Avis
de la
Commission d'accès à l'information

transmis à la
Commission parlementaire de l'économie et du travail

concernant
l'avant-projet de loi

Loi sur la normalisation juridique des nouvelles technologies de l'information

Juillet 2000
00 10 00

TABLE DES MATIÈRES

INTRODUCTION

L'omniprésence des nouvelles technologies de l'information est un constat que nul ne peut contester. Ces outils de communication que la technologie met maintenant à notre disposition ont révolutionné nos modes d'échanges. Tant l'État que les entreprises du secteur privé recourent à ces nouvelles technologies pour rejoindre leur clientèle respective.

Peu à peu, nous glissons d'un univers papier, que d'aucuns appellent le cyberespace, à un univers électronique, le cyberespace. De tels changements requièrent évidemment toute notre vigilance afin que les droits des citoyens, reconnus par plusieurs lois fondamentales, ne soient pas transformés en droits théoriques ou virtuels.

Les nouvelles technologies de l'information ne doivent donc pas mettre en berne le droit d'accès aux documents des organismes publics, le droit d'accès aux renseignements personnels et le droit de rectification de ces renseignements, droits reconnus entre autres par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la Loi sur l'accès), la *Loi sur la protection des renseignements personnels dans le secteur privé* (la Loi sur le secteur privé), la *Charte des droits et libertés de la personne* et le *Code civil du Québec*.

En 1997, dans son *Rapport quinquennal sur la mise en oeuvre de la Loi sur l'accès et de la Loi sur le secteur privé* (1) , la Commission d'accès à l'information qualifiait d'enjeu

majeur les nouvelles technologies de l'information et de communication. Elle insistait également sur l'importance d'assurer la sécurité et la confidentialité des renseignements personnels. À ce chapitre, la Commission soulignait le caractère urgent et important de la problématique de la cryptographie tout comme elle invitait l'administration publique à examiner les conditions et modalités à mettre en place en vue d'assurer l'authenticité et l'intégrité des messages et communications sur l'inforoute.

Les années qui ont suivi le Rapport de la Commission ont été fertiles en événements de toutes sortes qui ont à nouveau permis de sensibiliser l'administration publique à l'importance de la sécurité et de la confidentialité des échanges électroniques.

Ainsi, en novembre 1997, le Conseil des ministres confiait à la Commission le mandat de faire enquête sur les mesures de sécurité destinées à assurer le caractère confidentiel des renseignements personnels détenus par les ministères, le Conseil du trésor et les organismes gouvernementaux (2) . Rendu public en octobre 1998, le Rapport de la Commission formule toute une série de recommandations visant à resserrer la sécurité et la confidentialité des renseignements personnels (3) .

Dans la foulée de ce Rapport, le Conseil des ministres adoptait, en mai 1999, un plan d'action gouvernemental pour la protection des renseignements personnels. À l'automne de la même année, le Conseil du trésor adoptait la *Directive concernant la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale*.

Cette dernière directive confie expressément au ministère de la Justice le mandat "d'élaborer le cadre légal nécessaire pour assurer la sécurité juridique de la documentation et de l'information, ainsi que la valeur juridique des communications et des transactions effectuées au moyen des technologies de l'information, y compris celles de l'Administration gouvernementale."..Le résultat de ce mandat est traduit dans l'avant-projet de loi intitulé *Loi sur la normalisation juridique des nouvelles technologies de l'information* déposé en juin dernier à l'Assemblée nationale par le ministre délégué à l'Autoroute de l'information et aux Services gouvernementaux.

Il importe également de faire référence au projet de loi n° 122, *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, la Loi sur la protection des renseignements personnels dans le secteur privé, le Code des professions et d'autres dispositions législative*s. Déposé à l'Assemblée nationale le 11 mai dernier par le ministre des Relations avec les citoyens et de l'Immigration, ce projet de loi répond également en partie aux inquiétudes soulevées par la Commission dans son Rapport de 1997.

Dans ce dernier rapport, la Commission mentionnait qu'il n'était pas nécessaire, dans l'immédiat, de modifier substantiellement la Loi sur l'accès et la Loi sur le secteur privé pour tenir compte des développements technologiques des dernières années. En effet, le champ d'application de ces lois ne dépend pas du mode de traitement de l'information. Elles s'appliquent quelle que soit la forme des documents : écrite, graphique, sonore, visuelle, informatisée ou autre.

Trois ans plus tard, il ne fait cependant plus de doute pour la Commission que l'implantation massive des technologies d'information et de communication ne peut plus se faire sans qu'un cadre juridique ne vienne délimiter certains droits et obligations des intervenants.

L'avant-projet de loi sur la normalisation juridique des nouvelles technologies de l'information couvre un très vaste chantier et va bien au-delà des droits énoncés par la Loi sur l'accès et la Loi sur le secteur privé. Ainsi, cet avant-projet de loi, dont les objectifs poursuivis sont décrits à son article premier, vise à la fois

- la sécurité juridique des communications ;

- la cohérence des règles de droit et leur application aux communications effectuées au moyen de documents qui sont sur des supports faisant appel à diverses technologies de l'information ;

- l'équivalence fonctionnelle des documents et la reconnaissance de leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent ;

- le lien entre une personne et un document technologique par tout moyen qui permet de les associer, dont la signature, ou qui permet de les identifier et, au besoin, de les localiser, dont la certification ;

- la concertation en vue de l'harmonisation des systèmes et des normes techniques permettant la communication au moyen de documents technologiques et l'interopérabilité des supports et des technologies de l'information.

