Protection des renseignements personnels dans le secteur privé – Position du Québec d'hier à aujourd'hui

Me Christiane Constant
Commissaire – Commission d'accès à l'information[1]

The Canadian Institute's Forum on Privacy Law and Compliance

Toronto – 20 et 21 septembre 2011

Tout d'abord, je tiens, au nom de Me Jean Chartier et en mon nom personnel, à remercier les personnes qui ont participé à l'organisation de ce colloque. Me Chartier ne pouvait pas être présent aujourd'hui, car il se trouve à Dakar (Sénégal) pour une rencontre de l'*Association francophone des autorités de protection des données*[2] (AFAPDP) dont il est président depuis le mois de février 2011, soit un mois après sa nomination à titre de président de la Commission d'accès à l'information (Commission). Il m'a demandé de le remplacer, ce que j'ai accepté avec plaisir.

Ce matin, je vais vous présenter certaines des réflexions de la Commission en matière de protection des renseignements personnels dans le secteur privé. Certaines de ces réflexions sont développées dans le *Rapport quinquennal 2011* de la Commission. Ce rapport n'est pas encore publicisé. Donc, je ne pourrai

---

1 Je tiens à remercier Cynthia Chassigneux pour sa précieuse collaboration à la préparation de cette présentation.

2 Pour plus de détails sur l'Association francophone des autorités de protection des données, voir notamment la présentation qui en est faite sur le site de la Commission nationale de l'informatique et des libertés à l'adresse suivante : http://www.cnil.fr/index.php?id=112.

pas faire état des recommandations formulées par la Commission. Certaines de ces réflexions sont semblables à celles que vous avez probablement au sein de vos organismes, notamment en ce qui concerne la sensibilisation et la promotion de la protection des renseignements personnels dans le secteur privé.

Mais avant d'entrer dans le vif du sujet, je vous dirai quelques mots sur la Commission au sein de laquelle je suis commissaire depuis plus de 10 ans.

I. La Commission : structure, mandat et pouvoirs

La Commission existe depuis bientôt 30 ans. Au début, son mandat était de veiller à l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[3].

Comme le laisse entendre son titre, cette loi vise l'accès aux documents détenus par un organisme public (*c.-à-d.* ministère, organismes municipaux, organismes scolaires, établissement de santé ou de services sociaux, etc.) dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers. Elle vise également la protection des renseignements personnels contenus dans de tels documents.

En 1994, son mandat a été étendu au secteur privé avec l'entrée en vigueur de la *Loi sur la protection des renseignements personnels dans le secteur privé*[4]. Cette loi est importante pour plusieurs raisons.

---

3 R.S.Q, c. A-2.1 (« Loi sur l'accès »).

4 R.S.Q., c. P-39.1 (« Loi sur la protection dans le secteur privé»).

D'une part, elle encadre l'exercice des droits énoncés au Code civil du Québec[5] en matière de protection des renseignements personnels. D'autre part, elle fait écho aux *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* adoptées en 1980 par l'Organisation de Coopération et de Développement Économiques (OCDE)[6]. Elle a également assuré aux entreprises québécoises un niveau de protection adéquat[7] lors de l'entrée en vigueur, en Europe, en 1998, de la *Directive sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[8]. Enfin, elle a fait du Québec un pionner en Amérique du Nord en encadrant le traitement des renseignements personnels tant dans les secteurs public que privé.

Pour mener à bien son mandat, la Commission est, depuis 2006, divisée en deux sections[9] : juridictionnelle et de surveillance.

- **la section juridictionnelle** constitue le volet tribunal administratif de la Commission. Elle est composée de 5 membres, dont le président.

  Elle entend les demandes de révision en vertu de la *Loi sur l'accès*[10]. Une telle demande peut être présentée par une personne à qui un organisme a

5 R.S.Q., c. C-1991, art. 35 à 40.

6 Paris, 23 septembre 1980.

7 COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Au Québec : Les conséquences d'une directive européenne sur la protection des renseignements personnels », Fiche-conseil.

