds social fait partie du domaine public ou encore des pouvoirs d'enquête et de l'immunité des membres de la section juridictionnelle de la Commission. Il en va également du nécessaire passage de la transparence au gouvernement ouvert.

Pour ce faire, la Commission recommande que l'application du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*[3] soit étendue aux organismes publics qui en sont exemptés. Elle reconnaît que cette étape n'est pas une fin en soi et qu'il ne s'agit que d'un premier pas vers le concept de gouvernement ouvert. Elle rappelle que l'entrée en vigueur de ce règlement a permis le passage d'une divulgation réactive sur demande à une diffusion proactive de certains documents et renseignements. Toutefois, le citoyen revendique désormais de nouvelles façons de participer plus directement à la vie démocratique et d'influencer les orientations politiques. Les différentes plateformes de communication permettent de répondre à cette attente et font en sorte que l'on assiste peu à peu à un changement de paradigme. La Commission encourage donc le gouvernement à s'inscrire dans cette démarche d'ouverture inspirée de la culture d'Internet favorisant la transparence, soit la libération des données publiques, et la participation citoyenne.

3 L.R.Q., c. A-2.1, r. 0.2.

Recommandations

La protection des renseignements personnels à l'ère numérique

Recommandation 1 : La Commission recommande au législateur d'obliger les organismes publics et les entreprises à adopter des politiques de confidentialité simplifiées présentant, en termes clairs et compréhensibles, une vue d'ensemble de leurs engagements en matière de protection des renseignements personnels.

Recommandation 2 : La Commission recommande au législateur d'imposer aux organismes publics et aux entreprises l'utilisation de pictogrammes de protection informant les citoyens de leurs engagements en matière de protection des renseignements personnels.

Recommandation 3 : La Commission recommande au législateur d'obliger les organismes publics et les entreprises à signaler la présence de mécanismes susceptibles d'identifier ou de localiser une personne physique lors de l'utilisation de leurs produits.

Recommandation 4 : La Commission rappelle aux organismes publics et aux entreprises d'intégrer les principes de protection des renseignements personnels dès la conception de leurs biens et services et de les appliquer tout au long du cycle de vie de ces renseignements.

Les natifs du numérique

Recommandation 5 : La Commission recommande que le réseau de l'éducation développe des programmes scolaires au niveau du primaire et du secondaire visant à éduquer les jeunes aux enjeux des TI et du Web 2.0.

Recommandation 6 : La Commission invite le législateur à s'interroger sur la pertinence de modifier les lois de protection du consommateur ou des renseignements personnels notamment pour interdire le profilage des jeunes dans les environnements électroniques.

La déclaration des failles de sécurité

Recommandation 7 : La Commission recommande que la *Loi sur l'accès* et la *Loi sur la protection dans le secteur privé* soient modifiées par l'ajout d'une obligation de lui déclarer les failles de sécurité qui surviennent dans les organismes publics et les entreprises et qui impliquent des renseignements personnels.

Recommandation 8 : La Commission recommande que soient déterminées les conditions et les modalités conduisant à déclarer des failles de sécurité impliquant des renseignements personnels.

Recommandation 9 : La Commission recommande que lui soit confié le pouvoir d'ordonner aux organismes publics et aux entreprises d'aviser, aux conditions qu'elle déterminera, les personnes concernées d'une faille de sécurité impliquant leurs

renseignements personnels et de prendre les mesures qu'elle jugera nécessaires pour assurer une protection adéquate de leurs renseignements personnels.

La fonction de responsable dans le secteur privé

Recommandation 10 : La Commission recommande que la *Loi sur la protection dans le secteur privé* prévoit la création de la fonction de responsable de l'accès et de la protection des renseignements personnels.

Recommandation 11 : La Commission recommande que la fonction de responsable dans le secteur privé puisse être déléguée par l'entreprise à une personne œuvrant au sein de l'entreprise.

Le passage de la transparence au gouvernement ouvert

Recommandation 12 : La Commission recommande que l'application du *Règlement sur la diffusion* soit élargie aux organismes publics actuellement exemptés.

Recommandation 13 : La Commission recommande que les organismes publics soient assujettis à un régime élargi d'ouverture des données publiques qui permette l'accès libre à l'ensemble de l'information gouvernementale utile aux citoyens.

Recommandation 14 : La Commission recommande qu'un débat public regroupant l'ensemble des partenaires (parlementaires, citoyens, associations, experts) soit instauré afin d'établir un modèle pour l'ouverture du gouvernement québécois fondé sur la participation et la collaboration.

Le délai pour motiver un refus d'accès à un renseignement

Recommandation 15 : La Commission recommande de modifier la *Loi sur l'accès* afin de préciser que le délai prévu à l'article 47 pour répondre à une demande d'accès et motiver un refus sur la base d'une restriction facultative à l'accès est de rigueur et emporte déchéance.

Recommandation 16 : La Commission recommande qu'un organisme public ne puisse être relevé du défaut d'invoquer un motif de refus facultatif dans le délai de rigueur prévu pour répondre à une demande d'accès que dans des circonstances exceptionnelles, qu'il aurait le fardeau de démontrer à la Commission.

Recommandation 17 : La Commission recommande de modifier la *Loi sur la protection dans le secteur privé* afin de préciser que le délai prévu à l'article 32 pour répondre à une demande d'accès et motiver un refus sur la base d'une restriction facultative à l'accès est de rigueur et emporte déchéance.

Recommandation 18 : La Commission recommande qu'une entreprise ne puisse être relevée du défaut d'invoquer un motif de refus facultatif dans le délai de rigueur prévu pour

répondre à une demande d'accès que dans des circonstances exceptionnelles, qu'elle aurait le fardeau de démontrer à la Commission.

La représentation par avocat devant la Commission

Recommandations 19 : Devant une telle situation et sous réserve des décisions qui doivent être rendues par la Cour du Québec, la Commission suggère qu'une réflexion soit engagée avec les partenaires impliqués afin d'analyser la pertinence et la nécessité d'assouplir les exigences de la *Loi sur le Barreau* à l'égard des demandes de révision et d'examen de mésentente qui lui sont présentées par des personnes morales.

L'assujettissement des organismes dont le fonds social fait partie du domaine public

Recommandations 20 : La Commission recommande que soit modifiée la *Loi sur l'accès* afin d'assujettir tous les organismes dont le fonds social est détenu à plus de 50 % par l'État.

Les pouvoirs d'enquête et l'immunité des membres de la section juridictionnelle de la Commission

Recommandation 21 : La Commission recommande que la *Loi sur l'accès* et, par concordance, la *Loi sur la protection dans le secteur privé* soient modifiées pour accorder explicitement à tous ses membres les pouvoirs et les immunités des commissaires nommés en vertu de la *Loi sur les commissions d'enquête*.