

**CONFÉRENCE DE M^e CHRISTIANE CONSTANT
COMMISSAIRE
COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC**

PORTANT SUR LE THÈME:

« ATTENTION! RENSEIGNEMENTS PERSONNELS EN CIRCULATION ... »

ORGANISÉE PAR :

L'ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION

À QUÉBEC

LES 23 ET 24 AVRIL 2008

Monsieur le Président,

Au nom de M^e Jacques Saint-Laurent, président de la Commission d'accès à l'information (la Commission), qui se trouve présentement en Commission parlementaire, je vous remercie de m'avoir invitée à participer au 16^e congrès de l'Association sur l'accès et la protection de l'information (l'AAPI) ayant pour thème « Attention! Renseignements personnels en circulation... ».

Nous vivons dans une société où la surveillance de personnes a toujours existé; elle prend diverses formes et les renseignements personnels concernant ces personnes peuvent être recueillis ou colligés en tout temps et à leur insu.

Tout d'abord, il est opportun de rappeler qu'au Québec, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*¹ et la *Loi sur la protection des renseignements personnels dans le secteur privé*² nous définissent ce qu'est un renseignement personnel. On peut souligner, en quelques mots, qu'il s'agit d'un renseignement concernant une personne physique permettant de l'identifier et qui se trouve dans un document, peu importe sa forme, qu'il soit électronique ou en format papier.

Pour que la Commission exerce la compétence qui lui est conférée dans sa Loi statutaire, un renseignement personnel concernant une personne physique doit se trouver dans un document.

En matière d'accès, une personne a un droit d'avoir accès à tout document qui la concerne. Il appartient à l'organisme ou l'entreprise de faire connaître à cette personne les motifs pour lesquels il refuse de lui transmettre ce document, sous réserve de certaines dispositions législatives.

En matière de surveillance, ce ne sont ni les mêmes critères ni les mêmes règles qui s'appliquent. Nous y reviendrons un peu plus loin.

Mais en fait, que signifie le mot « surveillance »? Le dictionnaire *Le Petit Larousse illustré*³ nous informe qu'il s'agit de l'action de « surveiller ». Ce mot réfère à l'action d'« observer attentivement pour contrôler ».

Les entreprises et organismes gèrent et manipulent quotidiennement des quantités énormes de renseignements personnels concernant des citoyens. Ils s'intéressent donc à la vie privée de ces citoyens. L'on ne peut pas traiter de la vie privée sans retenir les dispositions de la *Charte des droits et libertés de la*

¹ L.R.Q., c. A-2.1, la Loi sur l'accès.

² L.R.Q., c. P-39.1, la Loi sur le privé.

³ Édition 2002.

*personne*⁴ qui spécifient notamment que « *toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation* ». La Charte prévoit également que « *toute personne a droit au respect de sa vie privée* ». Ces éléments essentiels et incontournables doivent demeurer constamment à l'esprit du gestionnaire, de l'employé et de toute autre personne à chaque fois qu'il est question de traitement de ces renseignements. Ce n'est pas toujours le cas.

La surveillance de personnes implique la collecte des renseignements personnels, de la communication, de l'utilisation, de la conservation et de la destruction des renseignements détenus par un organisme public ou une entreprise privée. Ces organismes doivent prendre des mesures de sécurité adéquates afin de voir à la protection de ces renseignements.

La Commission, étant l'autorité chargée de l'application de la Loi sur l'accès et de la Loi sur le privé au Québec, fait tout en son pouvoir pour s'assurer que les dispositions de ses lois soient respectées. De plus, depuis l'adoption du projet de loi 86 au mois de juin 2006, la Commission est notamment chargée d'assurer le respect et la promotion de l'accès aux documents et de la protection des renseignements personnels. Aussi, dans l'exercice de ses fonctions de surveillance, la Commission possède le pouvoir d'autoriser un membre de son personnel ou toute personne à agir comme inspecteur à l'égard d'un organisme ou d'une entreprise privée.

LA SURVEILLANCE

La surveillance de personnes dans les lieux publics et privés prend une dimension plus importante qui nous interpelle tous. C'est une réalité pour la plupart d'entre vous qui êtes des experts en matière d'accès à des documents et en matière de surveillance, mais il ne faut pas prétendre tout savoir puisque les nouvelles technologies de l'information, telles que l'Internet, la biométrie, l'identification par radiofréquence et la vidéosurveillance nous incitent, ou plutôt, nous obligent tous à parfaire nos connaissances afin de faire face à cette réalité étendue à l'échelle planétaire.