8 JO des Communautés européennes n° L281 du 23 octobre 1995, p. 31-50.

9 Pour plus de détails sur les principales activités de la Commission et sur sa structure organisationnelle, voir notamment : COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Rapport annuel de gestion 2009-2010*, Québec, Commission d'accès à l'information du Québec, 2010, pp. 17 et suiv.

refusé l'accès à un document administratif ou l'accès à des renseignements personnels qui la concernent ou leur rectification.

Elle est également saisie des demandes d'examen de mésentente en vertu de la *Loi sur la protection dans le secteur privé*[11]. Une telle demande peut-être déposée à la Commission par une personne lorsqu'une entreprise a refusé l'accès à des renseignements personnels qui la concernent ou leur rectification.

Lorsqu'elle est saisie de tels recours, la Commission peut désigner un des avocats de la section juridictionnelle pour tenter d'amener les parties à s'entendre à l'amiable[12]. En effet, depuis 2008, la Commission propose aux parties un processus de médiation. Ce processus est gratuit, confidentiel et basé sur une démarche libre et volontaire. Ce procédé a permis de réduire les délais de mise au rôle des dossiers, car plusieurs dossiers se règlent avant que ne soit émis un avis de convocation. Il convient néanmoins de préciser que la médiation et la mise au rôle sont deux processus qui se déroulent selon leur propre calendrier.

Lorsqu'un dossier est mis au rôle, les parties reçoivent un avis de convocation au moins 10 jours avant la date fixée pour la tenue de l'audition. Lors de l'audience, un des membres de la section juridictionnelle entend les représentations de chacune des parties avant de prendre la

---

10 *Loi sur l'accès*, art. 135.

11 *Loi sur la protection dans le secteur privé*, art. 42.

12 *Loi sur l'accès*, art. 138.1; *Loi sur la protection dans le secteur privé*, art. 48.

cause en délibéré. Il a alors trois mois pour rendre sa décision, à moins que le président, pour des motifs sérieux, ne prolonge ce délai. La décision est écrite et motivée et elle est susceptible d'appel devant la Cour du Québec.

• **la section de surveillance** dont je suis membre se compose de deux membres, dont le président. En effet, en vertu de la *Loi sur l'accès*, le président est assigné aux deux sections de la Commission.

Cette section est chargée de la promotion de nos deux lois auprès des organismes publics, des entreprises et des citoyens. Elle mène également des enquêtes de sa propre initiative ou à la suite d'une plainte[13].

Ces enquêtes lui permettent de s'assurer que les organismes publics ou les entreprises respectent les dispositions de la *Loi sur l'accès* et de la *Loi sur la protection dans le secteur privé*. Au terme de son enquête, la Commission peut, après avoir fourni à l'organisme public ou à l'entreprise l'occasion de présenter ses observations, recommander ou ordonner l'application de toutes mesures correctives qu'elle juge appropriées. Les ordonnances de la Commission sont exécutoires après 30 jours et sont susceptibles d'appel.

La Commission, dans l'exercice de ses fonctions de surveillance, dispose également de pouvoirs d'inspection[14]. La personne qui agit alors comme inspecteur peut entrer, à toute heure raisonnable, dans l'établissement d'un

---

13 *Loi sur l'accès*, art. 127; *Loi sur la protection dans le secteur privé*, art. 81.

14 *Loi sur l'accès*, art. 123.1; *Loi sur la protection dans le secteur privé*, art. 80.2.

organisme public ou d'une entreprise assujetti à sa juridiction. L'inspecteur peut exiger qu'on lui présente tout renseignement ou tout document requis pour l'exercice de sa fonction de surveillance et, le cas échéant en tirer copie. Ces pouvoirs lui permettent, dans un objectif de prévention et de formation, de vérifier le respect des lois qu'elle administre. Dans cette optique, la Commission a à connaître de situations relatives, entre autres, à l'installation de caméra de surveillance, à la conservation de dossiers contenant des renseignements personnels, la sécurité dans des unités de recherche.

