

31^e Conférence internationale des commissaires à la protection des données et de la vie privée

Séances parallèles

Séance B

Les Autorités sous-nationales, sous-étatiques ou fédérées de protection de données et d'administrations publiques : expériences et stratégies proactives en éducation et en santé

La Commission d'accès à l'information du Québec. Canada

Chers amis,

Je tiens d'abord à remercier les organisateurs de la 31^e Conférence internationale des commissaires à la protection des données et de la vie privée de l'invitation qui nous a été faite de discuter d'expérience et de stratégies proactives en éducation et en santé, à titre d'autorité sous-nationale, sous-étatique ou fédérée de protection des données.

Je m'en voudrais de ne pas féliciter les organisateurs de la Conférence internationale, plus spécialement le directeur de l'agence espagnole de la protection des données et son équipe, pour la qualité de l'organisation de l'événement et la pertinence des sujets traités.

1. Introduction générale

La Commission d'accès à l'information que je préside est en fait l'autorité de protection des données personnelles au Québec. Il s'agit d'une autorité fédérée faisant partie du Canada. Comme vous le savez, le Québec est situé à l'est du Canada, du côté de l'océan Atlantique. La province est traversée d'est en ouest par le fleuve Saint-Laurent. Le vaste territoire québécois fait partie de l'Amérique du Nord. Il s'agit du seul état francophone de ce continent. À l'opposé des autres provinces et territoire canadiens, le droit interne respecte les principes du droit civil plutôt que ceux de la Common Law

1.1 Régime de protection de données au Québec

La Loi constitutionnelle canadienne détermine les pouvoirs qui sont confiés à l'État fédéral, d'une part, et aux États fédérés, d'autre part.

Chaque province dispose, à l'égard des responsabilités qui lui ont été confiées par la Loi constitutionnelle, de tous les pouvoirs d'un État. Il s'agit

d'exercer pleinement les pouvoirs législatifs, exécutifs et judiciaires pour les domaines de compétence délégués.

Ainsi, à l'égard de la protection des données personnelles, l'Assemblée nationale du Québec a, en 1982, adopté une loi concernant le secteur public. Il s'agit de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

À ce moment là, l'Assemblée nationale du Québec a décidé de légiférer non seulement à l'égard de la protection des données personnelles mais également concernant l'accès aux documents administratifs. En effet, faisant œuvre de pionnier en la matière, le législateur québécois a regroupé dans une même législation, et sous l'autorité d'un seul organisme de contrôle, les principes de transparence de l'État et de protection des données personnelles dans le secteur public. C'est d'ailleurs pour cette raison que l'autorité de protection des données personnelles au Québec porte le nom de Commission d'accès à l'information qui se rapporte au seul volet de sa mission relatif à l'accès à l'information.

En 1994, l'Assemblée nationale du Québec a élaboré les principes de protection des données personnelles dans le secteur privé. Les règles de base se retrouvent au Code civil du Québec alors que la Loi sur la protection des renseignements personnels dans le secteur privé précise le cadre juridique concernant la protection des données dans le secteur privé.

1.2 Les régimes de santé et d'éducation au Québec

La protection des données personnelles dans le secteur de l'éducation doit respecter les exigences prescrites par les lois dont nous avons discutées précédemment, autant pour le secteur public que pour le secteur privé. Il faut se référer aux interprétations données par la Commission d'accès à l'information, dans l'exercice de ses pouvoirs juridictionnels et de surveillance, pour comprendre à quel point l'autorité de contrôle exige que les données personnelles des étudiants soient rigoureusement protégées.

Dans le secteur de la santé, l'Assemblée nationale du Québec, en plus des dispositions législatives précitées dans les secteurs public et privé, a élaboré des dispositions particulières pour limiter encore davantage l'accès au dossier de santé de l'utilisateur ou la communication de ces renseignements sensibles à des tiers, même avec le consentement de l'utilisateur.

En fait, comme dans plusieurs États, les renseignements relatifs à l'état de santé d'une personne sont considérés, au Québec, comme des renseignements très confidentiels à l'égard desquels des mesures rigoureuses de protection s'imposent. D'ailleurs, l'obligation de prendre des mesures adéquates a été confirmée à plusieurs reprises par des décisions de la Commission d'accès à l'information du Québec.