La surveillance comporte notamment la création d'une base de données existant sous forme papier et l'utilisation des nouvelles technologies de l'information capables de communiquer, en très peu de temps, des renseignements personnels concernant un nombre incalculable d'individus. Chacune de ces technologies présente des enjeux différents eu égard à la protection des renseignements personnels de façon collective et individuelle.

⁴ L.R.Q., c. C-12.

Ces nouveaux moyens de communication exigent de s'interroger, notamment, sur le critère de nécessité pour un organisme public ou une entreprise de collecter des renseignements personnels concernant un citoyen. Cette cueillette doit être nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont cet organisme a la gestion.

La surveillance visant la collecte, la communication, l'utilisation et la conservation des renseignements personnels est souvent effectuée dans un but spécifique pour son auteur. La Commission possède une obligation légale d'intervenir. Il appartient donc à l'organisme ou à l'entreprise de démontrer que cette collecte, cette communication, cette utilisation et cette conservation de renseignements sont nécessaires et qu'il n'existe pas d'autres moyens pour les obtenir.

Il est opportun de rappeler qu'en règle générale, l'installation d'une nouvelle technologie de l'information dans un lieu public ou privé vise à protéger les intérêts de celui qui l'a installée ou qui l'a fait installer. Lorsqu'il s'agit notamment de collecter de façon habituelle ou systématique des renseignements personnels concernant des citoyens, on parle de surveillance, qu'elle soit nécessaire ou non. Considérant l'importance et l'ampleur de ce sujet, j'ai pensé vous entretenir particulièrement du domaine de la vidéosurveillance, de la protection des renseignements personnels et de la vie privée des individus.

LA VIDÉOSURVEILLANCE

Le principe de base est qu'on ne doit pas capter les images d'une personne ni recueillir des renseignements personnels la concernant sans son consentement.

Dans cette société de surveillance où nous vivons, ce n'est pas toujours le cas. L'on a qu'à garder à l'esprit les citoyens qui se surveillent les uns les autres, ceux qui se donnent la permission de le faire, les organismes publics et entreprises privées qui utilisent notamment les nouvelles technologies de l'information afin de recueillir les renseignements personnels sur des personnes.

L'installation de la vidéosurveillance dans les lieux publics nécessite une attention particulière puisqu'il faut connaître, notamment, l'endroit où elle est installée, savoir si les images captées sont enregistrées, qui est responsable de l'enregistrement, la formation de la personne en matière de confidentialité et de protection de renseignements personnels, quelles sont les finalités recherchées de manière à s'assurer que l'utilisation de cette surveillance ne porte pas atteinte à la vie privée des citoyens qui y apparaissent, d'autant plus que cela se fait sans leur consentement.

La Commission considère que la vidéosurveillance doit être installée après que tous les efforts concrets aient été déployés par l'organisme qui n'a pu obtenir les résultats escomptés concernant une problématique précise et que cette vidéosurveillance soit le seul moyen qui lui permette d'arriver à cette fin.

Par exemple, la direction d'une école, faisant partie d'une commission scolaire, décide de procéder à l'installation de caméras à l'intérieur et à l'extérieur de son établissement. Dans le cadre d'une enquête menée par la Commission auprès de la direction de cette école, il en est ressorti, essentiellement, que les motifs invoqués visent à contrer les méfaits causés par certains étudiants à l'égard des biens mobiliers et immobiliers appartenant à la Commission scolaire. Ainsi, l'installation de cette vidéosurveillance permettrait d'identifier les étudiants qui commettent des délits, tels le vol, le vandalisme, l'intimidation à l'endroit d'autres étudiants et d'enseignants et elle aurait un effet dissuasif sur les auteurs de ces délits.