Elle a aussi à connaître de demandes qui proviennent le plus souvent de chercheurs afin de pouvoir recevoir communication de renseignements personnels sans le consentement de la personne concernée, le tout à des fins d'étude, de recherche ou de statistiques. Nous reviendrons sur ces demandes.

Par ailleurs, la Commission a pour rôle de conseiller le législateur concernant les projets de loi ou de règlement. À ce titre, elle prépare des avis à l'intention de l'Assemblée nationale, du gouvernement et des ministères et organismes. Ces avis visent à assurer une certaine cohérence législative et réglementaire en matière d'accès aux documents des organismes publics et de protection des renseignements personnels. Ils entendent aussi faire bénéficier l'appareil administratif de l'expertise de la CAI. Ainsi, par exemple, la Commission a émis

des avis sur des projets de loi relatifs à la carte santé du Québec, au ministère du Revenu du Québec, au Code de la sécurité routière.

Elle émet également des avis sur des ententes de communication de renseignements personnels entre organismes publics, notamment dans le domaine de la santé et des services sociaux. Ou encore sur des projets de systèmes d'information et d'autres projets administratifs.

II. La Commission : actions et réflexions au fil des ans

Après ce survol du rôle et des pouvoirs de la Commission, je vais mettre l'accent sur certaines des actions et des réflexions de la Commission en matière de protection des renseignements personnels dans le secteur privé.

Comme indiqué précédemment, la Commission veille notamment au respect par les entreprises des droits et obligations énoncées dans la *Loi sur la protection dans le secteur privé*. Il en va ainsi des règles entourant la collecte des renseignements personnels et leur caractère confidentiel. Il en va aussi des règles relatives à l'accès par les personnes concernées à leurs renseignements personnels.

La Commission veille donc au respect des droits et des obligations de la collecte à la destruction des renseignements personnels, et ce, quel que soit le support envisagé. En effet, la *Loi sur la protection dans le secteur privé*, comme de nombreuses autres lois dans le domaine, est neutre technologiquement, c'est-à-dire qu'elle s'applique aux renseignements personnels 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[15].

Ainsi depuis l'adoption de cette loi, la Commission a eu à se pencher sur différentes problématiques : dossiers de crédit, dossiers d'assurance, baux de location, marketing direct, dossiers médicaux, environnements électroniques, etc. pour lesquelles elle a notamment produit des fiches-conseils, des guides ou encore des avis.

Dans le cadre de ma présentation, je ne retiendrai que certaines de ces problématiques. Quelques-unes font l'objet du *Rapport quinquennal 2011* de la Commission, c'est pourquoi je ne pourrai pas vous dévoiler aujourd'hui les recommandations faites par la Commission à leur sujet ce dernier bien que remis au ministre responsable au mois de juin dernier n'a toujours pas été publicisé.

1. Les baux de location

Comme vous le savez au Québec, le début de l'été est synonyme de déménagement pour plusieurs personnes. Ainsi, pour permettre aux locateurs et aux locataires de connaître les principes et les balises à respecter lors de la signature d'un bail de location, la Commission propose sur son site une fiche-conseil[16].

---

15 *Loi sur la protection dans le secteur privé*, art. 1(2).

16 COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Le bail et la protection des renseignements personnels : des principes et des balises à respecter », Fiche-conseil, Dernière mise à jour : juin 2010.

Elle rappelle qu'avant la conclusion du bail, le locateur peut collecter certains renseignements personnels. Toutefois, il doit le faire dans le respect du droit à la vie privée et il ne doit collecter que les renseignements nécessaires / indispensables à la conclusion du bail.

Le locateur peut donc demander au futur locataire des renseignements personnels établissant son identité ou encore permettant de vérifier son comportement ou d'établir ses habitudes de paiement, le tout avec son consentement.

Par contre, le locateur ne peut pas collecter ni le numéro d'assurance sociale ni celui qui apparaît sur le permis de conduire ou sur la carte d'assurance maladie.

2. Les environnements électroniques et leurs applications

La Commission a produit des guides sur les enjeux inhérents aux environnements électroniques et à certaines de leurs applications, notamment le courrier électronique, la technologie d'identification par radiofréquence (puces RFID)[17], l'imagerie à l'échelle de la rue.

