Note introductive

Les rapports entre les usagers et les instances gouvernementales de même que les règles relatives aux usages de l'information sont en grande partie délimités par les droits et les obligations définis par le droit, de même que par certains principes éthiques et déontologiques. L'évolution contemporaine des environnements dans lesquels interagissent les citoyens et les différentes instances de l'État nécessite de revoir plusieurs des approches et façons de faire. De la même façon, il est nécessaire d'analyser et de comprendre les exigences découlant du droit car les services publics doivent nécessairement fonctionner dans le respect des lois.

Dans le contexte de l'État en réseau, l'identification des droits et obligations relatives à l'information prend de plus en plus d'importance. La numérisation tend à modifier les façons dont le droit encadre les situations d'échanges d'information et les autres transactions, ce qui influe sur ce qu'il est permis de faire dans la conception et l'exploitation de systèmes d'information. Le droit situe aussi les responsabilités des personnes et des organisations qui produisent, détiennent et transmettent de l'information.

Or, les tendances associées à l'émergence de ce qu'il est convenu de désigner par l'expression Web 2.0 contribuent à accentuer certains enjeux et risques. Le rôle accru de l'usager contribue à déplacer et à démultiplier les lieux où se manifestent des risques et enjeux dont plusieurs peuvent présenter des dimensions juridiques. En raison du rôle actif qu'il tient, l'usager lui-même devient un nœud de normativité dont doivent forcément tenir compte les autres acteurs. Les décisions que prend l'usager sont, plus que dans l'Internet de première génération, susceptibles d'emporter des conséquences pour les tiers. Mais comme l'environnement du web 2.0 s'inscrit en dehors d'un modèle dans lequel une entité centrale assume les responsabilités, le cadre juridique se trouve caractérisé par un ensemble de risques répartis entre un nombre indéterminé d'acteurs de dimensions et de statuts différents. Ces mutations nécessitent de penser autrement plusieurs encadrements juridiques de l'administration publique traditionnellement conçue selon un mode hiérarchique très formalisé.

Dans ce document, l'on aborde les encadrements juridiques de l'information en portant attention aux principaux événements de son cycle de vie. On examine de façon intégrée les exigences des lois, les règles applicables au Québec et présidant à la distribution des droits et des devoirs relatifs au traitement de l'information, en particulier les renseignements personnels. L'accent est mis sur les exigences à connaître et à intégrer aux processus plutôt que sur le détail de chacune des dispositions des lois et règlements.

Ce document n'a aucune prétention à l'exhaustivité. Les références mentionnées le sont habituellement à titre d'exemples; les développements présentés visent à cerner les principaux aspects des lois et autres règles applicables. Les explications contenues dans ce texte ne sont pas l'expression d'une opinion juridique sur une question de droit en particulier mais une présentation générale des principes applicables en vertu des lois actuelles.

1. Le phénomène du e-gouvernement

La notion de e-gouvernement concerne l'accomplissement de fonctions gouvernementales en ayant recours aux possibilités offertes par les réseaux informatiques. C'est donc à un questionnement sur les dimensions juridiques relatives à la gouvernance dans un univers en réseau qu'il s'agit d'apporter une contribution.

Les conditions issues de la numérisation et de la cyberspatialisation induisent des façons nouvelles de concevoir les services gouvernementaux de même que plusieurs des interactions associées à la gestion des affaires publiques. Le phénomène d'« internetisation » a un impact sur les processus de décision, d'interaction et de régulation[1]. Il reflète plusieurs tendances caractéristiques de la société de l'information. Ces impacts se manifestent sur les perceptions à l'égard de la légitimité de l'intervention de l'État et de la forme que prend celle-ci. Si certains fondements classiques de l'intervention du droit paraissent avoir perdu leur raison d'être, les conditions engendrées par la numérisation de même que par la post-modernité fondent de nouvelles légitimités pour l'intervention du droit.

Les remises en question et autres secousses qui agitent l'État ne sont pas des phénomènes isolés. Ils concernent les institutions et les valeurs de la modernité. La logique de la modernité, caractérisée par l'empire de la raison, envisage l'État comme un artefact doté de la puissance souveraine expression de la puissance collective détenue par les citoyens. Plusieurs signes donnent à croire que les sociétés contemporaines — et singulièrement, les gouvernements — sont entrées dans une logique nouvelle résumée et condensée par le concept de post-modernité. Chevallier observe que « l'État post-moderne est un État dont les traits restent précisément, et en tant que tel, marqués par l'incertitude, la complexité, l'indétermination; et ces éléments doivent être considérés comme des éléments structurels, constitutifs de l'État contemporain »[2].

Le mouvement actuel et prévisible de l'évolution du e-gouvernement requiert de penser autrement l'intervention du droit et les conditions de la gouvernance. Un regard innovateur doit être posé sur l'intervention de l'État et ce tant au plan des rationalités qui en justifient l'existence qu'au regard de ses modes de fonctionnement. On peut donc considérer que le principal changement juridique induit par l'avènement du e-gouvernement s'inscrit au niveau des façons d'envisager, de concevoir le droit dans un monde en réseaux.