2. La protection des données personnelles dans les secteurs de la santé et de l'éducation

La variété de situations concernant la protection des données personnelles dans les secteurs de la santé et de l'éducation exigerait une discussion beaucoup trop longue par rapport au temps dont nous disposons dans le cadre de la conférence actuelle. Nous nous limiterons à faire état de certains risques auxquels sont exposées ces données. Ces risques font l'objet d'une attention soutenue par la Commission d'accès à l'information.

En principe, la personne concernée par des renseignements personnels peut consentir à la collecte, à la conservation ou à la communication des renseignements qui la concernent. Dans le secteur de la santé ou de l'éducation, il faut apporter des réserves à ce principe tenant compte des difficultés, pour certaines personnes, de comprendre l'enjeu ou de donner un consentement valable. Dans le secteur de l'éducation, la possibilité pour un étudiant de consentir à la collecte des renseignements personnels qui le concernent évolue en fonction, notamment, de l'âge. La facilité de convaincre les jeunes en fait des proies faciles, avec des conséquences particulièrement sérieuses lorsqu'il s'agit de vol d'identité et de fraude. Tenant compte de ces risques, l'autorité de contrôle doit alors imposer des mesures qui tiennent compte de la nécessité de protéger adéquatement les personnes concernées.

Dans le secteur de la santé, la capacité de donner un consentement valide pour la collecte, la conservation ou la communication n'est pas absolue, même lorsque nous sommes en présence d'adultes. L'autorité de protection des données personnelles doit rappeler régulièrement cette difficulté. Par exemple, on ne peut affirmer qu'une personne peut donner un consentement libre et éclairé à un assureur ou à un employeur qui exige la communication de renseignements personnels. La crainte de perdre un emploi ou le bénéfice de l'assurance peut forcer l'individu à consentir. En effet, les conséquences du refus de communiquer les renseignements demandés peuvent être telles que la personne concernée n'a pas le choix. L'autorité de protection des données personnelles doit exercer un contrôle très attentif pour éviter que les assureurs ou les employeurs, par exemple, abusent de cette position dominante à l'égard de leurs assurés ou de leurs employés.

La Commission d'accès à l'information est également soucieuse du risque que les renseignements relatifs à l'état de santé d'une personne soient communiqués à des tiers alors que cette communication n'est pas autorisée par la loi et que la personne concernée n'y a pas consenti. Pour un renseignement relatif à l'état de santé d'une personne ou un dossier scolaire, la Commission d'accès à l'information répète constamment aux organismes publics et aux entreprises que les risques et les conséquences d'une communication non-autorisée exigent une rigueur absolue. En matière de communication de données sensibles, on ne peut présumer de la volonté des personnes concernées.

2.1 Dans le secteur public

Tenant compte de ce qui a déjà été exprimé au niveau de la protection des données personnelles dans les secteurs de la santé et de l'éducation, il suffit, à ce stade, de rappeler que, pour le Québec, l'Assemblée nationale a élaboré des législations distinctes pour le secteur public puis le secteur privé. Ces législations sont conformes aux standards internationaux généralement reconnus en matière de protection des données personnelles.

Le principe fondamental de la confidentialité des renseignements doit être respecté. Non seulement les renseignements personnels doivent demeurer confidentiels mais également il est interdit de recueillir un renseignement personnel s'il n'est pas nécessaire à l'exercice des attributions de l'organisme public concerné ou nécessaire à l'objet du dossier constitué par l'entreprise privée.

Les principes à considérer comprennent également le droit inaliénable d'accès par la personne concernée aux renseignements personnels qui sont conservés à son sujet. Ce droit d'accès s'accompagne de la possibilité de demander la rectification d'un renseignement personnel inexact, incomplet ou équivoque et la suppression d'un renseignement qui est faux ou dont la conservation n'est pas autorisée.

2.2 Dans le secteur privé

Pour le secteur privé les commentaires sont les mêmes. Il y a lieu de rappeler que ces principes fondamentaux se retrouvent au Code civil du Québec d'une part et à la Loi sur la protection des renseignements personnels dans le secteur privé d'autre part.

3. Le rôle de l'autorité indépendante au Québec

Au moment d'élaborer la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, en 1982, l'Assemblée nationale du Québec a non seulement choisi de regrouper les activités d'accès aux documents des organismes publics et de protection des renseignements personnels dans une seule loi, mais également de déléguer à l'autorité de contrôle plusieurs pouvoirs. On comprendra que ces différents pouvoirs se complètent et ont pour objectif de faire en sorte que l'autorité de protection des données personnelles soit en mesure d'agir de façon coercitive et indépendante.