La Commission accueille favorablement les principes véhiculés par l'avant-projet de loi sur la normalisation des nouvelles technologies de l'information. Comme nous le verrons ci-après, les dispositions de l'avant-projet de loi relatives à la sécurité juridique des communications effectuées au moyen de documents électroniques pourront également assurer une meilleure protection des renseignements personnels, sans pour autant nier le droit d'accès des citoyens aux renseignements de l'administration publique ou aux renseignements personnels qui les concernent. Le présent avis de la Commission s'attardera à commenter plus spécifiquement l'impact de cet avant-projet de loi sur les droits et obligations énoncés dans la Loi sur l'accès et la Loi sur le secteur privé..

1. SÉCURITÉ ET CONFIDENTIALITÉ : DEUX NOTIONS À NE PAS CONFONDRE

Plusieurs considèrent qu'il y a équivalence entre la notion de sécurité et celle de confidentialité. Pourtant, ces deux notions visent des finalités fort différentes. La sécurité peut, par exemple, garantir l'intégrité d'un document ou encore sa transmission à un destinataire précis. La notion de confidentialité réfère quant à elle à toute une série de règles qui ont pour but de limiter l'accès à certains renseignements aux seules personnes légalement autorisées.

Ainsi, la transmission d'un document encodé peut sembler tout à fait sécuritaire. Cependant, si le destinataire n'est pas légalement autorisé à recevoir ces renseignements encodés, il y aura bris de confidentialité même si toutes les mesures de sécurité ont été respectées. Par exemple, serait illégale la communication d'un renseignement médical concernant une personne à une compagnie d'assurance si la personne concernée n'y a pas consenti. Même si l'organisme qui communique ce renseignement a pris toutes les mesures de sécurité requises pour la transmission de ces renseignements, il y aura tout de même illégalité.

La Commission considère que l'avant-projet de loi fait bien les distinctions qui s'imposent en la matière : la sécurité n'est qu'un outil qui permet de garantir le caractère confidentiel d'un document.

Ainsi, précise l'article 37 de l'avant-projet de loi, lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication ouverts ou fermés.

La personne qui communique un renseignement confidentiel doit donc s'assurer dans un premier temps que le destinataire a droit aux informations. Si tel est le cas, les mesures de sécurité requises pour sa transmission prendront alors toute leur importance. L'avant-projet de loi n'impose pas aux organismes ou entreprises le choix d'une technologie particulière pour respecter ses obligations de sécurité.

À ce sujet, la Commission tient à signaler qu'elle approuve sans réserve le fait que l'avant-projet de loi, tout comme le projet de loi n° 122, ne privilégie pas une technologie particulière pour garantir la sécurité des documents.

La Commission considère en effet que le législateur ne devrait jamais assujettir le respect de droits fondamentaux à l'existence, bien souvent éphémère, d'une technologie particulière. C'est à cette dernière à s'adapter aux droits que le législateur reconnaît aux citoyens et non pas le contraire.

2. LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Conformément à la Loi sur l'accès et à la Loi sur le secteur privé, les renseignements personnels, c'est-à-dire ceux qui concernent une personne physique et permettent de l'identifier, sont confidentiels. Cette confidentialité, dont l'assise est le respect du droit à la vie privée, est également reconnue par la Charte des droits et libertés de la personne et le Code civil du Québec. La confidentialité d'un renseignement garantit que ce dernier ne sera pas indûment rendu accessible ou communiqué à une personne qui n'y a pas droit.

L'avant-projet de loi ne remet aucunement en cause la confidentialité des renseignements personnels. Au contraire, plusieurs de ses dispositions viennent préciser certaines obligations à la confidentialité ou encore les moyens qui permettent de garantir cette dernière. Bien sûr, cet avant-projet de loi n'a pas pour objet d'assurer la protection des renseignements personnels, cette protection étant déjà reconnue entre autres par la Loi sur l'accès et la Loi sur le.secteur privé, lois dont le caractère est par ailleurs prépondérant sur les autres lois québécoises, y compris une éventuelle loi sur la normalisation des nouvelles technologies de l'information. Toutefois, les dispositions de l'avant-projet de loi qui visent la sécurité des renseignements confidentiels auront un impact que l'on ne peut ignorer tant sur les renseignements personnels détenus par les organismes publics que ceux détenus par les entreprises du secteur privé.

La protection des renseignements personnels ne se limite pas à la seule confidentialité de ces renseignements. La Loi sur l'accès et la Loi sur le secteur privé énoncent en effet plusieurs règles qui visent à limiter la cueillette de renseignements personnels et à restreindre l'utilisation qui en est faite par celui qui les recueille. Cette protection englobe de plus des normes à respecter en matière de conservation et de destruction

des renseignements personnels. À l'exception de la destruction des renseignements, l'avant-projet de loi n'aborde pas ces derniers volets de la protection des renseignements personnels.