Un ensemble de réalités diversifiées sont visées par la notion d'administration électronique, la Banque mondiale en propose la définition suivante :

---

1 La notion de régulation se distingue de celle de réglementation en ce qu'elle concerne les processus, souvent diversifiés par lequel le comportement d'un système complexe est maintenu ou ajusté en conformité à quelques règles ou normes. Voir André-Jean ARNAUD (dir.) *Dictionnaire encyclopédique de théorie et de sociologie du droit*, deuxième édition, Paris, LGDJ 1993, p.521.

2 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 19.

> *E-Government refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends : better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions.*[3]

L'expression renvoie évidemment aux changements que la généralisation des technologies de l'information induit dans l'administration publique. Dominique Gerbod et Fabien Paquet relèvent deux tendances fondamentales qui leur semblent caractériser l'administration électronique[4]. Il s'agit de l'orientation vers le citoyen et la gestion collaborative. Orientée vers le citoyen, l'administration électronique vise à profiter des possibilités des technologies de l'information pour rapprocher le citoyen de l'administration, faciliter les démarches et les interactions que ce dernier entretient avec les administrations gouvernementales. Ces dernières fonctionnent de plus en plus en étroite relation.

Kenneth Kernaghan et Justin Gunraj observent que l'adoption croissante par les administrations gouvernementales des technologies de l'information prédispose les organismes publics à changer leurs structures et leurs modes de gestion[5]. Un premier facteur de changement induit par les technologies de l'information est la pression engendrée par les lourds investissements et le mouvement conséquent pour une coopération plus intensive entre les organismes gouvernementaux. Un second facteur tient au besoin accru pour de l'expertise de même que des capacités accrues de partager l'information. Cela porte à la création d'entités non ministérielles, au Canada, on a créé des « agences » qui se présentent comme des structures qui posséderaient des caractéristiques plus adaptées à l'accomplissement de fonctions horizontales. Un troisième facteur de changement serait le déplacement d'une partie du niveau intermédiaire de gestion au profit d'une certaine horizontalisation de la hiérarchie administrative, de l'autorité et des contrôles.

Ce type de mutations coïncide avec un redéploiement du rôle et de la configuration de l'État lui-même une mutation complexe dont on cherche à rendre compte à l'aide de diverses notions.

---

3 World Bank Group, A Definition of E-Government, < http://www1.worldbank.org/publicsector/egov/definition.htm >. D'autres définitions sont consignées dans Gilles ST-AMANT, Gouvernement en ligne : cadre d'évolution de l'Administration électronique. Version finale, 7 novembre 2003, révisée en juillet 2005, < www.services.gouv.qc.ca/fr/publications/ enligne/organisation/demarche/modele_evolution.pdf >.

4 Dominique GERBOD et Fabien PAQUET, *Les clés de l'e-administration, vade mecum de l'administration électronique*, Colombelle, Éditions EMS, 2001, 347 p. Voir aussi : Réjean ROY, *Vers un modèle intégré de gouvernement électronique*, Québec, CEFRIO, 2005, 21 p.

5 Kenneth KERNAGHAN and Justin GUNRAJ, « Integrating information technology into public administration : Conceptual and practical considerations,» [2004] *47 Canadian Public Administration*, 525-546.

1.1 Diverses notions pour appréhender l'encadrement normatif

Diverses notions sont évoquées afin de rendre compte de la normativité relative aux environnements de e-gouvernement.

Il est question de morale, d'éthique, de droit et de déontologie. La gestion des données personnelles dans les environnements de e-gouvernement est en effet encadrée par des lois. Mais comme ces lois font un large usage de concepts flous ou à contenu variable, certains ont tendance à avoir recours aux questionnements caractéristiques des démarches éthiques afin d'aider aux analyses qui doivent précéder les décisions de mise en œuvre des environnements d'information. Cette tendance indique que l'on se trouve dans un contexte de régulation, c'est-à-dire un processus continu dans lequel il importe de rechercher et de maintenir les équilibres. En plus de la consience des exigences découlant des règles de droit, il faut se donner la capacité d'évaluer les enjeux et déterminer la signification que prendront, dans un contexte spécifique les notions floues et à contenu variable telles que l'intérêt public, la finalité d'une information personnelle, le caractère suffisant des précautions.

1.1.1. La morale

Selon le *Dictionnaire encyclopédique de théorie et de sociologie du droit*, la morale reçoit une définition sociologique : ensemble des règles de conduite jugées comme adéquates, dans une société donnée, par l'opinion dominante (ses proche de moeurs), étant entendu que ces règles sont variables selon les lieux et les temps.