Au cours de son enquête, l'enquêteur désigné par la Commission a notamment vérifié si les 20 *Règles minimales d'utilisation des caméras de surveillance* avaient été respectées. Je vais commenter quelques-unes d'entre elles :

1. *L'organisme doit démontrer que l'objectif recherché par l'usage de la vidéosurveillance est sérieux et important.*
2. *Il doit indiquer de façon concrète quel est le but recherché.*
3. *Un rapport doit être réalisé concernant les risques concrets et les dangers réels que présente une situation au regard de l'ordre public et de la sécurité des personnes, des lieux ou des biens. Cet organisme doit donc être en mesure de démontrer et d'identifier notamment les événements dont il se plaint qui ont été produits dans son établissement ou sur son territoire, l'étendue du problème et les gestes qu'il a posés afin d'enrayer ce problème.*
4. *Des solutions de rechange moins préjudiciables à la vie privée doivent avoir été envisagées ou mises à l'essai et s'être avérées inefficaces, inapplicables ou difficilement réalisables. L'organisme doit être capable de démontrer par ailleurs que la vidéosurveillance ne vise pas à remplacer ou court-circuiter d'autres moyens humainement et matériellement disponibles et acceptables, lesquels sont déjà mis en place pour assurer la sécurité des citoyens. Ces moyens doivent demeurer. Conséquemment, la vidéosurveillance devient un apport supplémentaire.*

5. *L'impact réel de la vidéosurveillance doit être mesuré.* L'organisme doit être en mesure de fournir des précisions eu égard au résultat atteint par rapport au résultat escompté.
6. *L'organisme public doit s'assurer de la légitimité de ses objectifs de sorte que la finalité de la vidéosurveillance ne puisse être détournée ou déformée.*
7. *La finalité de la vidéosurveillance doit être transparente et explicite. Il est essentiel que l'organisme consulte les intervenants impliqués dans le domaine.* Dans le cas de l'exemple que je vous ai soumis concernant l'école, la direction de l'école doit préalablement consulter le conseil d'établissement et le conseil étudiant afin de connaître leur point de vue eu égard à l'installation de la vidéosurveillance.
8. *La vidéosurveillance doit être considérée avec au moins un des éléments déjà énoncés, telles des solutions de rechange moins préjudiciables à la vie privée du citoyen.* Elle ne doit pas être vue comme la seule solution.
9. *En ce qui a trait aux règles relatives à la collecte des renseignements,* l'organisme public doit désigner au départ une personne responsable de la collecte, de la conservation et de la communication des données recueillies au moyen de la surveillance.
10. *La vidéosurveillance doit être ajustée au besoin et adaptée à la situation.* L'organisme public doit circonscrire son usage. La Commission estime qu'il faut avoir un juste équilibre entre la protection des renseignements, la vie privée et la sécurité. Il est essentiel de connaître les périodes couvertes par l'enregistrement en continu.
11. *La vidéosurveillance doit être utilisée uniquement lors d'évènements critiques et pour des périodes limitées.* Cet appareil ne doit pas être en marche 24 heures sur 24 et 7 jours sur 7. Il doit être programmé de manière à ce que les enregistrements soient faits durant une période précise. En dehors de ces heures, la caméra peut seulement être activée par un détecteur de mouvement. Il est de plus essentiel que la personne responsable de la collecte des données soit en mesure de visionner ce qui se passe à un moment spécifique.
12. *Seuls les enregistrements nécessaires doivent être effectués.*

13. *La disposition des caméras et le type de technologie utilisée doit minimiser les effets de la surveillance sur la vie privée des gens.* Il ne doit pas y avoir de caméras branchées vers un endroit qui concerne strictement la vie privée des citoyens.
14. *Les personnes assurant le fonctionnement des appareils doivent être bien au fait des règles visant à protéger la vie privée.* Celles manipulant les caméras doivent avoir reçu une formation relativement aux principes et aux règles de la protection des renseignements personnels. Aussi, il est important qu'elles connaissent ce qui peut porter atteinte à la vie privée et les conséquences qui en découlent.
15. *Le public visé par cette surveillance doit être informé par avis approprié.* Il est essentiel d'informer le public que des caméras sont installées à tel endroit et que cet endroit fait l'objet d'une surveillance et d'enregistrement. L'affichage doit également identifier le responsable de la vidéosurveillance et le numéro de téléphone pour le joindre.
16. *Concernant les règles de gestion des renseignements, il est primordial que les équipements utilisés pour l'enregistrement et les enregistrements soient protégés.* La Commission considère que le système d'enregistrement doit être placé sous clé dans un endroit accessible uniquement aux personnes autorisées qui sont en charge de ce système. Le visionnement des enregistrements doit se faire dans le poste de surveillance et être accessible uniquement au responsable de la vidéosurveillance.
17. *L'utilisation des enregistrements doit être limitée.* Par exemple, le visionnement des enregistrements doit se faire uniquement et exclusivement par le responsable et lors d'évènements qui le nécessitent.
18. *Les supports d'enregistrement doivent être pris en compte dans le calendrier de conservation.* Exemple, les images captées seront conservées par l'organisme pendant combien de temps? Une fois que l'enregistrement est fait, l'on ne doit pas être en mesure de les reproduire ni de remonter aux enregistrements qui ont été effectués précédemment.
19. *Une personne a droit d'accès aux renseignements la concernant.* L'organisme doit informer le citoyen de son droit d'avoir accès aux enregistrements qui la concernent, en vertu de la Loi sur l'accès ou la Loi sur le privé, s'il s'agit d'une entreprise privée, pour la période selon laquelle ces enregistrements sont conservés. Il doit également informer