Rappelons que la Commission, avec ses homologues du fédéral, de l'Alberta et de la Colombie-Britannique, ont publié, en avril 2009, une fiche

[17] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La technologie d'identification par radiofréquence (RFID) doit-on s'en méfier ?,* Mai 2006.

d'information intitulée *Vous êtes photographiés* sur la technologie de l'imagerie à l'échelle de la rue[18].

Il y est fait mention que même si les autorités de protection « recognize the popularity of these applications, they have also expressed reservations because the technology captures images not just of places, but of people as weel »[19].

Ainsi, il est rappelé que

> « in addition to companies being proactive and creative in their public communications to ensure that Canadians know when their cities – and, therefore, they themselves – may be photographed, we think these companies need to be more privacy sensitive in the areas they choose. […] They should also use proven and effective blurring technologies for faces and vehicle licence plates, so that people cannot be identified when their images are posted. Where individuals may be identifiable, companies must offer fast and responsive mechanisms to allo the images to be blocked or taken down. Companies […] must also hace a good reason to keep the original, unblurred images in their databanks. If the do retain unblurred images, they must limit how long they keep them and protect them with appropriate security measures. »[20]

---

18 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, INFORMATIONS AND PRIVACY COMMISSIONER OF ALBERTA, INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Captured on Camera - Street-level imaging technology, the Internet and you », Fact Sheet, April 2009.

19 *Id*.

20 *Id*.

À l'été 2009, ces mêmes autorités de protection ont fait parvenir une lettre[21] à *Google Inc*. concernant son application *Google Street View* dans laquelle elles indiquent :

> « we would again highlight the need for knowledge and consent – you must let citizens know that they are going to be photographed, when, why, and how they can have their image removed. »[22]

La Commission continue à s'intéresser à l'imagerie à l'échelle de la rue d'autant plus que les voitures et les caméras de *Google Inc*. sont depuis quelques semaines de retour dans les rues de Montréal.

3. La biométrie

La Commission s'intéresse également à la biométrie, notamment lorsque celle-ci a pour but de vérifier ou de confirmer l'identité d'une personne. En effet, si une entreprise souhaite créer une banque de caractéristiques ou de mesures biométriques elle doit préalablement en aviser la Commission[23].

Cette obligation existe depuis 2001. Elle est inscrite dans *Loi concernant le cadre juridique des technologies de l'information*.

---

21 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, INFORMATIONS AND PRIVACY COMMISSIONER OF ALBERTA, INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Letter to Google Inc. regarding the company's proposed retention plan for images collected for its StreetView application », August 21, 2009.

22 *Id*.

23 *An Act to establish a legal framework for information technology*, R.S.Q., c. C-1.1, art. 45(1).

Ainsi, pour aider les entreprises, mais aussi les organismes publics, dans leurs démarches, la Commission propose sur son site un *Formulaire de déclaration d'une banque de caractéristiques ou de mesures biométriques*.

Dès lors, l'entreprise qui souhaite mettre en place une telle banque doit notamment faire état du consentement de la personne dont l'identité sera ainsi vérifiée ou confirmée et transmettre le formulaire de consentement utilisé à la Commission.

Elle doit également préciser les raisons pour lesquelles elle recourt à la biométrie et indiquer quelles sont les caractéristiques qui seront ainsi collectées (empreintes digitales, forme de la main, du visage, reconnaissance de l'iris, de la voix, de la signature, etc.). Elle doit dire si un mode alternatif est envisagé.

Elle doit faire état des mesures de sécurité adoptées pour protéger la banque et des droits d'accès et de rectification accordés à la personne concernée.

Elle doit, le cas échéant, annexer à sa déclaration l'analyse de risques et d'impacts en regard de la sécurité et de la protection des renseignements personnels réalisée.

Après analyse, la Commission peut rendre toute ordonnance quant à la confection, l'utilisation, la consultation, la communication et la conservation

de telles applications[24]. Elle peut également suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction[25].