En philosophie, la morale serait la « recherche par l'individu de la perfection intérieure de son être». Dans la philosophie de l'action, la morale se définirait comme étant la « recherche de l'action juste, conforme à une conception idéale de l'homme, objective et universelle ».[6]

1.1.2 L'éthique

L'éthique est l'une des branches de la philosophie. Elle s'intéresse à la morale et élabore des analyses et des théories sur la nature, la fonction et la valeur des jugements moraux. Ces jugements fondent nos évaluations du comportement d'autrui, de l'organisation de la société et guident nos propres actions.[7]

1.1.3 La déontologie

La déontologie est définie par Bentham comme étant « la science de ce qu'il est convenable de faire ». Les juristes appellent déontologie l'ensemble des devoirs imposés à l'individu dans le

---

6 André-Jean ARNAUD (dir.), *Dictionnaire enclyclopédique de théorie et de sociologie du droit*, Paris, L.G.D.J., 1993, p. 383.

7 Pierre BLACKBURN, *L'éthique, fondements et problématiques contemporaines*, Saint-Laurent (Québec) Éditions du renouveau pédagogique, 1996, p. 4

cadre de sa profession[8]. Dans cette dernière utilisation, la notion concerne l'éthique professionnelle.

Un même événement peut être examiné sous différentes facettes : l'éthique, la déontologie ou le droit. Mais les champs respectifs de l'éthique, de la déontologie et de la responsabilité au plan du droit ne se départagent pas selon des frontières étanches.

Situer les frontières entre ce qui relève de l'éthique, du droit ou de la déontologie est une tâche difficile. Selon les conceptions diversifiées à l'égard de l'éthique, de la morale, du droit et de la déontologie, la ligne sera tracée à des positions différentes. Ainsi, ceux qui adhèrent à une conception limitativement positiviste du droit conviendront aisément de situer en dehors du champ du droit les interrogations que l'on peut entretenir au sujet de l'acceptabilité de telle ou telle conduite. Dans une pareille perspective, le droit s'en tient à sanctionner ce qui est interdit par la loi tandis que la morale fournit des indications afin de délimiter ce qui est juste. Mais avec la constitutionnalisation des droits fondamentaux, il est devenu difficile de postuler que le sens tout entier d'un droit ou d'une liberté, au plan du droit, serait inscrit uniquement dans la loi ou la jurisprudence.

Au surplus, le mécanisme principal en droit québécois pour assurer la détermination de la responsabilité civile repose sur la faute. Le mécanisme utilisé ressemble à celui auquel on a eu recours pour formuler les droits fondamentaux soit l'énoncé d'un standard, c'est-à-dire une prescription commandant à l'interprète de s'enquérir des pratiques jugées raisonnables.

La technique du standard est fréquemment utilisée dans les lois. Le standard est défini par Roscoe Pound comme étant « une mesure moyenne de conduite sociale correcte »[9]. De son côté, Chaïm Perelman écrit qu'il s'agit de « critères fondés sur ce qui paraît normal et acceptable dans la société du moment où les faits doivent être appréciés.»[10] Un standard est une norme souple fondée sur un critère intentionnellement indéterminé.[11]

Cette technique législative convient aux situations pour lesquelles il est difficile de formuler une règle *a priori* afin d'encadrer les comportements que doivent avoir les personnes visées. Par exemple, la diffusion d'émissions de radio ou de télévision s'accommode mal de règles détaillées car elle se déroule dans un univers caractérisé par une évolution rapide et la place importante que tient l'activité créatrice.

---

8 André-Jean ARNAUD (dir.), *Dictionnaire enclyclopédique de théorie et de sociologie du droit*, Paris, L.G.D.J., 1993, p. 174.

9 Roscoe POUND, « Hierarchy of Sources and Forms in Different Systems of Law », [1933] 7 *Tulane L. R.*, 475, p. 482.

10 Chaïm PERELMAN, « Les notions à contenu variable en droit, essai de synthèse », dans Chaïm PERELMAN et Raymond VANDER ELST, *Les notions à contenu variable en droit*, Bruxelles, Établissements Émile Bruylant, 1984, 363 à la p. 368.

11 André-Jean ARNAUD (Dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., Paris, LGDJ, 1993, p.581.

Il est certaines questions pour lesquelles il est difficile ou impossible de légiférer par prescriptions ou interdictions décrivant un comportement. Cela est particulièrement vrai dans les secteurs fortement marqués par l'évolution rapide des techniques et des façons de faire. À l'égard de certaines réalités volatiles comme celles qui caractérisent les activités gouvernementales, l'on constate souvent que le législateur ne maîtrise pas les données esthétiques, scientifiques et techniques, ou que ces données sont susceptibles de changer. Plutôt que de formuler la loi en se référant à un contexte susceptible de changer très rapidement, l'on va plutôt établir, dans la loi, les caractéristiques que doivent posséder les réalités que l'on régit[12].