ce citoyen de la procédure à suivre afin qu'il puisse visionner l'enregistrement le concernant. Il pourra également faire une demande de rectification, le cas échéant.

Pour la Commission, la décision de recourir à la vidéosurveillance doit être revue périodiquement.

20. *L'organisme public doit revoir périodiquement (au minimum sur une base annuelle) la nécessité de ses choix en matière de vidéosurveillance.* Il s'agit d'une évaluation annuelle qui doit être assez précise, de manière à ce que l'organisme soit capable de faire des comparaisons pouvant considérer ou examiner des éléments qui ont conduit à l'installation de la vidéosurveillance dans son établissement ou sur son territoire. Par exemple :

- Le type d'incident et de méfait;
- L'endroit où se sont produits ces incidents et méfaits;
- Le nombre de personnes (ou d'élèves) qui y étaient impliqués;
- La portion des méfaits identifiés à l'aide de caméras.

Dans le cas de l'école ayant servi comme exemple, l'enquête a démontré que les recommandations émises par la Commission ont permis à l'école de prendre les mesures qui s'imposent dans le respect des 20 règles établies auxquelles je vous ai référées précédemment.

Aussitôt que les fins pour lesquelles ces caméras ont été installées sont satisfaites, l'organisme doit cesser de les utiliser.

Parmi les enquêtes menées par la Commission impliquant l'installation de la vidéosurveillance dans un lieu public, l'organisme désireux de procéder ainsi fait souvent ressortir qu'il s'agit d'une question de sécurité pour les citoyens; ces derniers, sachant que l'endroit par lequel ils passent est muni d'une vidéosurveillance se sentent en sécurité, ils sont d'accord et n'ont rien à cacher. Néanmoins, on peut se demander s'il s'agit d'une réelle sécurité ou d'une apparence de sécurité? Cette notion mérite que l'on s'y attarde un peu.

En fait, que signifie le mot « sécurité » ? Sécurité peut comporter deux significations : L'une objective, c'est-à-dire une personne qui n'est exposée à aucun danger⁵ :

⁵ Le Petit Larousse illustré, Édition 2002, p. 928.

Ensemble des mesures législatives et administratives qui ont pour objet de garantir les individus et les familles contre certains risques [...].

Le mot « sécurité » peut également comporter une interprétation subjective : en tenant compte de la culture d'une personne, sa langue, son niveau sociologique, etc. L'une des valeurs fondamentales en démocratie c'est le respect de la vie privée. Une personne ne peut être constamment sous surveillance, un juste équilibre entre la « sécurité » et le respect de la vie privée doit exister.

Il faut toujours se rappeler qu'avant de procéder à l'installation d'une vidéosurveillance dans un lieu public, le critère de nécessité doit être l'élément primordial à examiner, d'autant plus qu'elle peut constituer une méthode pour suivre à la trace un citoyen. Ce moyen ne doit pas être intrusif sur le plan de la vie privée des individus concernés étant donné les fins visées et le contexte ayant donné lieu à l'installation de cette vidéosurveillance compte tenu des renseignements personnels enregistrés.

Une autre forme de surveillance dont j'aimerais vous entretenir est la technologie concernant des cartes à puce. Ce système est répandu dans divers domaines, notamment dans le domaine du transport en commun. Une étude réalisée en septembre 2004 par la Revue Card Technology⁶ démontre que l'utilisation de ce système a connu une augmentation de 20%, ce qui représente en quelque sorte 75 millions de cartes dans près de 30 pays.