2.1 De meilleures garanties de confidentialité

… lors de la consultation

La Commission accueille très favorablement l'article 28. Cette disposition a entre autres pour objet de garantir la confidentialité des renseignements personnels lors de leur consultation. Ainsi est-il prévu que la personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

… lors de la transmission

En outre, tel que le précise l'article 37, la confidentialité d'un document peut être protégée, au moment de sa transmission, entre autres, par le chiffrement du document avant sa transmission, par l'utilisation de canaux de communication munis de fonctions de chiffrement, par l'utilisation de canaux de communication dont une personne est responsable et qui sont dédiés à la transmission de ses documents ou de ceux provenant de personnes à qui elle donne accès à ces canaux ou par tout autre moyen convenu entre l'expéditeur et le destinataire.

Cet article 37, croit la Commission, serait un outil concret et explicite favorisant une meilleure protection des renseignements personnels et compléterait bien les articles 62.1 de la Loi sur l'accès et 10 de la Loi sur le secteur privé, tels qu'ils devraient être modifiés par le projet de loi n° 122. Ces deux nouvelles dispositions prévoiraient en effet q'un organisme public ou une entreprise du secteur privé qui recueille, détient, utilise ou communique des renseignements personnels doit prendre et appliquer des mesures de sécurité propres à assurer le caractère confidentiel de ces renseignements, y compris lors de l'utilisation d'une technologie.

… lors de la destruction

L'article 23 de l'avant-projet de loi précise que les documents dont la loi exige la conservation peuvent être détruits s'ils ont fait l'objet d'un transfert sur un support faisant appel à une autre technologie. Toutefois, si le document est en possession de l'État ou d'une personne morale de droit public, cette destruction devra respecter le calendrier de conservation établi conformément à la Loi sur les archives.

De plus, dans tous les cas, la personne responsable de la destruction des documents devra s'assurer de.la protection des renseignements confidentiels et personnels que peuvent comporter les documents devant être détruits. Une telle obligation est déjà implicitement prévue dans la Loi sur l'accès et la Loi sur le secteur privé. En outre, l'article 23 est tout à fait compatible avec les *Exigences minimales relatives à la*

*destruction des renseignements nominatif*s, exigences établies en 1993 par la Commission.

… lors de la détention par un prestataire de services

La Commission souligne de plus la pertinence de l'article 29 qui stipule qu'un prestataire de services à qui un document est confié est tenu, durant la période où il en a la garde, d'en assurer la sécurité, d'en préserver l'intégrité et, les cas échéant, d'en protéger la confidentialité et d'en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Ce prestataire de services devra également assurer le respect de toute autre obligation prévue dans la loi relativement à la conservation du document.

Encore une fois, cette disposition reprend des obligations que les articles 67.2 de la Loi sur l'accès et 20 de la Loi sur le secteur privé imposent déjà aux mandataires ou aux personnes parties à un contrat de services ou d'entreprise avec un organisme public ou une entreprise du secteur privé.

En obligeant les détenteurs de renseignements personnels, quels qu'ils soient, à prendre les mesures de sécurité nécessaires, il est indéniable que la confidentialité de ces mêmes renseignements sera mieux assurée.

2.2 Contrôler l'accès aux renseignements personnels qui ont un caractère public

L'article 27 de l'avant-projet de loi vise à restreindre l'accès aux renseignements personnels qui ont un caractère public. Cette disposition aurait un impact majeur et important sur l'article 55 de la Loi sur l'accès. Ce dernier article précise qu'un renseignement personnel qui a un caractère public en vertu de la loi n'est pas confidentiel alors que l'article 27 de l'avant-projet de loi précise ce qui suit :

> 27. Pour assurer le respect de la finalité pour laquelle a été rendu public un document technologique qui comporte des renseignements personnels, l'utilisation de fonctions de recherche extensive doit être préalablement autorisée par la personne responsable de l'accès à ce document ; celle-ci peut fixer des conditions pour l'utilisation de ces fonctions.
>
> Cependant, les critères permettant d'autoriser l'utilisation de fonctions de recherche extensive dans de tels documents technologiques sont déterminés par règlement du gouvernement.

Cet article 27 propose une piste de solution intéressante à un problème longuement décrit dans le Rapport quinquennal de la Commission de 1997.

Ainsi, chaque fois qu'une disposition législative prévoit le caractère public de renseignements personnels, une fin bien précise est visée. Ainsi, le caractère public des renseignements consignés dans un rôle d'évaluation permet aux citoyens de connaître,

aux fins de comparaison, pour l'une ou l'autre des unités d'évaluation, l'identité et l'adresse du propriétaire ainsi que la valeur de ses immeubles. Le caractère public de certains renseignements concernant les fonctionnaires de l'État permet d'assurer une transparence dans les communications ou dans la gestion des fonds publics. Afin d'éviter la fraude électorale et d'assurer la transparence du processus du choix des élus, les lois électorales prévoient également le caractère public de certains renseignements personnels.