Lorsqu'ils sont saisis de questions relatives à la possible responsabilité des entités publiques, les tribunaux doivent nécessairement s'enquérir de ce que commandent les « bonnes pratiques » au regard d'une activité donnée. Il n'est pas surprenant qu'ils jettent alors un coup d'œil sur les préceptes moraux, éthiques, déontologiques pertinents à l'activité concernée. À cet égard, Pierre-Marie Dupuy observe que :

> […] *la responsabilité se situe toujours à un carrefour; au point de rencontre ou de collision entre deux logiques ou deux aspirations. Citons, dans un ordre (ou un désordre) faussement chronologique : à la rencontre entre la justice divine et l'inconstance humaine; entre la liberté de la personne et l'indifférenciation de la collectivité; entre la morale individuelle et l'éthique sociale; entre l'assurance et le châtiment; entre le dommage, la faute et le risque; entre la logique de la causalité et celle de l'imputabilité; entre les obligations du responsable et les droits des victimes, entre la punition assurée par la collectivité et la justice privée*.[13]

Selon le point de vue, les auteurs placent soit l'éthique, soit la morale ou la déontologie ou le droit au centre de leurs préoccupations. Lorsque l'on se présente comme un éthicien, le droit est présenté comme un accessoire dont on doit tenir compte mais qui serait moins complet que l'éthique. Pour le juriste, l'éthique, qui se confond souvent avec la morale, est perçue comme une sorte de réservoir d'idées et d'arguments pour justifier tantôt une règle de conduite tantôt une décision. Ces univers normatifs portent des regards différents sur les mêmes réalités. Mais comme il s'agit généralement des mêmes réalités, il peut arriver que des instances éthiques et des instances juridiques portent des jugements sur des comportements. L'un pouvant s'alimenter aux raisonnements de l'autre.

D'un point de vue philosophique, on entend par la morale, la « recherche par l'individu de la perfection intérieure de son être»[14] ou encore suivant la philosophie de l'action, « la recherche de l'action juste, conforme à une conception idéale de l'Homme, objective et universelle». Armande Saint-Jean écrit que :

---

[12] Pierre TRUDEL, « Law in Puirsuit of Information Quality », in Urs GASSER (Ed.) *Information Quality Regulation : Foundations, Perspectives and Applications,* Baden Baden, Schulthess, 2004, 91-105.

[13] Pierre-Marie DUPUY , « Responsabilité », dans Denis ALLAND et Stéphane RIALS, *Dictionnaire de la culture juridique*, Paris, Lamy, PUF, 2003, p. 1341.

[14] André-Jean ARNAUD (Dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., Paris, LGDJ, 1993, p. 383.

> […] *morale et éthique se différencient l'une de l'autre, bien que l'une n'aille pas sans l'autre. En fait la morale prend appui sur des valeurs reconnues pour proposer de nouveaux critères et, d'une certaine façon, relativiser les principes, les valeurs, les normes, les codes, les règlements. La différence principale entre la morale et l'éthique réside dans la distance qui sépare l'absolu du contingent, l'abstrait du concret.*[15]

Saint-Jean ajoute que :

> *Là où la morale pose des principes indépendamment de toute condition ou de tout rapport avec autre chose, l'éthique détermine les choix à faire dans la conscience des principes absolus et dans la connaissance des contingences imposées par les circonstances.*[16]

Envisagée d'un point de vue sociologique, la morale se présente comme l'ensemble des règles de conduite jugées comme adéquates dans une société donnée, par l'opinion dominante, ces règles étant variables selon les lieux et le temps. La morale, dans ce dernier sens, se confond avec les mœurs.

Philippe Jestaz remarque que :

> *l'ensemble formé par les mœurs se présente comme un réseau plus ou moins touffu de règles sociales disparates qui ont en commun* […] *une origine anonyme,* […] *une absence de contrainte sociale spécialement organisée* […] *et une grande efficacité malgré tout*.[17]

La déontologie s'envisage comme la « science de ce qu'il est convenable de faire». On la définit également comme étant « l'ensemble des devoirs imposés à l'individu dans le cadre de sa profession»[18]. À l'instar de la morale, la déontologie, selon Pierre Fortin et Pierre-Paul Parent, « renvoie au devoir faire qui réfère au bien et au mal, à ce qui est acceptable ou non dans un groupe, et qui permet d'assurer une meilleure cohésion au sein de ce groupe»[19].

Toutes les introductions au droit relèvent les controverses au sujet de ce qui doit être tenu pour faire ou non partie du droit. Ainsi, une première grande dichotomie est due à la coexistence des traditions jusnaturalistes, selon lesquelles le droit est l'expression de la justice et des traditions

---

15 Armande SAINT-JEAN, *Éthique de l'information-Fondements et pratiques au Québec depuis 1960*, Montréal, Presses de l'Université de Montréal, 2002, p. 38.