Pour l'heure, les déclarations soumises à la Commission portent principalement sur des empreintes digitales et la forme de la main à des fins d'*horodatage* ou encore d'accès à des lieux contenant des médicaments, des dossiers médicaux… ou à des parcs d'attractions où votre empreinte digitale associée à votre numéro de carte de crédit vous permet de payer vos activités, vos collations du bout des doigts tout en laissant votre carte de crédit au vestiaire.

4. Les demandes à des fins d'étude, de recherche ou de statistiques

Comme mentionné précédemment, la Commission peut autoriser une personne à recevoir à des fins d'étude, de recherche ou de statistique, communication de renseignements personnels sans le consentement de la personne concernée[26]. Ces demandes représentent une grande part de mon travail. En effet, la Commission reçoit en moyenne 200 demandes d'autorisation par année.

Voici le parcours d'une demande d'autorisation avant qu'elle n'arrive sur mon bureau. Le chercheur fait parvenir le *Formulaire de demande d'autorisation de recevoir des renseignements personnels à des fins de recherche, d'étude ou de statistique*, disponible sur notre site, à la

24 *Id*., art. 45(2).
25 *Id*., art. 45(3).
26 *Loi sur l'accès*, art. 125; *Loi sur la protection dans le secteur privé*, art. 21.

Commission. Dès sa réception, un dossier est ouvert et est assigné à l'un des analystes de la section surveillance.

L'analyste étudie alors la demande au regard du formulaire transmis par le chercheur, du protocole de recherche, de l'engagement de confidentialité, de l'avis d'un Comité d'éthique à la recherche et de tout autre document communiqué par le chercheur.

Dans le formulaire, le chercheur aura indiqué, entre autres, l'organisme détenteur des renseignements, l'objet de la recherche, la taille de l'échantillon, les étapes de la recherche, les renseignements personnels qu'il estime nécessaire à sa recherche, les mesures de sécurité envisagées, les raisons pour lesquels il ne peut pas obtenir le consentement des personnes concernées.

Par contre, si le chercheur a obtenu un consentement, il peut le transmettre à la Commission qui vérifiera si ce dernier répond aux exigences du consentement, à savoir s'il est manifeste, libre, éclairé, donné à des fins spécifiques et pour la durée nécessaire à la réalisation de ces fins.

L'analyste peut également faire des démarches supplémentaires, par exemple effectuer une revue de littérature sur le sujet, prendre contact avec le chercheur pour valider sa compréhension du projet de recherche et des renseignements requis.

Une fois que l'analyste a fini d'examiner le projet au regard des droits et des obligations contenus dans la *Loi sur l'accès* et dans la *Loi sur la protection dans le secteur privé*, mais aussi le cas échéant dans d'autres lois, il rédige une note à l'intention du directeur de la section de surveillance. Ce dernier, s'il n'a pas de questions, me transmet le dossier.

Je prends alors connaissance de la demande et de l'analyse avant de rendre ma décision en m'assurant que l'usage projeté n'est pas frivole, que les fins recherchées ne peuvent être atteintes que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes, que les renseignements seront utilisés d'une manière qui en assure le caractère confidentiel.

Il est à noter que je peux autoriser la communication des renseignements personnels sous certaines conditions et, que dans certains cas une autorisation peut être retirée si nous nous apercevons que le chercheur ne respecte pas la confidentialité des renseignements personnels ou encore les conditions qui lui ont été fixées.

5. Le consentement

En 2006, l'étendue du consentement a été modifiée dans la *Loi sur la protection dans le secteur privé*. En effet, la notion de « consentement à la collecte » est venue s'ajouter au « consentement à la communication ou à l'utilisation »[27]. Le consentement doit donc désormais être considéré tout au long du cycle de vie des renseignements personnels.

Comme indiqué précédemment, le consentement doit être donné par une personne capable d'exprimer sa volonté ou par son représentant. Il doit être libre et éclairé. Il doit être donné à des fins spécifiques et pour la durée nécessaire à la réalisation de ces fins.