Au Québec, la Société de transport de l'Outaouais avait mis sur pied un tel système qui devait être utilisé par l'ensemble de ces usagers. Tel qu'il est indiqué dans le rapport final « l'instauration de ce système n'est pas sans soulever certains enjeux en matière de protection des renseignements personnels dans la mesure où plusieurs renseignements personnels sont recueillis. » La Commission a décidé de mener une enquête conformément à la Loi sur l'accès.

Pour les représentants de cette société, ce système avait deux objectifs principaux : donner un meilleur service à la clientèle composé d'étudiants, de personnes adultes et d'aînés et ainsi pouvoir améliorer leurs opérations.

Sans entrer dans tous les détails de l'enquête, il a été démontré que pour être détenteur d'une carte mensuelle de transport, une personne devait compléter un formulaire dans lequel se trouvaient deux catégories de renseignements, ceux « obligatoires » et ceux « facultatifs ».

⁶ Septembre 2004, volume 9, numéro 9.

Parmi les renseignements obligatoires se trouvaient le nom, la ville dans laquelle l'utilisateur réside, son sexe, le type d'utilisateur et les photographies numérisées le concernant. La catégorie de renseignements facultatifs visait l'adresse de résidence de la personne, sa date de naissance, l'institution, la langue d'usage, les numéros de téléphone, et l'adresse courriel. Les renseignements sont conservés dans une banque de données bien identifiée.

Cependant, l'information concernant les transactions effectuées avec les cartes à puce était logée dans une autre banque de données.

Il a de plus été démontré que les usagers complétaient le formulaire d'identification sans aucune difficulté en regard de la cueillette des renseignements personnels, puisqu'ils semblaient être en accord avec l'aspect visant un meilleur service à la clientèle. La Loi sur l'accès prévoit que:

64. Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a la gestion.

Un organisme public peut toutefois recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en oeuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.

La collecte visée au deuxième alinéa s'effectue dans le cadre d'une entente écrite transmise à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission.

Selon la Société de transport de l'Outaouais, les renseignements facultatifs étaient demandés afin d'être en mesure d'identifier la bonne personne (par son adresse et son numéro de téléphone) pour savoir à qui on a affaire (est-ce un étudiant ou une personne aînée : date de naissance, etc.) et être capable de réagir en cas de vol ou de perte de la carte à puce.

Il est évident qu'une personne détentrice d'une carte à puce ne pourrait pas utiliser le transport en commun de façon anonyme. Cette carte est personnalisée et les renseignements personnels sont stockés dans une ou deux banques de données. L'on peut se demander notamment si, en complétant ce formulaire d'identification et en fournissant tous les renseignements personnels recherchés :

- L'utilisateur a donné un consentement libre et éclairé. Les finalités visées, portent-elles atteinte à la vie privée du citoyen qui souhaite détenir une telle carte et qui souhaite utiliser ce moyen de transport de façon anonyme?
- Tous les renseignements personnels collectés sont-ils nécessaires à l'obtention de cette carte à puce à la lumière de la Loi sur l'accès?
- Existe-t-il d'autres moyens dont cette société pourrait se prévaloir pour délivrer une carte à puce aux usagers du transport en commun?

Peu importe les motifs invoqués pour l'installation ou la création d'une carte à puce au sein d'un organisme quelconque, les renseignements personnels qui suivent permettent d'identifier un usager à partir du moment où on est capable de :

- Procéder au jumelage et de faire la comparaison avec les renseignements personnels d'un individu contenus dans des banques de données,
- Connaître les informations sur ses déplacements au sein du transport en commun, c'est-à-dire le parcours emprunté, le numéro d'autobus,
- Connaître, entre autres, la date, l'heure, le numéro de la carte à puce,
- Reconnaître une personne en examinant sa photographie.

Il est opportun de souligner que la *Loi concernant le cadre juridique des technologies de l'information*⁷ prévoit :

43. Nul ne peut exiger que l'identité d'une personne soit établie au moyen d'un procédé ou d'un dispositif qui porte atteinte à son intégrité physique.

À moins que la loi le prévoie expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve.

Il a été démontré que la carte à puce est plus avantageuse et plus économique à l'utilisateur qui utilise régulièrement le transport en commun de la Société de transport de l'Outaouais.