Consignés sur un support papier, ces renseignements seront accessibles aux personnes qui prendront le temps de se déplacer pour les consulter ou qui formuleront une demande écrite pour les obtenir. Ces modes d'accès qui, règle générale, étaient les seuls possibles lorsque les lois ont reconnu un caractère public à certains renseignements, garantissent le respect de l'objectif visé par la reconnaissance de ce caractère public. Par contre, lorsqu'ils deviennent facilement accessibles par voie électronique, on peut se demander si une communication massive de renseignements personnels ne vient pas détourner ou contourner cet objectif. L'obtention massive de renseignements personnels à caractère public respecte rarement la finalité visée par le législateur et ouvre facilement la voie à des activités de nature commerciale ou de sollicitation. Tel que l'a déjà mentionné la Commission des droits de la personne et des droits de la jeunesse devant la Commission parlementaire de la culture, la diffusion massive de ce genre de renseignements comporte des risques du point de vue des droits garantis par la Charte des droits et libertés de la personne.

Pour ces raisons, la Commission recommandait donc en 1997 de modifier l'article 55 de la Loi sur l'accès afin de limiter la diffusion de banques de données qui contiennent des renseignements personnels à caractère public.

Malheureusement, le projet de loi n° 122 ne tient pas compte des inquiétudes de la Commission à ce sujet. En fait, le projet de loi esquive complètement cette question en n'apportant aucun amendement à la Loi sur l'accès. Seule la Loi sur le secteur privé est amendée afin d'y ajouter l'article 18.2. Si elle devait être adoptée, cette disposition prévoirait qu'une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement qui a un caractère public en vertu de la loi.

Sans aucune balise, il est à craindre que cet article 18.2 ait un impact aussi néfaste, si ce n'est plus, sur le droit à la vie privée que l'article 55 de la Loi sur l'accès. Cette disposition ouvrira la voie à une commercialisation massive de banques de données contenant des renseignements personnels qui ont un caractère public. Qui plus est, les entreprises du secteur privé pourront communiquer des renseignements personnels à caractère public qu'ils auront pu obtenir des organismes publics conformément à l'article 55 de la Loi sur l'accès.

De plus, cet article 18.2 viendra-t-il limiter l'application des articles 22 à 26 de la Loi sur le secteur privé ? En vertu de ces dispositions, une entreprise peut, sans le consentement de la personne concernée, communiquer à un tiers une liste nominative (nom, adresses et numéros de téléphone) si, au préalable, elle a offert aux personnes concernées l'occasion valable de refuser que ces renseignements soient utilisés par un tiers à des fins de prospection commerciale ou philanthropique.

Une personne qui désire faire retrancher d'une liste nominative des renseignements personnels la concernant peut également le faire, en tout temps, au moyen d'une

demande verbale ou écrite auprès de la personne qui détient ou utilise cette liste. Ce droit au retrait d'une liste nominative sera-t-il mis en sourdine lorsque des renseignements personnels auront un caractère public ?

Dans un tel contexte, il est loin d'être assuré que la finalité visée par les dispositions législatives qui reconnaissent un caractère public à certains renseignements personnels pourra être respectée.

Dans un avis récemment transmis à la Commission parlementaire de la culture, la Commission formule le souhait que le législateur puisse apporter les correctifs appropriés au projet de loi n° 122.

L'article 27 de l'avant-projet de loi permettra-t-il d'éviter l'impact négatif que craint la Commission ? La Commission croit que cette disposition ne répond qu'en partie à ses craintes. Certes l'article 27 limite la communication des renseignements personnels qui ont un caractère public lorsque l'accès à ces renseignements est rendu possible, par exemple, sur un site internet d'un organisme public ou.d'une entreprise du secteur privé. Dans une telle situation, l'utilisation d'une fonction de recherche extensive peut en effet être contrôlée. Mais qu'arrivera-t-il si cet organisme ou cette entreprise communique ces renseignements sur un support papier ou s'il y a commercialisation d'une banque de données contenant de tels renseignements ? Dans ces situations, l'utilisation d'une fonction de recherche extensive est soit inappropriée, soit hors du contrôle de l'organisme public ou de l'entreprise privée.

La Commission comprend par ailleurs que cet article 27 s'inscrit à l'intérieur des objectifs poursuivis par l'avant-projet de loi et qu'il n'a pas nécessairement comme principe d'assurer une forme de protection aux banques de données constituées de renseignements personnels qui ont un caractère public.

De plus, contrairement à la Loi sur l'accès et à la Loi sur le secteur privé, l'avant-projet de loi n'a pas un caractère prépondérant sur les autres lois. Ainsi, il serait plus facile de passer outre à cet article 27 dans une loi particulière sans avoir recours à une disposition dérogatoire.

La Commission croit donc toujours que l'article 55 de la Loi sur l'accès et la Loi sur le secteur privé devraient limiter l'accès aux banques de données qui contiennent des renseignements personnels à caractère public.

2.3 Les intermédiaires et leur responsabilité

Les articles 25, 30, 39 et 40 de l'avant-projet de loi décrivent la responsabilité d'un intermédiaire qui fournit des services de consultation ou de transmission sur un réseau de communication ou qui fournit les services d'un réseau de communication.