Sur la question du consentement à la collecte, la Commission, comme plusieurs de ses homologues, est d'avis qu'il convient de redéfinir les moyens de présenter et de communiquer les engagements des entreprises en matière de protection des renseignements personnels.

En effet, il serait naïf de considérer que le fait 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 de type *Facebook* ou *Twitter*.

---

27 *Loi sur la protection dans le secteur privé*, art. 14. Il est à noter que pareille disposition ne se retrouve pas dans la Loi sur l'accès. Toutefois, la Commission applique les critères reconnus dans la *Loi sur la protection dans le secteur privé* au secteur public.

Partant, même si ces politiques sont longues, manquent de clarté et ne sont pas compréhensibles, elles demeurent néanmoins un outil informationnel à considérer. C'est pourquoi la Commission mène une réflexion sur la présentation de ces politiques de confidentialité et sur la matérialisation du consentement à la collecte.

Cette réflexion a également lieu au sein de l'organisme américain indépendant de régulation du commerce, soit la *Federal Trade Commission*[28], du Commissariat à l'information et à la protection de la vie privée de l'Ontario[29], du Groupe de travail de l'article 29[30] en Europe. Elle interpelle aussi l'ensemble des autorités de protection comme l'illustre une résolution adoptée, en 2003, visant l'amélioration des pratiques d'information en matière de protection des données et de la vie privée[31].

La Commission continue également sa réflexion sur l'information à transmettre aux personnes utilisant des objets susceptibles de les localiser et de les identifier. Nous n'avons qu'à penser à la biométrie comportementale qui permet d'identifier un individu en utilisant entre autres sa manière d'utiliser la souris de son ordinateur ou encore sa démarche, au

---

28 FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymarkers*, December 2010.

29 INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *Response to the FTC Framework for Protection Consumer Privacy in an Era of Rapid Change*, January 2011.

30 ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 15/2011 on the definition of consent*, WP187, July 13, 2011.

31 *Resolution on Improving the Communication of Data Protection and Privacy Information Practices*, 25th International Conference of Data Protection and Privacy COmmissioners, Sydney (Australia), September 2003.

GPS, aux puces RFID, à la reconnaissance faciale, aux vélos *Bixi* de Montréal ou de Toronto, aux différentes applications de votre téléphone intelligent ou encore à la vidéosurveillance.

Il est, en effet, nécessaire que les entreprises qui développent et recourent à de telles technologies s'assurent que les utilisateurs ont compris et consentent à ce que celles-ci puissent les localiser et les identifier en tout temps.

Par exemple, en matière de vidéosurveillance, la Commission a établi certaines règles. Certes, ces règles sont énoncées pour le secteur public, mais elles trouvent également application dans le secteur privé avec les adaptations nécessaires.

En ce moment, j'ai sur mon bureau un dossier de plainte contre une entreprise qui a installé plusieurs caméras de surveillance dans ses locaux.

Je dois donc me prononcer sur le fait de savoir si le recours à la vidéosurveillance par cette entreprise est nécessaire. S'il sert un objectif sérieux et légitime. Je dois également considérer si l'entreprise a envisagé des moyens alternatifs ou encore si elle a réalisé une analyse quant aux répercussions d'un tel procédé sur la sécurité et la protection de la vie privée. Je dois aussi m'assurer qu'elle a élaboré une politique d'utilisation, qu'elle a informé ses employés du recours à un tel procédé. Et, je dois considérer les mesures de sécurité mises en place.

6. La sécurité

La sécurité est un principe fondamental en matière de protection des renseignements personnels. Les entreprises, mais aussi les organismes publics, doivent respecter ce principe et adopter des mesures de sécurité propres à assurer le caractère confidentiel des renseignements.

Ce principe a été renforcé en 2006, tant dans les secteurs publics que privé. Ainsi la *Loi sur la protection dans le secteur privé* a été modifiée afin d'insister sur la nécessité d'adopter des mesures de sécurité « qui sont raisonnables compte tenu, notamment, de [la] sensibilité [des renseignements personnels], de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support »[32].