16 Armande SAINT-JEAN, *Éthique de l'information-Fondements et pratiques au Québec depuis 1960*, Montréal, Presses de l'Université de Montréal, 2002, p. 38.

17 Philippe JESTAZ, *Le droit*, 4e édition, Paris, Dalloz, 2002, p. 29.

18 André-Jean ARNAUD (Dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., Paris, LGDJ, 1993, p.174.

19 Pierre FORTIN et Pierre-Paul PARENT, *Le souci éthique dans les pratiques professionnelles, guide de formation*, Paris, L'Harmattan, 2004, p. 56.

positivistes postulant que le droit est constitué des seules lois posées par les personnes ou organes institués pour ce faire[20].

D'autres environnements normatifs peuvent nécessiter de juger des comportements. Ainsi, pour les professionnels, la responsabilité déontologique sanctionne les écarts de conduite des professionnels. Plus généralement, la morale, qui présente un caractère diffus, se décelant dans les opinions plus ou moins généralement partagées contribue à structurer les jugements qui sont portés sur les faits et gestes des personnes.

En somme, l'activité gouvernementale est forcément régie par un ensemble de principes qui peuvent se rattacher à la morale. Il s'agira habituellement d'une morale citoyenne découlant des principes généralement partagés dans le contexte d'une société démocratique. Lorsque l'on convient de se soumettre à un ensemble normatif fondé sur la morale, il y a un risque que cet ensemble de règles et de préceptes en vienne à se confondre avec les règles de droit appliquées par les tribunaux et possédant un caractère impératif.

1.1.4 Le droit

La définition du droit figure au nombre des controverses scientifiques les plus séculaires. L'on s'accorde toutefois à reconnaître que le droit est l'ensemble des règles en vigueur dans un ordre juridique donné. C'est ce qu'on appelle généralement le « droit positif ». Ainsi, les lois actuellement en vigueur au Québec constituent une partie du droit positif béninois. Lorsque le terme mot est employé à l'égard des personnes, (j'ai le droit, tu n'as pas le droit) il désigne un pouvoir accordé par le droit positif à des individus ou groupes d'individus de faire quelque chose. Un autre sens, plus ancien encore est donné au vocable droit : le droit serait l'ensemble des rapports justes entre les hommes. L'étude et la pratique du droit consisteraient en l'art de l'équitable et du bon sens. Cette justice est appréciée selon l'ordre de l'univers.

1.1.5 La gouvernance

La gouvernance est devenue, depuis la décennie 1990 le « mot fétiche censé condenser et résumer à lui seul l'ensemble des transformations qui affectent l'exercice du pouvoir dans les sociétés contemporaines […] »[21]. La notion correspond à la manière d'orienter, de guider, de coordonner les activités d'un pays, d'une région, d'un groupe social ou d'une organisation privée ou publique. Le mot est ancien mais il connaît un regain de popularité depuis une décennie. Il désigne « un mode de gouvernement organisé sur la base d'une coopération, d'un partenariat ou

---

20 André-Jean ARNAUD (Dir.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., Paris, LGDJ, 1993, p.190.

21 Jacques CHEVALLIER, « La gouvernance, un nouveau paradigme étatique ? » (2003) 105/106 *Revue française d'administration publique*, 203-217, 203.

d'un contrat, entre une pluralité d'acteurs aussi bien publics que privés »[22]. La gouvernance renvoie à une idée de réunion, de collaboration de l'ensemble des acteurs de la société quel que soit le niveau. Ainsi, elle se conçoit, selon Thomas B. Riley, comme étant le « résultat de l'interaction du gouvernement, de la fonction publique et des citoyens dans l'ensemble du processus politique ». Selon Andrée Lajoie, s'appuyant sur une étude faite pour la Commission du droit du Canada par Tim Plumptre[23], le concept de gouvernance « concerne tout ce qui a trait aux institutions, aux processus et aux traditions qui interviennent dans les débats d'intérêt public »[24] ce qui inclut le gouvernement et le secteur public, mais aussi la société civile, le secteur privé, les citoyens, les médias, etc. C'est comme s'il importait plus que jamais de reconnaître que le pilotage de la société passe non seulement par les structures de l'État mais par un ensemble beaucoup plus large de lieux de délibération et de pouvoir.

Pour apprécier l'importance du concept dans le contexte du e-gouvernement, il suffit de référer à la nécessité d'associer tous les partenaires pour assurer le développement harmonieux d'un territoire donné[25]. Plus globalement encore, il faut constater que la société de l'information fait éclater et rend de plus en plus obsolètes les fonctionnements cloisonnés, qu'ils soient le fait de l'État lui-même ou de la société civile. Steven Rossel écrit à cet égard que :

> *À mesure que la société devient plus interconnectée, complexe et turbulente, les façons plus traditionnelles de l'organiser et de la gouverner deviennent dépassées. Dans un environnement plus scolarisé, interconnecté et riche en informations, les systèmes gouvernementaux qui reposent sur un flux limité d'informations, y compris la bureaucratie et la démocratie représentative, perdent leur crédibilité et leur autorité*.[26]

L'exercice des fonctions gouvernementales passe de plus en plus par une capacité de dialogue avec l'ensemble des participants concernés. Il faut aussi anticiper les conséquences, au plan du droit, des possibilités sans précédent de produire et d'échanger des informations. Le paradigme du « flux limité et contrôlé » d'information fait place au paradigme de la disponibilité illimitée d'information.