De façon générale, l'intermédiaire engagera sa responsabilité dans les situations suivantes :

- l'intermédiaire qui offre des services de conservation de documents sur un réseau de communication pourra devenir responsable s'il a connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite et qu'il n'agit pas pour rendre l'accès aux documents impossible (article 25) ;

- l'intermédiaire qui offre des services de référence à des documents dont un index, des hyperliens, des répertoires ou des outils de recherche sera responsable s'il a connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse pas de fournir ses services aux personnes qu'il sait être engagées dans cette activité (article 25) ;

- l'intermédiaire qui fournit les services d'un réseau de communication exclusivement pour la transmission de documents ou qui les conserve à la seule fin d'assurer l'efficacité de leur transmission ultérieure aux personnes qui y ont un droit d'accès peut être responsable s'il est lui-même à l'origine de la transmission du document, s'il sélectionne ou modifie l'information du document, s'il sélectionne la personne qui le transmet ou le reçoit ou qui y a accès ou s'il conserve le document plus longtemps que nécessaire pour sa transmission (articles 39 et 40) ;

- l'intermédiaire qui, dans le cadre des services de transmission qu'il fournit sur un réseau de communication, conserve sur celui-ci les documents que lui fournit son client, à seule fin d'assurer l'efficacité de leur transmission ultérieure aux personnes qui ont droit d'accès à l'information peut devenir responsable s'il ne respecte pas les conditions d'accès aux documents, s'il prend des mesures pour empêcher la vérification de qui y a eu accès ou s'il ne retire pas du réseau ou ne rend pas l'accès au document impossible alors qu'il a eu connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il n'est pas possible aux personne qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a .ordonné le retrait du réseau ou en a interdit l'accès (article 40).

La Commission n'entend pas commenter chacune de ces dispositions. Néanmoins, elle considère que ces dernières pourraient favoriser un meilleur respect des droits énoncés dans la Loi sur l'accès et la Loi sur le secteur privé.

Ainsi, l'intermédiaire ne pourrait nier sa responsabilité s'il constate que des renseignements personnels font l'objet d'un commerce illicite au moyen des services de transmission qu'il offre. Par ailleurs, l'intermédiaire ne saurait empêcher une personne d'avoir accès à un document auquel elle a droit sans engager sa responsabilité.

Quoiqu'il en soit, cette responsabilité de l'intermédiaire ne doit aucunement diminuer celle du détenteur légal de l'information ou du responsable du document, c'est-à-dire, lorsque la Loi sur l'accès ou la Loi sur le secteur privé sont en cause, l'organisme public ou l'entreprise du secteur privé.

De plus, l'avant-projet de loi énonce clairement, et à raison, que le contenu du document demeure sous la responsabilité du responsable du document. Ainsi, l'article 30 précise que l'intermédiaire qui fournit les services d'un réseau de communication ou qui conserve ou transporte des documents sur un tel réseau n'est pas tenu d'en surveiller l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite. Toutefois, mentionne cet article 30, l'intermédiaire ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs fonctions relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions.

La Commission considère qu'il est tout à fait à propos de stipuler qu'un intermédiaire ne doit pas empêcher un responsable de l'accès aux documents d'exercer ses fonctions. Tout comme elle ne s'oppose pas à ce que les autorités responsables puissent exercer leurs fonctions relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions. Dans ce dernier cas toutefois, la Commission croit qu'il serait opportun de préciser que les autorités responsables doivent exercer leurs fonctions conformément à la loi. Ainsi, si une loi prévoit qu'un mandat ou l'autorisation d'un tribunal est nécessaire avant de prendre connaissance ou possession d'un document, il ne faudrait pas que l'article 30 permette de contourner cette obligation.

Finalement, tout en soulignant la pertinence des articles 25, 30, 39 et 40, la Commission souhaite que l'on réfléchisse à la possibilité d'inclure, dans la Loi sur l'accès et la Loi sur le secteur privé, les obligations que devraient respecter les intermédiaires. Cette inclusion, croit la Commission, pourrait permettre de mieux répondre aux besoins spécifiques que poursuivent ces deux lois.

3. L'ÉTABLISSEMENT D'UN LIEN ENTRE UNE PERSONNE ET UN DOCUMENT TECHNOLOGIQUE

L'avènement des nouvelles technologies de l'information a soulevé dans son sillon toute une série de questions reliées à l'authentification, la signature électronique, la non-répudiation d'un document. Bien sûr, et ce fait est confirmé par l'avant-projet de loi, la fiabilité d'un document ne se limite pas à ces seules questions.

Ainsi, conformément à l'article 5, est fiable le document dont les composantes sont délimitées et structurées de manière à en assurer l'intégrité au cours de son cycle de vie. Quant à cette intégrité, elle est assurée lorsque, d'une part, il est possible de vérifier que l'information n'est pas altérée et qu'elle est maintenue dans son intégralité et, d'autre part, lorsque le support qui porte l'information lui procure stabilité et la pérennité voulue. L'article 5 précise par ailleurs que dans l'appréciation de l'intégrité, il.est tenu compte des mesures de sécurité prises pour protéger le document au cours de son cycle de vie.

Outre le caractère fiable d'un document, un lien doit nécessairement pouvoir être établi entre ce dernier et une personne pour assurer une réelle sécurité juridique. C'est ce que s'emploie à faire avec succès le chapitre III de l'avant-projet de loi.

3.1 Les moyens de relier une personne et un document technologique

Tel que le précise l'article 41, le lien entre une personne et un document technologique peut être établi par tout procédé ou par une combinaison de moyens, dans la mesure où ils permettent :

1° de confirmer l'identité d'une personne qui effectue la communication ainsi que son association au document et, au besoin, sa localisation ;

2° d'identifier le document et, au besoin, sa provenance, son parcours et sa destination à un moment déterminé.