Au premier niveau, la responsabilité d'assurer la protection des données personnelles concernant la collecte, la conservation, l'utilisation ou la communication appartient à l'entreprise ou à l'organisme public, selon le cas. Les organismes et les entreprises ont la responsabilité de prendre les mesures

appropriées dans les circonstances. Pour les organismes publics, la personne responsable de l'accès aux documents et de la protection des renseignements personnels doit répondre aux demandes d'accès ou de rectification qui lui sont adressées. L'entreprise doit en faire autant lorsque les circonstances le requièrent.

Cette mise en contexte introduit le pouvoir juridictionnel délégué à la Commission d'accès à l'information par l'Assemblée nationale. Ainsi, l'autorité de protection des données personnelles doit réviser, comme un tribunal, les décisions prises par les responsables de l'accès des organismes publics et par les entreprises concernant les demandes d'accès et de rectification relatives à des données personnelles.

En outre, pour le Québec, la Commission d'accès à l'information dispose de pouvoirs de surveillance de l'application de la loi pour les organismes publics et les entreprises. Cette surveillance s'exerce notamment par des activités d'inspection ou d'enquête à la suite de plaintes que reçoit la Commission ou de sa propre initiative lorsqu'elle le juge opportun.

La fonction de surveillance de la Commission d'accès à l'information comprend également la responsabilité de donner des avis au gouvernement ou aux membres de l'Assemblée nationale au sujet de projets de lois, de projets de règlements ou d'ententes impliquant la collecte, la communication, l'utilisation ou la conservation de renseignements personnels. En outre, depuis juin 2006, le législateur québécois a demandé à la Commission d'accès à l'information de promouvoir l'accès aux documents administratifs et la protection des données personnelles.

3.1 Soutenir la protection des données et la transparence

En faisant référence à nos expériences respectives, on peut assez facilement imaginer plusieurs situations où les fonctions juridictionnelles et de surveillance décrites précédemment ont permis à la Commission d'accès à l'information de contraindre les organismes publics et les entreprises de respecter les principes de protection des données personnelles.

Outre l'exercice de pouvoirs coercitifs la Commission d'accès à l'information du Québec accorde une importance primordiale à l'accompagnement des organismes publics et des entreprises qui œuvrent dans le secteur de l'éducation et de la santé. L'autorité de protection des données se fait un devoir d'être présente dans les établissements d'éducation et de santé pour faire connaître les principes de protection des données personnelles et contribuer à l'identification des mesures à prendre pour mettre en œuvre la protection de ce droit fondamental des personnes concernées.

Cette présence dans le milieu a aussi pour objectif d'illustrer, de façon concrète, la sensibilité des renseignements personnels concernés et l'importance que la protection de ces données représente pour chaque établissement.

3.2 Contribuer à la bonne gouvernance

Malgré les progrès réalisés depuis plus de vingt ans, il n'est pas rare de constater, dans les secteurs public et privé, que les autorités en place ne prennent pas les mesures de protection adéquates, parce qu'elles croient, devant la complexité du sujet, qu'il est impossible de déployer des mesures de protection effectives des données personnelles dans leur organisation.

Par des mesures d'information, de formation et de promotion la Commission d'accès à l'information vise à changer cette perception que la protection des données est tellement complexe qu'il est préférable de ne rien faire. En fait, dans un contexte de bonne gouvernance, nous proposons aux établissements de se donner un cadre de protection des données personnelles conforme à la loi, simple et qui répond à la logique de l'entreprise.

Notre objectif demeure de responsabiliser les organismes publics et les entreprises en suscitant une prise de conscience par l'information et la formation et en évitant la coercition.

4. Les modes d'intervention de l'autorité indépendante au Québec

4.1 La responsabilité des organismes publics et des entreprises privées

Nous avons exposé précédemment le principe applicable au Québec concernant la responsabilité première des organismes publics et des entreprises à l'égard de la protection des données personnelles. Il suffit de rappeler que ces organisations doivent, au premier chef, prendre des mesures de protection et décider à la suite des demandes qui leur sont présentées.