Le respect de cette obligation prend tout son sens aujourd'hui au regard des nombreuses failles de sécurité – *Sony*, *Facebook*, *Apple* – qui ont fait la une des journaux ces derniers mois faisant en sorte que certains journalistes qualifient 2011 comme étant l'année des failles de sécurité.

Face à cette problématique, la Commission regarde ce qui se fait ailleurs dans le cadre de sa réflexion sur cette question. En effet, par exemple, aux États-Unis, depuis 2002, la Californie s'est dotée d'une loi qui impose aux organismes publics et aux entreprises l'obligation de déclarer aux personnes concernées les failles de sécurité[33]. Notons que cette loi vient

---

32 *Loi sur la protection dans le secteur privé*, art. 10.

33 *Cal. Civ. Code*, 1798.29 et 1798.82.

d'être modifiée[34]. Ainsi, à partir du 1er janvier 2012, toute faille de sécurité visant plus de 500 résidents californiens devra être déclarée au procureur général et toute déclaration faite aux personnes concernées devra contenir un certain nombre d'informations à savoir :

- *the name and contact information of the reporting agency subject to this section;*
- *a list of the types of personal information that were or are reasonably believed to have been the subject of a breach;*
- *if the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice;*
- *a general description of the breach incident, if that information is possible to determine at the time the notice is provided;*
- *the toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.*

En Alberta, depuis mai 2010, les organisations doivent déclarer à l'*Office of the Information and Privacy Commissioner* (OIPC) « any incident involving the loss of or unauthorized access to or disclosure of the personal information »[35]. Cette déclaration doit se faire dès qu'il existe un risque réel de préjudice important pour un individu en raison de la perte, de l'accès non autorisé ou de la divulgation. Dès lors, l'OIPC peut recommander à l'organisation d'aviser les personnes concernées par cet évènement. Il est

34 *Senate Bill n°24* (An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information).

35 *Personal Information Protection Act*, S.A. 2003, c. P-6.5, art. 34.1(1).

à noter que les organisations conservent, en tout temps, la possibilité d'aviser les personnes concernées de leur propre chef[36].

En Europe, les États membres avaient jusqu'au 25 mai 2011 pour transposer dans leurs législations une disposition selon laquelle les failles de sécurité doivent être dénoncées à l'autorité nationale compétente et aux personnes concernées. Ainsi, depuis la fin août, soit avec quelques mois de retard, on peut désormais lire dans la loi française « Informatique et Libertés » que

> « En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés.
>
> Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé.
>
> La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.
>
> À défaut, la Commission nationale de l'informatique et des libertés peut, après avoir examiné la gravité de la violation, mettre en demeure le fournisseur d'informer également les intéressés. »[37]

---

36 *Id*., art. 37.1(7).

37 *Loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés*, art. 34 bis (II).

Comme vous pouvez vous en douter, il s'agit d'une problématique qui interpelle la Commission. Notons que pour l'heure, au Québec, cette déclaration se fait sur une base volontaire.

Par exemple, nous avons reçu des déclarations concernant la perte de différents supports (disques durs, documents papier, clés USB) lors de déplacements, l'accès non autorisé à des renseignements via Internet, la mise aux rebuts non sécuritaire de matériel contenant des renseignements personnels.

Pour nous déclarer leur faille de sécurité, les entreprises peuvent se référer à un *Aide-mémoire*[38] développé par la Commission précisant qu'en plus de contacter la Commission et les personnes concernées, il peut être nécessaire, selon le cas, d'aviser la police, les assureurs, les ordres professionnels, les banques et les agences de crédit. Il indique également quand et comment informer la Commission et les personnes concernées. Il rappelle surtout l'importance de circonscrire rapidement le problème et de mettre en place des mesures pour éviter qu'une telle situation ne se reproduise, notamment en testant régulièrement les mesures de sécurité en place et, le cas échéant, en procédant aux ajustements nécessaires ce qui permet de maintenir des mesures efficaces et efficientes.