Cet article 41 laisse libre choix pour la technologie qui servira à établir ce lien entre la personne et le document technologique. Ainsi, tout développement technologique à ce chapitre pourra être mis à profit sans qu'il ne soit pour autant nécessaire de modifier à nouveau la législation.

Tout en laissant le choix d'une technologie, l'avant-projet de loi reconnaît cependant, à l'article 42, que la signature peut servir à l'établissement d'un lien entre la personne et le document technologique. Par ailleurs, ajoute l'article 44, le système de cryptographie asymétrique pourra permettre d'apposer une signature ou autrement servir à l'établissement d'un lien entre une personne et un document. Quant à l'article 43, il établit que la signature d'une personne apposée à un document technologique lui est opposable lorsqu'il s'agit d'un document fiable et qu'au moment de la signature et depuis, le lien entre la signature et le document est assuré.

3.2 L'identification des personnes

Les articles 41 à 44 s'emploient donc à décrire les moyens de relier une personne et un document. Encore faut-il prévoir des mesures qui permettront de confirmer l'identité des personnes. Les articles 45 et suivant de l'avant-projet de loi énoncent donc ces règles qui permettront entre autres d'établir l'identification et le repérage des personnes. La vérification de l'identité d'une personne pourra se faire au moyen de divers documents. Encore une fois, et la Commission l'apprécie, l'avant-projet de loi maintient une ligne de neutralité technologique.

Ainsi, l'identité d'une personne pourra être établie en se référant aux registres prévus au Code civil du Québec ou à la *Loi sur la publicité légale des entreprises individuelles, des sociétés et des personnes morale*s. La vérification de l'identité d'une personne pourra également être établie à partir de caractéristiques, connaissances ou objets qu'elle présente ou possède. Un document technologique pourra également servir à cette identification.

À ce dernier sujet, la Commission tient à rappeler que certaines lois interdisent l'utilisation d'identifiants créés à des fins précises. Ainsi, par exemple, la carte d'assurance-maladie ne peut être exigée que pour vérifier l'identité et l'admissibilité d'une personne qui requiert des soins ou services de santé. L'obligation d'exhiber son permis de conduire est également strictement encadrée par la législation québécoise. En conséquence, la Commission croit qu'il serait approprié de préciser que la vérification de l'identité d'une personne doit se faire dans le respect de la loi.

Finalement, la Commission accueille favorablement les articles 45 et 46 qui visent entre autres à.maintenir confidentiels certains renseignements nécessaires à l'établissement de l'identité d'une personne. Ainsi, l'article 45 prévoit que les renseignements confidentiels que contient un document qui sert à confirmer l'identité d'une personne doivent être protégés. Quant à l'article 46, il précise que le document technologique qui sert de preuve d'identité doit être protégé contre l'interception lorsque sa conservation ou sa transmission sur un réseau de communication rend possible l'usurpation de l'identité de la personne visée par ce document. De plus, ajoute ce même article, la confidentialité de ce document doit être protégée, le cas échéant, et sa consultation doit être journalisée.

L'ensemble de ces mesures, estime la Commission, facilitera grandement les échanges entre le citoyen et l'administration publique et entre ce même citoyen et les entreprises avec lesquelles il fait affaire.

En effet, les règles relatives à la fiabilité des documents et à l'identification des personnes éviteront que des personnes non autorisées puissent avoir accès à des renseignements personnels lorsque les nouvelles technologies de l'information serviront de base aux communications, l'usurpation de l'identité sera rendue plus difficile et l'exactitude des renseignements échangés sera mieux assurée.

3.2.1. La biométrie comme outil d'identification

Outre les moyens décrits précédemment pour identifier une personne, l'article 50 de l'avant-projet de loi ouvre la voie à l'utilisation de caractéristiques ou de mesures biométriques pour vérifier ou confirmer l'identité d'une personne. La biométrie permet de distinguer une personne d'une autre en ayant recours, par exemple, aux lecteurs d'empreintes digitales, aux lecteurs d'empreintes rétiniennes ou encore à la configuration de la main.

Ces modes d'identification sont pour l'instant peu utilisés, exception faite en matière criminelle où le recours aux empreintes digitales est de commune renommée. Cependant, la technologie offre maintenant de plus en plus la possibilité d'avoir recours à ce mode d'identification.

La Commission d'accès à l'information ne s'est jamais formellement opposée à ce mode d'identification, comme d'ailleurs elle ne l'a jamais autorisé expressément. Selon elle, le recours à cette nouvelle technologie devrait être sévèrement encadré par le législateur afin que soit préservée l'intégrité physique des personnes et soit évitée la création de banques de données nominatives à ce sujet.

Or, l'article 50 de l'avant-projet de loi prévoit toute une série de mesures qui tendent justement à limiter les effets indésirables de l'utilisation de la biométrie à des fins d'identification. Dans la mesure où toutes ces conditions seraient rendues obligatoires, la Commission n'entend pas s'opposer à la cueillette de renseignements biométriques, sous réserve des commentaires formulés à la suite de la description de l'article 50.

Les conditions prévues par cet article 50 sont les suivantes :

- Nul ne peut exiger que la vérification ou la confirmation de l'identité d'une personne soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques.

