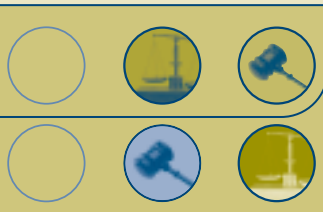
VOL. 2-NO 5
SEPTEMBRE / OCTOBRE 1996

l'informateur

PRIVÉ

Bulletin d'information concernant l'accès aux documents et la protection des renseignements personnels

À lire dans ce numéro :



ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION (AAPI)

PARTENAIRE FINANCIER

Relations avec les citoyens et Immigration Québec

SÉCURITÉ INFORMATIQUE ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

L'obligation de confidentialité et les autres obligations concernant la gestion des renseignements personnels, imposées par la Loi sur la protection des renseignements personnels dans le secteur privé et le Code civil du Québec, nécessitent la mise en place de certaines mesures particulières lorsque ces renseignements se trouvent sur support informatique. Dans ce premier d'une série d'articles sur le sujet, nous résumons les principales mesures proposées par la Commission d'accès à l'information aux organismes publics.

Rappel des principes de la Loi sur la protection des renseignements personnels dans le secteur privé

La gestion documentaire et la protection des renseignements personnels ne peuvent, de nos jours, être abordées sans référence au support informatique. Les concepteurs de logiciels, devant la demande des consommateurs, développent de plus en plus différents mécanismes propres à assurer la sécurité des données informatiques. On ne saurait, toutefois, s'en remettre uniquement aux concepteurs. C'est à l'entreprise qui détient les renseignements d'exiger et d'implanter les mesures de sécurité adéquates afin d'assurer la protection des renseignements personnels qui se trouvent sur support informatique. Quels sont ces mécanismes qui lui permettront de respecter les obligations imposées par la loi?

D'abord, un bref rappel... Les principales obligations auxquelles une entreprise doit veiller en regard des données personnelles qu'elle détient sur support informatique sont: (1) prendre et appliquer des mesures de sécurité propres à assurer leur caractère confidentiel (art. 10 et 13 de la loi et art. 37 C.C.Q.); (2) inscrire l'objet du dossier (art. 4 de la loi et 37 C.C.Q.) et la source du renseignement s'il a été obtenu auprès d'une autre entreprise (art. 7 de la loi) (3) ne permettre l'accès, à l'interne, qu'aux personnes ayant qualité pour en prendre connaissance et ne leur permettre l'accès que dans l'exercice de leurs fonctions (art. 20); (4) veiller à leur exactitude au moment où elles sont utilisées pour prendre une décision relative à la personne concernée (art. 11 de la loi) et (5) ne les utiliser qu'à des fins pertinentes à l'objet du dossier et uniquement tant que cet objet n'est pas accompli (art. 12 et 13 de la loi et art. 37 C.C.Q.) (6) ne recueillir que les renseignements nécessaires à l'objet du dossier (art. 5 de la loi).

Mesures de sécurité proposées dans le secteur public

La Commission d'accès publiait en 1992 un document intitulé «Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux», dans lequel elle énumère les mesures de sécurité informatiques minimales que doivent mettre en place les organismes publics du réseau de la santé et des services sociaux

Sommaire

quant aux dossiers des usagers. Ces normes devaient faire partie de tout nouveau système informatique et la Commission accordait un délai de 3 ans, soit jusqu'au 1er juillet 1995, pour modifier les systèmes déjà en place afin de les rendre conformes à ces exigences.

Ces mesures de sécurité informatique sont d'intérêt puisque la Commission a démontré son intention d'appliquer certains de ces dispositifs de sécurité à l'ensemble des organismes publics[1]. De plus, elles peuvent servir de base à l'élaboration de mesures de sécurité pour les entreprises privées.