1.1.6 La gouvernance électronique

Les processus associés à la gouvernance peuvent se dérouler dans cet espace qui paraît résulter des interconnexions entre des outils informatiques. Ce que l'on désigne par l'expression

---

22 « Les mots de la gouvernance, » *Sciences Humaines Hors série*, nº 44 mars-avril-mai 2004, p. 6; Catherine BARON, « La gouvernance : débats autour d'un concept polysémique, » (2003) 54 *Droit et Société*, 329-351.

23 Tim PLUMPTRE, *Vers un plan de recherche sur la gouvernance*, Commission de réforme du droit du Canada, Ottawa, 1998.

24 Andrée LAJOIE, *Gouvernance et société civile, Intervention devant la Société royale du Canada*, 20 novembre 1999, tapuscrit, 17 pages.

25 Jean-Yves PRAX, *Le management territorial à l'ère des réseaux*, Paris, Éditions d'organisation, 2002.

26 Steven A. ROSSEL (Dir.), *Gouverner dans une société de l'information*, Institut de recherche en politique publique, 1996, p. 93.

cyberespace[27]. Les réseaux découlent d'interactions entre personnes poursuivant un but commun. Le phénomène de réseautage suppose l'émergence d'environnements interconnectés unissant les décideurs, les chercheurs, les régulateurs de même que les autres acteurs jouant un rôle dans la gouvernance des espaces au sein desquels se déroulent les activités de gouvernance[28].

Dans l'univers cyberspatial, la gouvernance correspond à la « manière de diriger et d'administrer propre à un gouvernement en ligne, permettant à celui-ci, grâce à l'utilisation d'Internet et des technologies de l'information et de la communication (TIC), d'améliorer les services publics, de développer la responsabilisation et la transparence dans les relations entre les citoyens et l'Administration, tout en favorisant le développement d'une société de l'information et le processus de démocratisation qui l'accompagne ».[29]

Cette notion possède, selon Pierre Lévy, « trois caractéristiques essentielles, qu'il importe de bien saisir si l'on veut en tirer toutes les conclusions concernant les nouvelles formes de gouvernance : l'inclusion, la transparence et l'universalité »[30] :

- **inclusif** : le cyberespace « permet l'expression publique à tous les individus, groupes, institutions et communautés, y compris à des communautés (les communautés virtuelles) qui ne lui préexistaient pas »[31].
- **transparence** : le cyberespace autorise « un degré d'accessibilité à l'information supérieur à tout ce qui avait pu être expérimenté auparavant. [...] Cette nouvelle accessibilité de l'information [...] fait perdre une bonne part de leurs privilèges aux élites classiques du pouvoir politique »[32].
- **universalité** : le cyberespace « en même temps que d'autres facteurs techniques, économiques ou écologiques, [...] contribue donc à relativiser les frontières des États-nations et même des ensembles géopolitiques [...] »[33].

---

27 L'on convient généralement que le mot « cyberspace » (cyberespace en français) a été introduit dans le langage par l'auteur William Gibson dans son roman *Neuromancien*. Pour Gibson, le « cyberespace », appelé aussi « infosphère », est l'espace virtuel des ordinateurs reliés en réseaux qu'explorent les « cybernautes » dont les systèmes nerveux sont directement branchés sur ceux-ci grâce à une prise fixée sur leur crâne. L'expression est désormais utilisée dans un sens moins péjoratif pour désigner l'espace qui paraît résulter des raccordements entre une multitude d'ordinateurs et autres outils informatiques. Voir : Jean-Claude GUÉDON, *Internet le monde en réseau*, Paris, Découvertes Gallimard, 2000.

28 Manuel CASTELLS, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998; François OST et Michel de KERCHOVE, *De la pyramide au réseau : pour une théorie dialectique du droit*, Bruxelles, Publications des facultés universitaires Saint-Louis, 2002.

29 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp .

30 Pierre LÉVY, « Vers la cyberdémocratie », http://www.intervir.org/n1/levy/12.htm.

31 P. LÉVY, *id*.

32 P. LÉVY, *id*.

33 P. LÉVY, *id*.

Au plan du droit, les tendances lourdes induites par ces facteurs accentuent l'importance des droits fondamentaux relatifs à la participation aux espaces publics. Le phénomène suppose l'émergence de stratégies régulatrices qui sont conçues de façon différente de celle qui ont marqué l'État bureaucratique fondé sur l'information portée par le support-papier.