- Toutefois, une personne peut consentir expressément à ce que son identité soit établie par la biométrie. Ainsi, la volonté de personne doit être prise en compte. Si une personne consent à ce que procédé soit utilisé, elle devra alors, conformément à la Loi sur l'accès ou à la Loi sur le secteur privé, donner un consentement libre, éclairé, limité dans le temps et donné à une fin bien spécifique. La qualité du consentement n'est pas prévue par l'article 50 mais devrait néanmoins être respectée pour valider l'obtention d'un consentement. De plus, le recours aux moyens de biométrie ne doit servir qu'à la seule fin d'identifier cette personne.

- Lorsque la personne consent expressément à ce que son identité soit ainsi établie, il ne peut être fait appel qu'au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et qui comptent parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance. Cette obligation empêche que des renseignements personnels soient recueillis à l'insu de la personne concernée et que des renseignements personnels qui ne sont pas nécessaires fassent l'objet d'une cueillette.

- Tout autre renseignement concernant cette personne et qui pourrait être découvert à partir des caractéristiques ou mesures saisies ne peut être utilisé à aucune autre fin que la vérification ou la confirmation de son identité. Un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande. De même, aucune décision à l'égard de cette personne et qui serait relative à autre chose qu'à l'établissement de son identité ne peut être prise en se fondant sur ces caractéristiques ou mesures.

- Ces caractéristiques ou mesures ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

- La création d'une banque de caractéristiques ou de mesures biométriques doit être divulguée à la Commission d'accès à l'information et celle-ci peut rendre toute ordonnance concernant cette banque afin d'en déterminer la confection, l'utilisation, la consultation et la conservation y compris l'archivage et la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne.

Au sujet de cette dernière condition, la Commission croit toutefois qu'il serait plus approprié que son intervention puisse se faire *a priori*, c'est-à-dire avant que la banque de caractéristiques ou de mesures biométriques ne soit créée. Une telle intervention préalable lui permettrait de s'assurer du respect des conditions de l'article 50.

De plus, la Commission estime que le pouvoir d'ordonnance qui lui est reconnu par cet article 50 devrait également couvrir la communication des banques de données biométriques et non seulement leur confection, leur utilisation, leur consultation ou leur conservation. En effet, la meilleure protection qui pourrait être offerte aux individus à ce sujet serait de restreindre considérablement la possibilité qu'auraient les organismes publics de pouvoir se communiquer entre eux de telles banques de données.

3.3 La certification

Les articles 52 à 66 ont pour objet d'établir diverses règles relatives à la certification et de baliser la prestation de services de certification et de répertoire. Tel que l'énonce l'article 56, les services de certification et de répertoire pourront être offerts par une personne ou par l'État.

De plus, conformément à l'article 58, tout prestataire de services de certification pourra se faire accréditer par une personne ou un organisme déterminé par le gouvernement. De plus, la procédure et les conditions d'octroi de cette accréditation, les délais d'obtention, la modification des conditions d'accréditation, le renouvellement, la suspension ou l'annulation de l'accréditation, ainsi que les frais afférents, seront établis par règlement du gouvernement.

Il ne fait aucun doute que les autorités de certification auront un rôle de premier plan à jouer dans l'établissement et le maintien de la sécurité juridique des documents électroniques. Tout aussi majeur sera le rôle occupé par la personne ou l'organisme désigné par le gouvernement pour l'accréditation des prestataires de services de certification..À cet égard, la Commission entend faire preuve de vigilance et surveillera attentivement l'évolution législative de l'avant-projet de loi. La Commission se réserve également la possibilité d'intervenir en tout temps si les règles de certification et d'accréditation devaient entrer en conflit avec les droits reconnus par la Loi sur l'accès et la Loi sur le secteur privé.

4. LE RESPECT DU DROIT D'ACCÈS

Tel que la Commission l'a déjà précisé, les nouveaux modes de communication, telle l'autoroute de l'information, peuvent mettre en péril l'exercice du droit d'accès des individus dépourvus des outils informatiques requis. Pour ces raisons, la Commission recommandait, dans son Rapport de 1997, que les moyens conventionnels d'accès à l'information soient maintenus. Le droit de consulter un document sur place ou d'en obtenir une copie sous forme écrite et intelligible ne devrait pas être nié.

L'article 4 du projet de loi n° 122, récemment déposé à l'Assemblée nationale, modifie l'article 13 de la Loi sur l'accès et tient compte de cette recommandation : il clarifie l'exercice du droit d'accès en précisant qu'un document qui fait l'objet d'une diffusion peut toujours être obtenu sous une forme écrite et intelligible. Les frais prévus pour obtenir copie d'un document peuvent alors être exigés.

Les articles 26 et 34 de l'avant-projet de loi énoncent des règles de même nature.

L'article 26, qui ne vise que la consultation d'un document, prévoit que tout document auquel une personne a droit d'accès doit être intelligible, soit directement, soit par l'intermédiaire d'un dispositif ou à l'aide d'éléments structurants qui y donnent accès. Toujours selon cet article, le choix d'un support particulier, lors d'une consultation, tient compte de la demande de la personne qui a droit d'accès au document, sauf si ce choix soulève des difficultés pratiques sérieuses, notamment en raison des coûts ou de la nécessité d'effectuer un transfert.