Dans cette directive, la Commission propose d'abord la désignation d'une personne responsable de la sécurité informatique qui aura l'appui non équivoque de la haute direction de l'organisme. Elle suggère que le responsable de la protection des renseignements personnels peut très bien remplir ce rôle. Si le contexte s'y prête, la Commission recommande que cette personne soit appuyée, dans ses actions, par un comité sur la sécurité des données, qui aurait les responsabilités suivantes:

* développer un programme de sensibilisation et de formation du personnel en matière de sécurité et de protection des données;

* coordonner toutes les activités reliées à la protection des données et à la sécurité informatique;

* vérifier périodiquement que le programme de sécurité et de protection des données est respecté (peut être aidé par le vérificateur interne ou externe de l'entreprise);

* produire un bilan annuel (suivi et contrôle) de l'application du programme à la personne ayant la plus haute autorité au sein de l'entreprise.

Cette personne pourrait également voir à l'élaboration et à la diffusion d'une politique de protection des renseignements nominatifs sur support informatique.

Par ailleurs, les dispositifs de sécurité doivent au moins couvrir les aspects suivants, selon la Commission:

- l'identification des utilisateurs au regard de l'accès aux données, par exemple par un code d'identification, et leur authentification, notamment par l'entrée d'un mot de passe;

- définir, pour chaque utilisateur (employé, formation, programmeur, etc.) un profil d'accès qui déterminera les renseignements auxquels il a accès (médical, social, administration, dossier actif ou inactif) ainsi que le mode d'accès (écriture, lecture, destruction, etc.);

- veiller à ne recueillir que les données nécessaires et qu'elles soient inscrites par des personnes autorisées par l'organisme que celui_ci pourra identifier;

- faire périodiquement des copies de sécurité des données, programmes et logiciels, mais en limiter la circulation;

- limiter l'accès aux terminaux uniquement aux personnes autorisées et prendre les mesures nécessaires afin d'assurer le caractère confidentiel des renseignements qui se trouvent à l'écran;

- voir à la sécurité des lieux;

- prévoir la journalisation de tous les accès aux renseignements personnels informatisés et en faire la vérification;

- respecter le caractère confidentiel des renseignements lors de télécommunications et voir à ce que seules les communications autorisées soient faites;

- respecter la loi et des mesures strictes de sécurité lors de communications rendues nécessaires suite à l'octroi d'un mandat par l'organisme à une autre personne, organisme ou entreprise;

- prendre les précautions adéquates lors de l'utilisation de micro_ordinateurs;

- adopter une politique quant à l'impression des données personnelles, politique visant à assurer la sécurité de ces données.

La Commission a précisé, par la suite, certains aspects concernant l'accès à distance aux dossiers de santé[2]. Il s'agit principalement de l'accès au dossier de l'usager à partir de son domicile lors de soins donnés chez lui, ou encore à la clinique d'un médecin ou autre professionnel spécialisé.

En ce qui concerne l'accès au dossier médical, la Commission rappelle le principe général à l'effet que les établissements ne peuvent donner accès à distance (accès donnés à l'extérieur de l'établissement), à partir d'un poste de travail informatisé, qu'aux seuls médecins ou professionnels dont le nom apparaît, antérieurement à la demande d'accès, dans le dossier de l'usager. Dans tous les cas, ces médecins ou professionnels de la santé doivent faire partie du personnel de l'établissement qui détient le dossier de l'usager.

L'établissement doit donc prendre les mesures nécessaires afin d'éviter qu'un médecin (ou autre professionnel de la santé) puisse, en utilisant son micro_ordinateur à partir de sa clinique privée ou d'un CLSC, avoir accès, sans contrôle préalable, à tous les dossiers des usagers d'un centre hospitalier.

Ainsi, dans les cas où le nom du médecin qui demande l'accès à distance n'apparaît pas au dossier de l'usager, l'établissement doit d'abord obtenir le consentement écrit de l'usager. Dans les situations d'urgence, la Commission précise que ce consentement pourrait être transmis par télécopieur, à condition de respecter sa directive relative à l'usage des télécopieurs.