Il est évident qu'un usager qui ne souhaite pas être détenteur d'une carte à puce a le choix de payer comptant son droit de passage. L'intervention de la Commission dans ce dossier a nécessité que des modifications soient apportées, de sorte que

⁷ L.R.Q., c. C-1.1.

seuls les renseignements personnels nécessaires sont demeurés dans le formulaire d'identification et qu'une carte à puce anonyme a été créée.

Un article paru dans le journal *La Presse* le 20 avril 2008 a indiqué que la Société de transport de Montréal a débuté l'installation d'un système de cartes à puce à l'intention des usagers du transport en commun, c'est à suivre.

Par ailleurs, on peut penser que par un tel moyen technologique, une personne pourrait se servir des renseignements personnels se trouvant dans une banque de données afin d'établir, par exemple, le profil de l'utilisateur. Ces renseignements pouvant être accessibles à des tiers, ils peuvent servir, entre autres, à des fins de commercialisation, et ce, sans le consentement de cet utilisateur et même sans qu'il le sache.

Une multiplication de renseignements personnels sont détenus au sein des organismes et entreprises sans le consentement des personnes concernées. Lorsque ces renseignements ne sont pas détenus conformément à la Loi, la Commission a la responsabilité d'arrêter ou de freiner la circulation de ces renseignements, lorsqu'ils ne sont pas nécessaires.

Il est opportun de souligner que ces règles relatives à la protection des renseignements personnels doivent pouvoir s'adapter aux technologies de l'information. Cependant, ces technologies ne doivent pas mener à un affaiblissement de ces règles. Ainsi, dans son rapport final daté du mois de mai 2004, les membres de la Commission de la culture, (chargés de recueillir notamment les doléances de la Commission) à la suite de la consultation générale et des audiences publiques à l'égard du document intitulé « Une réforme de l'accès à l'information : le choix de la transparence⁸ ont notamment émis les commentaires suivants relatifs à la prestation du service aux citoyens :

« La Commission [de la culture] tient à rappeler que l'utilisation des technologies ne doit pas se faire au détriment des principes de protection des renseignements personnels et de la vie privée, ni mener à leur affaiblissement. Ainsi, quoiqu'elle constate que le développement de l'État en réseau puisse offrir des opportunités d'innovation et permettre une prestation de services plus efficace et efficiente, la Commission de la culture préconise une grande prudence en ce domaine. »

⁸ Rapport final, mai 2004, p. 17.

LA SECTION SURVEILLANCE

Parmi les nouvelles dispositions apportées à la Loi sur l'accès au mois de juin 2006, le législateur a cru opportun de créer la section de surveillance où j'exerce présentement mes nouvelles fonctions, en collaboration avec M^e Jacques Saint-Laurent qui, pour sa part, assume d'autres fonctions.

Essentiellement, la section de surveillance de la Commission traite des enquêtes et des ententes entre les organismes. Elle émet des avis relativement aux projets de règlement qui lui sont soumis en vertu de la Loi sur l'accès ainsi que les projets de décrets autorisant l'établissement des renseignements personnels de même que les demandes d'autorisation de recherche. Attardons-nous sur cette dernière partie.

LES AUTORISATIONS DE RECHERCHE

La Loi sur l'accès détermine les critères selon lesquels la Commission peut accorder à une personne ou à un organisme l'autorisation de recevoir à des fins d'étude, de recherche ou de statistique :

125. La Commission peut, sur demande écrite, accorder à une personne ou à un organisme l'autorisation de recevoir à des fins d'étude, de recherche ou de statistique, communication de renseignements personnels contenus dans un fichier de renseignements personnels, sans le consentement des personnes concernées, si elle est d'avis que:

1^o l'usage projeté n'est pas frivole et que les fins recherchées ne peuvent être atteintes que si les renseignements sont communiqués sous une forme nominative;

2^o les renseignements personnels seront utilisés d'une manière qui en assure le caractère confidentiel.

Cette autorisation est accordée pour la période et aux conditions que fixe la Commission. Elle peut être révoquée avant l'expiration de la période pour laquelle elle a été accordée, si la Commission a des raisons de croire que la personne ou l'organisme autorisés ne respecte pas le caractère confidentiel des renseignements qui lui ont été communiqués, ou ne respecte pas les autres conditions.