Dans une organisation étatique ainsi constituée en réseaux, l'enjeu auquel le droit vient répondre est celui de la régulation des droits et devoirs relatifs aux épisodes du cycle de vie de l'information. Alors que dans l'univers bureaucratique dominé par le papier, le droit insiste sur la délimitation des droits d'obtenir ou non telle ou telle information, dans l'univers en réseau, le droit tend vers l'organisation d'une régulation des permissions d'accès et d'usage dévolues aux décideurs et aux citoyens.

Un ensemble de systèmes de normes se discutent et s'appliquent dans l'espace du e-gouvernement. Aux réglementations étatiques et professionnelles s'ajoutent des processus ayant vocation à procurer les encadrements pour des activités qui ne peuvent être entièrement régies par les droits territoriaux. La technique et les contraintes qu'elle induit est aussi source de normativité dans les réseaux.

Dans son « modèle intégré du gouvernement électronique », Réjean Roy inclut les dimensions juridiques au nombre des éléments du cadre commun de gouvernance du gouvernement électronique. Les normativités juridiques concourent avec les normativités administratives, technologiques et politiques à encadrer les interactions et les échanges d'information au sein de l'appareil gouvernemental.

Le e-gouvernement présente les caractéristiques d'un réseau et cela se reflète forcément sur les cadres normatifs régissant son fonctionnement. Les environnements réseautiques ne sont pas des environnements entièrement fermés : il est impossible de postuler qu'ils sont maîtrisés par une ou plusieurs entités qui seraient en mesure de procurer des garanties absolues. Les réseaux sont des lieux au sein desquels on court plus ou moins de risques.

1.2 Les enjeux des politiques en matière de e-gouvernement

Les politiques relatives au e-gouvernement peuvent s'envisager selon les composantes du gouvernement en ligne telles que présentées dans les documents officiels. Au palier fédéral[34], on utilise l'expression « gouvernement en direct » et au niveau provincial québécois[35] on emploie « gouvernement en ligne » pour désigner cette réalité qui renvoie à de nouvelles façons de concevoir et d'assurer les services publics. L'accessibilité et l'efficacité découlant des nouvelles façons de renforcer la fourniture des prestations de l'État et l'exercice des droits démocratiques

---

34 SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Guide d'Internet du Gouvernement du Canada, Principes, objectifs et stratégie de l'initiative Gouvernement en direct*, < http://www.tbs-sct.gc.ca/ig-gi/gs-cd/gol-ged/gol-ged6_f.asp >.

35 MINISTÈRE DES SERVICES GOUVERNEMENTAUX, *Qu'est-ce que le gouvernement en ligne ?* < http://services.gouv.qc.ca/fr/enligne/index.asp >.

par les citoyens. La notion de gouvernement en ligne évoque aussi la proximité pour tous, grâce à un réseau de connexions Internet à haute vitesse couvrant l'ensemble du territoire.

Le gouvernement en ligne

L'expression « gouvernement en ligne » indique la volonté d'accélérer le déploiement de l'information et des services offerts par voie électronique. La notion s'inscrit pratiquement au cœur des efforts déployés, à la révision des processus administratifs afin d'améliorer et de simplifier la relation entre l'État et les citoyens.

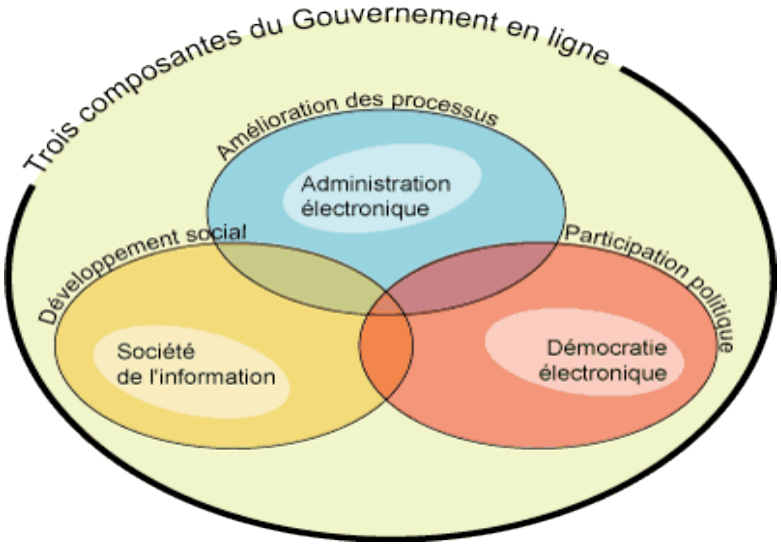
Pour le Ministère québécois des services gouvernementaux, le gouvernement en ligne est défini en fonction de trois grandes composantes qui sont :

l'Administration électronique vise l'amélioration de l'ensemble des processus administratifs internes et externes du gouvernement. On y trouve les services en ligne qui visent spécifiquement l'amélioration des processus de prestation de services avec le citoyen (particuliers et entreprises) ;

la cyberdémocratie vise le développement et l'amélioration des relations avec le citoyen en tant qu'acteur politique ainsi que les relations inter-gouvernementales ;

la société de l'information vise le développement et l'amélioration des relations sociales avec l ensemble des parties prenantes de la société civile : groupes de pression, associations sans but lucratif, etc.