Dans le cas de l'accès à distance aux résultats des analyses de laboratoires, elles sont évidement toujours accessibles au médecin qui en a fait la commande. Ces résultats peuvent, selon la Commission être affichés sur un écran ou imprimés dans les CLSC ou les cliniques privées. Naturellement, ces résultats peuvent également, selon la méthode plus traditionnelle, être imprimés au centre hospitalier et transmis par courrier au médecin les ayant commandés.

Ces principes pourraient inspirer les entreprises quant à l'adoption d'une politique concernant l'accès à distance à des données personnelles.

Des précisions S.V.P.

Nous reprendrons donc, dans les prochains numéros de L'Informateur, ces principales mesures de sécurité afin de les expliciter davantage. Nous aborderons également les mesures à adopter lors de l'implantation d'un système informatique.

Protection des renseignements personnels sur l'autoroute de l'information

La Commission d'accès à l'information a fait connaître sa position quant à l'autoroute de l'information[3]. Rappelant que le droit à l'information et au respect de sa vie privée sont deux droits fondamentaux consacrés dans la Charte des droits et libertés de la personne, la Commission considère que les principes établis dans la Loi sur l'accès aux documents, la Loi sur la protection des renseignements personnels dans le secteur privé et le Code civil du Québec sont suffisamment généraux pour s'adapter aux progrès de la technologie et qu'ils devraient présider à l'implantation de l'autoroute de l'information ou de toutes autres formes de réseaux interactifs de communication.

De façon plus précise, la Commission retient les principes suivants au chapitre de l'accès à l'information gouvernementale par le citoyen:

* L'autoroute de l'information doit être utilisée comme moyen pour véhiculer l'information d'intérêt public. Il est essentiel pour les fournisseurs de services publics qui utilisent des réseaux électroniques, de garantir l'accès à l'ensemble de l'information et aux services considérés d'intérêt public.

* Dans l'intérêt des citoyens qui choisiront de ne pas utiliser les services électroniques, les moyens conventionnels d'accès à l'information et aux services doivent être maintenus.

* L'adhésion aux services offerts sur l'autoroute de l'information doit être libre et volontaire.

En ce qui concerne la protection des renseignements personnels sur l'autoroute de l'information, la Commission rappelle qu'il s'agit de renseignements confidentiels et que tout organisme public ou entreprise privée à l'œuvre dans ces réseaux doit veiller à protéger ces renseignements. Pour y arriver, il faut retenir les principes suivants:

* Les institutions publiques et les entreprises privées qui ont comme projet d'implanter l'autoroute de l'information doivent, au préalable, procéder à une évaluation des éventuels impacts de cette nouvelle technologie sur la protection des renseignements personnels des citoyens au sein de leur entreprise ou organisme.

* La cueillette, la détention, l'utilisation et la communication des renseignements personnels doivent être conformes aux prescriptions de la loi.

* Des mesures de sécurité doivent être mises en place pour assurer la protection des renseignements personnels.

Quant à cette dernière exigence, la Commission suggère que les responsables de réseaux mettent à la disposition des fournisseurs de services les moyens techniques leur permettant d'assurer cette protection. Ainsi, chacun devrait se doter d'un code de conduite précisant les devoirs et obligations à l'égard des renseignements personnels.

Par ailleurs, certaines mesures devraient être destinées aux employés, notamment l'exigence d'un code d'accès et d'un mot de passe pour accéder aux systèmes, l'accès limité en fonction des

nécessités administratives, la signature d'un protocole de confidentialité et la journalisation des consultations de renseignements personnels. Il est évidemment très important que les employés soient bien informés des mesures mises en place par leur employeur à ce titre.

Quant aux mesures de sécurité destinées aux usagers, la Commission propose les suivantes: une carte d'accès par client et un code d'accès spécifique (NIP), un code d'accès pouvant être modifié par le détenteur à des points de services, l'identification de l'usager lors de l'émission de la carte ou de son remplacement, l'accès au courrier électronique seulement par la personne concernée et le rejet de la carte après trois tentatives infructueuses.