Par exemple, un chercheur s'adresse à la Commission afin de recevoir communication des renseignements personnels sans le consentement des personnes concernées. Cette autorisation ne sera accordée que si les exigences visant la confidentialité et la « dénominalisation » de ces renseignements sont respectées.

Toutes les conditions émises dans le cadre de cette autorisation doivent être respectées par le chercheur. Il doit notamment préciser l'objet de sa recherche, l'usage projeté, le moyen de transmission des renseignements en question, toutes les mesures qu'il compte prendre pour assurer la confidentialité et la sécurité des renseignements qu'il recevra de l'organisme détenteur, s'engager à ce que toute personne travaillant dans son dossier signe un engagement à la confidentialité. Ce chercheur devra en outre préciser que les renseignements ne seront pas communiqués à d'autres personnes que celles autorisées à les recevoir, les fins pour lesquelles ils sont communiqués, la durée de l'autorisation, la période de conservation et le moyen qu'il compte utiliser pour procéder à leur destruction.

Il doit aussi préciser et fournir à la Commission toute l'information nécessaire à l'étude de son dossier et démontrer notamment l'impossibilité d'obtenir le consentement de ces personnes ou faire état des démarches qu'il a effectuées et qui ne lui ont pas permis d'obtenir le consentement de ces personnes.

Dans la mesure où la Commission considère qu'il existe une possibilité pour le chercheur d'obtenir le consentement des personnes concernées, il sera invité à entreprendre des démarches à cette fin.

Par ailleurs, une demande positive de la Commission est conditionnelle à ce que l'organisme détenteur des renseignements personnels identifiés consente à leur communication. Il n'existe pas d'obligation légale pour la Commission de contraindre ce détenteur à les communiquer à un chercheur.

Aussi, lorsque les fins pour lesquelles l'autorisation a été accordée sont atteintes, le chercheur doit procéder à la destruction des renseignements en sa possession à la date fixée dans cette autorisation ou requérir une autorisation afin de les conserver pour une plus longue période, puisque les fins projetées ne sont toujours pas atteintes. La Commission peut par ailleurs en tout temps procéder à une inspection auprès du chercheur ayant reçu cette autorisation de recherche, d'étude ou de statistique afin de voir si toutes les conditions sont toujours respectées.

Par exemple, un professeur d'université (chercheur) ou une personne exerçant ses fonctions en matière de santé ou autre ayant reçu une réponse positive d'autorisation à des fins d'études, de recherche ou de statistique pour un sujet spécifique, doit respecter toutes les conditions déterminées par la Commission.

Lorsque cette recherche est terminée et qu'il souhaite utiliser les mêmes renseignements dans un domaine similaire ou autre, il doit soumettre une nouvelle demande d'autorisation à la Commission, conformément à la Loi sur l'accès.

Ces renseignements ne doivent pas être utilisés non plus par des tiers oeuvrant dans le même domaine ou dans un autre domaine, à moins que ceux-ci soumettent une demande et suivent le processus établi à cette fin pour obtenir l'autorisation de la Commission, le cas échéant.

Sans cette nouvelle autorisation, un chercheur doit s'abstenir d'utiliser ces renseignements à d'autres fins et les détruire. Il faut éviter la conservation de banques de données personnelles non nécessaires. En l'absence d'une telle demande et d'une réponse positive, la Commission pourra intervenir en vertu des pouvoirs qui lui sont conférés par la Loi sur l'accès.

Par ailleurs, la Commission est préoccupée par la circulation non autorisée des renseignements personnels concernant des citoyens sans leur consentement. Elle est récemment intervenue auprès d'organismes et d'entreprises privées, tels Home Sense, le Club Monaco et la Banque Canadienne Impériale de Commerce relativement à un bris de confidentialité dû notamment à la disparition de CEDEROM contenant des milliers de renseignements personnels et à un vol d'ordinateur portatif.