Par la suite, ces mesures de protection sont assujetties aux pouvoirs de surveillance et de contrôle de la Commission d'accès à l'information. De leur côté, les décisions des organismes publics et des entreprises sont susceptibles d'être révisées dans le cadre de l'exercice de la fonction juridictionnelle de la Commission.

4.2 Le volet de surveillance

4.2.1 En santé : Le dossier de santé du Québec (DSQ)

Après avoir exposé sommairement les activités de surveillance de l'autorité de protection des données personnelles au Québec, l'exemple du DSQ peut illustrer nos propos. Le DSQ est un projet informatique qui vise les renseignements de santé de la population québécoise. Le DSQ permettra de rendre accessible, de façon électronique, aux professionnels de la santé, certains renseignements cliniques pertinents pour le suivi des patients, quelque

soit le lieu où ces patients reçoivent des services au Québec. Toutefois, un usager pourra refuser qu'un dossier de santé électronique soit constitué à son sujet.

Dans l'élaboration du cadre législatif et des processus administratifs nécessaires, le ministre de la Santé et des Services sociaux du Québec a fait appel à la Commission d'accès à l'information du Québec pour exercer un suivi du projet expérimental dans la région de la Capitale Nationale.

L'autorité de protection des données personnelles a alors le privilège d'exercer un rôle extrêmement constructif, à la fois pour la protection des données personnelles ainsi que pour l'évolution technologique incontournable dans le secteur de la santé. En se basant sur notre expérience des dernières années, en effectuant l'analyse de projets semblables dans d'autres provinces ou dans d'autres pays, nous essayons d'apporter une contribution étroite et rigoureuse dans le développement du DSQ.

4.2.2 En éducation : Élève handicapé ou en difficulté d'adaptation et d'apprentissage (EHDA)

Après analyse, la Commission d'accès à l'information du Québec a reconnu la nécessité pour le ministre de l'Éducation de recueillir et d'utiliser des renseignements personnels concernant des élèves handicapés ou en difficulté d'adaptation et d'apprentissage, aux fins d'évaluation et de financement des programmes offerts à ces élèves, par les établissements d'enseignement publics ou privés.

Considérant la très grande sensibilité de ces renseignements, l'autorité de contrôle a pris la décision de prescrire des conditions particulières, notamment, pour limiter l'accès aux renseignements personnels aux seules personnes préalablement autorisées par la Commission, lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

Dans cet exemple, la Commission d'accès à l'information a exercé sa fonction de surveillance en imposant des normes à l'organisme public concerné vu la sensibilité des renseignements en cause.

Il y a lieu de mentionner que dans le cadre d'une activité ponctuelle de surveillance, dans le secteur de l'éducation, la Commission d'accès à l'information est intervenue, à la suite d'une plainte, pour s'assurer que les caméras de surveillance qui avaient été installées dans une école soient retirées.

4.3 Le volet juridictionnel

4.3.1 La médiation

4.3.2 Décisions du Tribunal administratif

Il est rare de retrouver, parmi les pouvoirs attribués à une autorité indépendante de protection des données, une fonction juridictionnelle. Par exemple, au Canada, la Commission d'accès à l'information du Québec est la seule autorité qui, en plus de rendre des décisions dans l'exercice de son pouvoir de surveillance, exerce une fonction juridictionnelle à l'égard de décisions rendues par des organismes ou des entreprises.

Je dois mentionner que cette fonction juridictionnelle permet aux citoyens d'exercer certains recours concernant la protection de leurs renseignements personnels. Ces recours n'existent pas dans tous les États.

En résumé, les recours que peuvent exercer les individus concernent plus spécialement l'accès aux renseignements personnels qui sont détenus par des organismes publics ou des entreprises à leur sujet. Ces personnes peuvent également demander que les renseignements personnels qui sont conservés soient rectifiés ou supprimés en certaines circonstances. Au Québec, plusieurs recours sont exercés par les individus et ont l'avantage de forcer les organismes publics et plus spécialement les entreprises, d'une part, à prendre conscience de l'importance de la protection des données personnelles dans leur organisation et, d'autre part, à prendre les mesures effectives pour respecter la loi.

Par ailleurs, les décisions de la Commission peuvent faire l'objet d'un appel à la Cour du Québec concernant toutes questions de droit ou de compétence. Par contre, l'appréciation des faits relève de sa compétence exclusive.