Enfin, la Commission précise que les mesures de sécurité doivent être élaborées en fonction de la sensibilité des renseignements.

1. «La sécurité informatique, c'est l'affaire de tous les organismes publics!», dans L'accès, C.A.I. Vol.9 no. 3, p.3.
2. «Les accès à distance aux dossiers de santé», dans L'accès, C.A.I. Vol. 9 no. 4, juin 1994, p.4.
3. «L'accès à l'information et la confidentialité des renseignements personnels sur l'autoroute de l'information», dans Contact, septembre 1995.

l'informateur PUBLIC ET PRIVÉ

L'informateur PUBLIC ET PRIVÉ est un bulletin d'information publié et distribué six fois par année par l'**Association sur l'accès et la protection de l'information (AAPI)**. Corporation à but non lucratif, l'AAPI a pour mission de promouvoir et faciliter la mise en application ainsi que le respect de la Loi sur l'accès et de la Loi sur le secteur privé; un de ses objectifs est de favoriser la recherche et la réflexion en matière d'accès à l'information et de protection des renseignements personnels.

Editeur
Association sur l'accès et la protection de l'information (AAPI)

Rédaction
M^e Diane Poitras

Collaboration chronique jurisprudentielle et enquêtes
Marc Bergeron, Évelyne Racette

Conception et montage infographique
Safran communication + design

Dépôt légal
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
1^er trimestre, 1995
ISNN 1481 2215

Pour commentaires, suggestions ou abonnement, écrire à :

L'informateur public et privé
6480, avenue Isaac-Bédard
Charlesbourg (Québec) G1H 2Z9
Tél.: (418) 624-9285
Fax: (418) 624-0738
courriel : aapi@aapi.qc.ca

www.aapi.qc.ca

Résumés des enquêtes et décisions de la COMMISSION et des TRIBUNAUX SUPÉRIEURS

DÉCISIONS: QUOI DE NEUF?

Résumés de décisions de la Commission d'accès et des tribunaux supérieurs rendues au cours des mois d'août et septembre 1996:

COMMISSION D'ACCÈS À L'INFORMATION

Dossier 95 05 57 *Mally c. Congrégation des témoins de Jéhovah d'Issoudun_Sud & Proc. Gén. du Québec*

Art. 1, 27, 29, 32 de la Loi sur le secteur privé - Art. 1525 du Code civil du Québec - Communication du dossier - Objection préliminaire - Juridiction de la Commission - Notion d'entreprise - La congrégation soutient ne pas être assujettie à la Loi sur le secteur privé, n'exploitant pas une entreprise au sens de l'article 1525 du CCQ. La Commission a rejeté l'objection préliminaire. Tout en poursuivant une mission religieuse, la congrégation exerce une activité économique organisée au sens du Code civil et de la Loi sur le secteur privé. Le législateur n'a certes pas voulu limiter la notion d'entreprise aux seules activités dominées par la loi du marché. Il ne faut pas confondre la mission avec l'exercice des activités pour atteindre cette mission. La preuve a démontré clairement que la congrégation s'acquitte entre autres de gérer les dons reçus, d'administrer les biens acquis à l'aide de ces dons, d'aliéner parfois ces biens, d'emprunter sur leur valeur et d'offrir des services à ses membres à même les fonds recueillis. La Commission a récemment fait l'analyse des objectifs poursuivis par le législateur, dans l'affaire Grenier c. Collège des médecins du Québec (1996) C.A.I. 15 et elle a décidé de consacrer une interprétation large à la notion d'entreprise suivant l'évolution du droit en matière d'accès à l'information. (1996_09_26)