J'aimerais citer un extrait d'un rapport (le Rapport Paré rédigé en 1981) ayant servi de référence à la rédaction de la loi, il y a plus de 25 ans. Cet extrait concerne les normes sévères et les précautions devant être prises lorsqu'il s'agit de transfert de données personnelles entre organismes (p. 18):

« Il convient d'établir des normes sévères quant aux transferts de données personnelles entre les organismes. La principale inquiétude a trait à la possibilité de regrouper, par ces transferts, l'ensemble des données recueillies sur une personne. L'informatique permet facilement le repérage et la réunion des données. D'une façon générale, la loi devra interdire les transferts de données personnelles entre fichiers. Toutes les exceptions devront être inscrites dans des lois, faisant ainsi l'objet d'un débat à l'Assemblée nationale. Ce débat permettra aux citoyens de connaître les pratiques actuelles en matière de transferts et aux parlementaires de juger de leur pertinence et leur nécessité. »

Ces commentaires sont d'autant plus importants, particulièrement lorsque l'on considère qu'aujourd'hui, par le biais de la technologie, il existe une facilité de colliger, d'utiliser et de conserver un nombre illimité d'information, sans oublier par

exemple, la possibilité de regrouper plusieurs fichiers de renseignements personnels pour n'en créer qu'un seul, et ce, à l'insu des personnes concernées. Quelle que soit sa forme, l'utilisation sans droit et sans autorisation d'une nouvelle technologie par un ou des individus représente une intrusion dans la vie privée d'un individu et les risques rattachés à un bris de confidentialité peuvent avoir des conséquences sérieuses à l'égard de cet individu.

L'intervention de la Commission à partir des exemples que je vous ai soumis a permis d'examiner notamment les mesures de sécurité additionnelles prises par ces organismes, de manière à éviter que de telles situations ne se reproduisent. Ces mesures de sécurité visent également les contractants et les sous-contractants qui font affaire avec eux, le cas échéant.

Le cadre législatif québécois auquel j'ai fait référence au cours de ma présentation, donne des outils à la Commission afin de s'acquitter du large mandat qui lui est confié à la Loi sur l'accès. Chaque étape visant la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels nécessite des précautions à prendre, en assurant le respect des droits des citoyens et en se basant notamment sur les principes de base établis par la Charte des droits, le Code civil, la Loi sur l'accès et la Loi sur le privé.

Peu importe le lieu, la province ou le pays où l'on se trouve, le principe de base demeure le même; les renseignements personnels concernant une personne ne doivent pas être mis en circulation à l'insu de cette personne mais plutôt avec son consentement ou avec l'autorisation de la Commission.

Je voudrais par ailleurs attirer votre attention sur l'entrée en vigueur d'une nouvelle disposition législative à la Loi sur l'accès qui démontre la rigueur qu'un organisme doit avoir en regard des renseignements personnels qu'il détient et qui peuvent faire l'objet d'une collecte, d'utilisation ou de communication. Il est indiqué :

70.1. Avant de communiquer à l'extérieur du Québec des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi.

Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalente à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la

tâche de détenir, de les utiliser ou de les communiquer pour son compte.

Cette disposition législative vient renforcer davantage le maintien du droit à la vie privée et le caractère confidentiel des renseignements personnels concernant un citoyen qui seront transigés à l'extérieur du Québec

Par ailleurs, dans un autre ordre d'idée, j'aimerais vous faire part de la première Conférence des commissaires à la protection des données personnelles de la Francophonie présidée par M^e Jacques Saint-Laurent s'est tenue à Montréal, le 27 septembre 2007. Elle s'est terminée par la création de l'Association francophone des autorités de protection des données confidentielles, dont M^e Saint-Laurent assure la présidence. Elle a été créée par une volonté commune de représentants des pays francophones de promouvoir et de défendre à travers la francophonie le droit des personnes à la protection des renseignements personnels.

J'attire votre attention sur quelques objectifs de cette association. Elle a notamment pour but :

[...]

5.2 d'encourager l'étude et la recherche sur des questions et pratiques relatives à la protection des données personnelles et partager les résultats de cette recherche entre les autorités;

5.3 de constituer un pôle d'expertise et d'échange d'expérience servant d'appui à l'adoption de textes législatifs nationaux ou d'instruments internationaux en matière de protection des données personnelles;

5.5 de fournir un forum de réflexion et d'échange aux autorités concernant les nouveaux enjeux et défis dans le domaine de la protection des données personnelles et de la vie privée;

5.6 de travailler avec d'autres organismes et associations francophones dans le cadre de la consolidation de la protection des données personnelles en tant que facteur de la promotion de l'État de droit et du développement démocratique.

J'ai voulu par ma présentation élargir la réflexion sur les nouvelles technologies de l'information.

Je vous remercie de votre attention.