En terminant, j'aimerais faire un lien entre la protection des données personnelles dans le secteur de l'éducation et les discussions que nous avons eues au cours des derniers jours concernant la protection des données personnelles dans Internet.

Conclusion

Inévitablement, lorsque nous référons au secteur de l'éducation, nous nous adressons à un public jeune, à des enfants et des adolescents. Comme nous le mentionnions précédemment, on ne peut pas présumer que les jeunes soient en mesure de donner un consentement à la collecte ou à la communication de leurs renseignements personnels quelques soient les circonstances. Il faut tenir compte de leur âge, de leur capacité de comprendre l'enjeu, ce à quoi ils acceptent de souscrire.

À cette difficulté de compréhension inhérente à la condition des jeunes s'ajoute la confusion dans laquelle nous plonge la technologie, par exemple en enregistrant automatiquement nos identifiants et nos mots de passe. Tout devient automatique et nous porte à croire que l'on peut confier à l'ordinateur la responsabilité de gérer notre sécurité virtuelle, y compris nos renseignements d'identité.

Alors qu'il serait important d'inculquer aux jeunes un souci de protéger adéquatement leur identité et les renseignements personnels qui les concernent, comme ils apprennent à se soucier des questions environnementales, ils sont plutôt plongés dans un automatisme invisible qui leur laisse croire qu'il n'est pas nécessaire d'être vigilant.

Même si sur le plan technologique il est possible d'automatiser plusieurs processus, je pense qu'il n'est pas prudent, pour des questions de sécurité, de laisser une personne décider seule du niveau d'intervention qu'elle souhaite exercer à l'égard de la sécurité de ses renseignements personnels, plus spécialement de ses renseignements d'identité. Si nous prenons l'exemple des autres secteurs d'activités de la société, par exemple la sécurité aérienne ou la sécurité automobile, nous ferons rapidement le constat que malgré les compétences supérieures que nous reconnaissons, par exemple au pilote d'avion, plusieurs mesures sont prises pour les assister dans la gestion de la sécurité. Personne ne remet en question la pertinence de ces règles exigeantes qui sont imposées aux pilotes ou aux conducteurs à l'égard de la sécurité des appareils qu'ils contrôlent.

Dans Internet, il me semble y avoir des lacunes à ce sujet.

Il faut féliciter les entreprises technologiques pour les nombreuses caractéristiques de sécurité qui ont été développées au cours des années pour assurer la robustesse des technologies disponibles. Des efforts considérables ont été déployés pour contrecarrer les attaques des fraudeurs et des mauvais plaisantins.

Par contre, il faudrait également s'attaquer aux risques que représentent les erreurs que peuvent commettre les utilisateurs au moment de naviguer dans Internet, notamment. Dans l'ensemble des processus sécuritaires qui sont développés actuellement, il faut reconnaître que l'utilisateur constitue le maillon faible. Dans ce contexte, laisser les questions de sécurité au seul bon jugement de l'utilisateur ou à son consentement ne se justifie pas bien. Malgré les précautions d'usage, la possibilité d'une erreur humaine paraît évidente.

De la même façon, laisser les questions de sécurité au seul bon jugement de l'utilisateur, lorsqu'il s'agit d'un enfant ou d'un adolescent, ne se justifie pas du tout. La vulnérabilité s'ajoute au risque d'erreur humaine.

C'est pourquoi, dans le secteur de l'éducation, nous avons l'objectif de sensibiliser les développeurs informatiques et les fabricants de matériel et de

promouvoir la nécessité d'ajouter des mesures de protection en fonction des risques d'erreur et de la vulnérabilité des jeunes.

Conscients de l'importance du travail à faire, nous avons comme deuxième objectif de demander l'aide des professionnels informatiques dans l'identification des mesures de sécurité requises et d'offrir notre collaboration aux experts pour renforcer le maillon le plus faible du processus de sécurité technologique.

Des mesures d'assistance à l'utilisateur s'imposent, principalement à l'égard des enfants.

Rappelons-le, il n'est pas raisonnable de laisser les questions de sécurité au seul bon jugement de l'être humain, que ce soit aux commandes d'un ordinateur ou d'un aéronef.

Je vous remercie de votre attention.

Jacques Saint-Laurent
Président
Commission d'accès à l'information du Québec