Dossier 95 15 15 *B. c. Groupe Écho_Trans Union du Canada inc.*

Art. 40 du Code civil du Québec - Art. 50 de la Loi sur la faillite et l'insolvabilité - Rectification - Dossier de crédit - Proposition concordataire - Le demandeur veut faire supprimer certaines mentions qui figurent à son dossier de crédit à l'entreprise. Le demandeur a déjà formulé une proposition concordataire qui a été par la suite acceptée et homologuée par la Cour. Au dossier, le titre de la rubrique «faillite» crée donc une certaine ambiguïté sur sa situation économique. Il s'avère, en preuve, que les renseignements inscrits au dossier du demandeur ne sont pas inexacts, incomplets ni équivoques au sens de l'article 40 de la Loi. Mais la Commission accueille partiellement la demande, en ordonnant à l'entreprise de renommer la rubrique « faillite et insolvabilité » afin d'éviter tout malentendu. La proposition concordataire vise justement à régler la situation financière de celui qui la demande pour ainsi lui éviter la faillite. (1996_08_21)

Dossier 95 16 88,89 *Kosko c. Équifax Canada inc.*

Art. 27, 32, 34, 39, 40 et 43 de la Loi sur le secteur privé - Dossier de crédit - Communication - Rectification - Renseignements personnels sur des tiers - Le demandeur tient à obtenir l'accès à la version intégrale de son dossier de crédit détenu par l'entreprise. En vertu de l'article 40 de la Loi, l'entreprise n'a pas démontré à la satisfaction de la Commission que la divulgation des renseignements personnels sur un tiers au demandeur risquerait à la fois de dévoiler des informations concernant ce tiers, et, par la même occasion, de lui nuire sérieusement. En conséquence, le dossier en litige devra être transmis en entier au demandeur suivant l'article 27. Par ailleurs, la Commission n'a pas compétence pour entendre une demande de rectification compte tenu de l'absence d'une demande à l'entreprise à ce sujet. (1996_09_03)

Dossier 96 00 28 F. *c. Dr Claude Bergeron*

Art. 40 du Code civil du Québec - Dossier médical - Demande de rectification - La patiente conteste le fait même d'avoir rendu visite à son médecin pour l'examen de contrôle noté dans son dossier médical. Le médecin soutient fermement avoir reçu la demanderesse dans sa clinique cette journée là. La Commission n'a pu, en regard de la preuve, découvrir la vérité, c'est pourquoi le dossier ne sera pas corrigé mais il devra désormais inclure une déclaration signée de la demanderesse présentant sa version des faits. Il est impossible de donner suite au recours en rectification de l'article 40 CCQ, puisqu'il s'agit ici de notes personnelles et subjectives du médecin, contenues au dossier médical. Dans l'affaire Belleau c. Démo_Club Services inc. (1995) C.A.I. 75, la Commission a précisé que la rectification des renseignements ne peut en effet viser que des données factuelles. Par une telle interprétation, on veut prévenir toute situation où l'opinion d'une personne pourrait être modifiée contre son gré. (1996_08_21)

ENQUÊTES DE LA COMMISSION

Résumés de décisions rendues par la Commission d'accès à l'information suite à des enquêtes complétées au cours des mois d'août et septembre 1996.

Dossier 95 14 73 *X. c. Gauthier & Martin inc.*

Art. 5, 8, 70, 77, 91, et 93 de la Loi sur le secteur privé - Collecte (moyens licites) - Agent de renseignements personnels - Une agence d'investigation aurait recueilli de manière frauduleuse des informations personnelles concernant le plaignant au profit de l'avocate de son épouse, agissant dans une cause de modification de mesures provisoires. Dans l'impossibilité de prouver le contenu de l'appel téléphonique reçu par le plaignant, la Commission a conclu d'informer l'entreprise par écrit des exigences de la Loi spécifiques à la collecte de renseignements personnels. Le représentant de ce type d'entreprise, celle_ci enregistrée auprès de la Commission comme agent de renseignements personnels, doit toujours s'identifier et non pas utiliser une identité fictive, informer la personne de l'objet de la demande de renseignements et de l'utilisation de ceux_ci. (Septembre 1996)