---

38 COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Aide-mémoire à l'intention des organismes et des entreprises – Que faire en cas de perte ou de vol de renseignements personnels ?*, Avril 2009. Voir également, COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Aide-mémoire à l'intention des citoyens – Perte ou vol de renseignements personnels : comment réagir ?*, Avril 2009.

7. Les jeunes

Enfin depuis plusieurs années, la Commission participe à différentes activités visant à informer les jeunes des dangers liés aux environnements électroniques. En effet, ils recourent aux blogues, à *Twitter*, à *MySpace* ou encore à *Facebook* pour communiquer avec leurs amis, 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.

Par le fait même, ils divulguent un certain nombre de renseignements permettant de les identifier et de les suivre à la trace. Certes, ils communiquent ces informations volontairement. Mais connaissent-ils l'usage que font de leurs renseignements personnels les responsables de sites Web commerciaux ou des réseaux sociaux? Savent-ils dans quels 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?

Rappelons que face à l'engouement toujours grandissant des environnements électroniques, les commissaires à la protection des

données et de la vie privée, réunis en conférence internationale, ont adopté la *Résolution sur la vie privée des enfants en ligne*[39].

Cette résolution met l'accent sur la nécessaire collaboration entre les gouvernements, les entreprises et les autorités de protection des consommateurs et de protection des renseignements personnels pour développer des outils permettant d'éduquer et de sensibiliser les jeunes aux risques liés à l'utilisation des environnements électroniques. Elle insiste également sur l'importance d'adopter des moyens visant à limiter ou à interdire le traitement des renseignements personnels notamment à des fins publicitaires. Elle recommande aussi aux responsables des sites Web ou des réseaux sociaux d'adapter leur politique de confidentialité à ce public.

Dès lors, dans le but de promouvoir la protection de leurs renseignements personnels auprès des jeunes, la Commission diffuse du matériel produit par l'*Association francophone des autorités de protection des données personnelles* (AFAPDP), association qui, rappelons-le, est présidée par le président de la Commission.

Il s'agit d'un signet, d'une affiche et d'un dépliant sur le thème *Internet : C'est moi qui décide !* qui présentent des « trucs et des astuces » pour éviter les pièges des environnements électroniques. Ce matériel tend à responsabiliser les jeunes. En effet, les informations qu'ils publient sur

39 *Resolution on Children's Online Privacy*, 30th International Conference of Data Protection and Privacy Commissioners, Strasbourg (France), October 2008.

Internet constituent des renseignements personnels sur eux, leur famille et leurs amis. Internet et le Web 2.0 étant de véritables terrains de jeux pour les jeunes, cette documentation vise à leur donner les outils nécessaires pour les aider à faire les bons choix, à comprendre les conséquences de leurs activités en ligne et à développer une certaine « pudeur numérique ».

La diffusion de ce matériel par la Commission s'inscrit dans son rôle de promotion de la protection des renseignements personnels. Cette façon de faire correspond aussi à l'approche de plusieurs autorités de protection, que l'on pense au site « ma vie privée. mon choix. ma vie » du Commissariat à la protection de la vie privée du Canada ou encore aux applications développées, en France, par la Commission nationale de l'informatique et des libertés, permettant d'apprendre « à rester net sur le web! » .

La sensibilisation des jeunes à la problématique « renseignements personnels et environnements électroniques » est une chose. Pour être complète, elle doit s'accompagner d'une sensibilisation de l'ensemble des acteurs : jeunes, milieu scolaire, parents, entreprises, etc. C'est pourquoi la Commission est en discussion avec certains de ces acteurs. Mais pour le moment, vous comprendrez qu'il m'est difficile d'en dire davantage.

Voici donc quelques-unes des actions et des réflexions de la Commission en matière de protection des renseignements personnels dans le secteur privé.

Actions et réflexions qui doivent tenir compte de la rapidité avec laquelle les choses évoluent de nos jours et qui doivent tenir compte des expériences menées ici et ailleurs.

C’est pourquoi je tiens encore à dire combien je remercie les personnes qui ont participé à l’organisation de ce colloque qui permet de discuter sur des problématiques qui nous interpellent tous.

En terminant, je tiens à vous remercier pour votre attention.