Quant à l'article 34, qui vise cette fois la transmission d'un document, il reconnaît que nul ne peut exiger de quelqu'un qu'il se procure un support ou une technologie spécifique pour transmettre ou recevoir un document, à moins que cela ne soit expressément prévu par la loi ou une convention. De même, nul n'est tenu d'accepter de recevoir un document sur un autre support que le papier ou au moyen d'une technologie dont il ne dispose pas.

L'avant-projet de loi modifie également les articles 10, 13, 16 et 84 de la Loi sur l'accès. Toutes ces dispositions visent les modalités de l'exercice du droit d'accès par une personne qui souhaite obtenir accès à un document détenu par un organisme public ou accès un renseignement personnel qui la concerne. La Commission ne s'oppose pas à ces modifications qui ont toutes pour objet de permettre la consultation à distance des documents requis.

Toutefois, la Commission tient à rappeler que les organismes publics qui offriraient la consultation de leurs documents à distance devront, lorsque ces derniers comportent

des renseignements personnels, avoir recours à toutes les mesures de sécurité qui permettront à la fois d'identifier avec certitude la personne qui formule une demande d'accès et de communiquer ces renseignements sans qu'il n'y ait bris de confidentialité.

CONCLUSION

Loin de s'opposer à l'avant-projet de loi sur la normalisation juridique des nouvelles technologies de l'information, la Commission d'accès à l'information invite le législateur à accueillir favorablement cette initiative.

Selon la Commission, les dispositions qui visent à assurer la fiabilité des documents technologiques et garantir les liens entre les personnes et ces documents favoriseraient le recours aux nouvelles.technologies de l'information sans pour autant amoindrir la portée des droits reconnus par la Loi sur l'accès et la Loi sur le secteur privé.

Toutefois, tel qu'elle en a fait état ci-dessus, certaines dispositions méritent réflexion afin que la protection des renseignements personnels puisse être encore mieux établie.

Aussi la Commission recommande-t-elle ce qui suit :

- Que l'accès aux renseignements personnels qui ont un caractère public soit davantage limité. Ainsi, l'article 27 de l'avant-projet de loi qui restreint l'utilisation de fonctions de recherche extensive devrait avoir une portée plus large. De plus, tant la Loi sur l'accès que la Loi sur le secteur privé devraient circonscrire l'accès à ces renseignements (pages 9 à 12).

- Qu'il soit précisé que les autorités responsables en matière de sécurité publique qui doivent s'adresser à un intermédiaire de service ont l'obligation d'exercer leurs fonctions conformément à la loi. Ainsi, si une loi prévoit qu'un mandat ou l'autorisation d'un tribunal est nécessaire avant de prendre connaissance ou possession d'un document, il ne faudrait pas que l'article 30 de l'avant-projet de loi permette de contourner cette obligation (pages 13 et 14).

- Que l'on réfléchisse à la possibilité d'inclure, dans la Loi sur l'accès et la Loi sur le secteur privé, les obligations que devraient respecter les intermédiaires qui fournissent des services de consultation ou de transmission sur un réseau de communication ou qui fournissent les services de réseau de communication. Cette inclusion, croit la Commission, pourrait permettre de mieux répondre aux besoins spécifiques que poursuivent la Loi sur l'accès et la Loi sur le secteur privé (page 14).

- Que soit précisé que la vérification de l'identité d'une personne doit se faire dans le respect de la loi. Ainsi, l'interdiction d'exiger la production de certains identifiants, comme la carte d'assurance-maladie ou le permis de conduire, serait mieux respectée (page 16).

- Que le recours aux caractéristiques ou aux mesures biométriques reconnu à l'article 50 soit rendu possible uniquement si toutes conditions prévues dans cette disposition sont rendues obligatoires et que la Commission d'accès à l'information puisse avoir un pouvoir de contrôle a priori et non après la création de banques de données biométriques et que le pouvoir d'ordonnance qui lui est reconnu par cet article 50 puisse également couvrir la communication des banques de données

biométriques et non seulement leur confection, leur utilisation, leur consultation ou leur conservation (pages 16 à 18).

- Que les organismes publics qui offriront la consultation de leurs documents à distance s'assurent obligatoirement, lorsque ces derniers comportent des renseignements personnels, que toutes les mesures de sécurité qui permettent à la fois d'identifier avec certitude la personne qui formule une demande d'accès et de communiquer ces renseignements sans qu'il n'y ait bris de confidentialité soient mises en place (page 20).

1. Commission d'accès à l'information, *Vie privé et transparence administrative au tournant du siècl*e, *Rapport sur la mise en oeuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels dans le secteur privé*, juin 1997, 169 p.

2. Gouvernement du Québec, Décret numéro 1498-97 (26 novembre 1997) *Concernant les mesures de sécurité destinées à assurer le caractère confidentiel des renseignements personnels détenus par les ministères, le Conseil du trésor et les organismes gouvernementau*x.

3. Commission d'accès à l'information, *La sécurité des renseignements personnels dans l'État québécois - Une démarche bien amorcée, Rapport sur la sécurité et la confidentialité des renseignements personnels dans l'appareil gouvernemental*, octobre 1998, 155 p.