Dossier 95 15 75 *X. c. Ciné vidéo club*

Art. 2, 13, 14, 22 de la Loi sur le secteur privé - Prospection commerciale - Renseignement personnel - Club vidéo - Une cliente de l'entreprise conteste la divulgation faite à une tierce compagnie de ses nom, adresse, et numéro de téléphone recueillis lors de son adhésion. La Commission a conclu qu'aucune disposition légale ne permet au club vidéo de transmettre des renseignements personnels concernant ses membres, sans leur consentement. La plainte est fondée en vertu de l'article 22 puisque l'entreprise aurait dû obtenir, au préalable, le consentement de la plaignante ou à tout le moins, elle aurait pu, dans les circonstances, lui offrir le choix de refuser la communication des informations à une autre entreprise. (Août 1996)

Dossier 95 17 29 *X. c. Centre Desjardins de traitement des cartes inc.*

Art. 8 de la Loi sur le secteur privé - Collecte (devoir d'information) - Dossier de crédit - La Commission a conclu que l'entreprise avait l'obligation, conformément à l'article 8, de fournir à un client qui fait la demande d'une carte de crédit, l'objet du dossier, l'utilisation faite des renseignements et l'endroit où sera détenu son dossier ainsi que les droits d'accès ou de rectification. On constate que le formulaire de demande de carte VISA de l'entreprise n'est pas conforme aux exigences de la Loi car il ne précise que l'objet du dossier. (Août 1996)

Dossier 95 17 35 *X. c. Caisse populaire Desjardins d'Issoudun & Équifax Canada inc.*

Art. 5, 12 et 13 de la Loi sur le secteur privé - Collecte - Dossier de crédit - Consentement - La Commission a conclu que dans la mesure où la Caisse entretient toujours un lien d'affaires avec le plaignant, elle peut utiliser les consentements qu'il avait signés lors de ses demandes de prêts pour obtenir d'une tierce entreprise des renseignements de nature financière à son sujet. Une entreprise peut donc considérer valide des consentements tant qu'elle est en mesure de prouver que les fins pour lesquelles ils ont été demandés sont toujours en vigueur. (Août 1996)

Dossier 96 04 62 *X. c. Madame Y*

Art. 1, 91 et 93 de la Loi sur le secteur privé - Art. 35 à 37 du Code civil du Québec - Communication - Renseignements personnels - Locateur - La propriétaire du logement de la plaignante aurait divulgué, à d'autres locataires, des renseignements personnels la concernant, dont le fait qu'elle se trouve présentement prestataire de la sécurité du revenu. Mais l'intervention de la Commission est limitée aux informations personnelles recueillies, détenues, utilisées ou communiquées par une entreprise, quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles (art. 1 de la Loi). Donc, seule la communication du statut de bénéficiaire de la sécurité du revenu peut faire l'objet d'une intervention, puisque seule cette information se retrouve dans un dossier détenu par la propriétaire. La Commission a simplement recommandé de lui transmettre par écrit la teneur de ses obligations face au respect de la vie privée de ses locataires, prévues dans la Loi sur le secteur privé ainsi que dans le Code civil du Québec. (Août 1996)

Dossier 96 07 64 *X. c. RONA*

Art. 5 de la Loi sur le secteur privé_ Collecte - Numéro de téléphone - Paiement par carte de guichet automatique - La Commission a conclu que l'entreprise avait porté atteinte aux dispositions de la Loi sur le secteur privé en exigeant le numéro de téléphone de la cliente lors d'un achat par carte de guichet automatique. Dans une enquête antérieure (réf. dossier 95 02 12), la Commission a décidé qu'il n'était pas nécessaire de recueillir des renseignements personnels lors d'un paiement par carte de débit. (Août 1996)

NOTE: Le mot «loi» utilisé seul, dans le présent bulletin, réfère à la «Loi sur la protection des renseignements personnels dans le secteur privé, (1993) L.Q.c.-17.