Ces trois ensembles se recoupent comme le montre la représentation des trois composantes du gouvernement en ligne reprise au schéma suivant.



Source : GOUVERNEMENT DU QUÉBEC, Ministère des services gouvernementaux, *Qu'est-ce que le gouvernement en ligne ?,* < http://www.services.gouv.qc.ca/fr/enligne/index.asp >.

Les manifestations juridiques de l'émergence du e-gouvernement se manifestent dans le cadre juridique global : il est en effet nécessaire d'assurer l'émergence de la « société de l'information par la mise en place d'un cadre régulateur exempt d'entraves au déroulement des interactions en ligne. De façon plus spécifique, des mesures concernent le déploiement du gouvernement en ligne assurent la mise en place de services publics accessibles en ligne et enfin, la virtualisation de certains processus délibératifs, ce que l'on désigne par le vocable de cyberdémocratie reflète les possibilités que les réseaux ouvrent au regard de la qualité de la vie démocratique.

Mais la généralisation de l'internet associé au Web 2.0 emporte des défis supplémentaires. L'expression Web 2.0 renvoie à un ensemble de réalités et de situations qui échappent à une définition qui serait exhaustive[36]. Caractérisé par certains éléments emblématiques, le Web 2.0 renvoie à une constellation de fonctions possédant des caractéristiques communes. Parmi ces caractéristiques, il y a un niveau élevé d'implication des usagers dans la fourniture de contenus. On associe également au Web 2.0 ces environnements structurés dans lesquels les contenus sont générés en bonne partie par les utilisateurs comme les sites d'édition collective tel celui de l'encyclopédie *Wikipedia*. Ces sites permettent aux internautes d'éditer et de modifier des contenus à leur guise. Dans d'autres cas de figure, on évoque la possibilité de combiner des applications et des contenus et synchroniser un site Web avec d'autres[37]. Les sites de partage de contenus comme *YouTube* ou *Dailymotion* permettent aux internautes de diffuser des contenus en ligne. Les sites de réseaux sociaux comme *Facebook* ou *Myspace* permettent aux individus de diffuser leur profil personnel de même que d'autres informations portant sur d'autres personnes[38]. Un auteur observe que la notion de Web 2.0 « désigne la tendance, observée chez certaines entreprises présentes sur le Web, à publier un contenu généré par les utilisateurs plutôt que de recourir au modèle d'affaires traditionnel de mise en ligne de contenus médiatiques propriétaires. »[39] On associe souvent au Web 2.0 différentes approches caractérisées par le partage de contenus, de mixage de ceux-ci et leur réutilisation au gré des initiatives des usagers.

L'administration 2.0

Thierry Weibel[40] constate que la période actuelle est marquée par de profondes mutations. Il avance que « les paradigmes traditionnels doivent être reconsidérés ». Dans un tel esprit, l'Administration 2.0, explique Weibel « ce n'est ni la continuité, ni la rupture mais la

---

36 Dion HINCHCLIFFE, « Review of the Year's Best Web 2.0 Explanations' », *Web 2.0 Journal*, < http://web2journal.com/read/165914_p.htm >; Pierre TRUDEL, « La régulation du Web 2.0 », (2008) 32 *Revue du droit des technologies de l'information* 283.

37 Mary MADDEN et Susannah FOX, « Riding the Waves of 'Web 2.0' more than a Buzzword, but still not easily defined, Pew Internet, Backgrounder, < http://www.pewinternet.org/pdfs\PIP_Web_2.0. pdf >; Lis VEASMAN, « 'Piggy Backing' on the Web 2.0 Internet : Copyright Liability and Web 2.0 Mashups », [2008] 30 *COMM/ENT* 311-337.

38 Steven JAMES, « Social Networking Sites : Regulating the Online 'Wild West' of Web 2.0 », [2008] 2 *Ent. L.R.* 47-50.

39 Nicolas W. VERMEYS, « Responsabilité civile et Web 2.0 », *Repères*, juillet 2007, < http://rejb.editionsyvonblais.com/ > (page visitée le 27 novembre 2011).

40 Thierry WEIBEL, *Admininistration 2.0 le service public numérique*, Atela Voirin consultants, octobre 2010.

transformation du service public. Ces transformations sont provoquées par la conjugaison de plusieurs tendances lourdes.

Au nombre de ces tendances, il y a l'émergence de nouvelles technologies, le fait que de plus en plus de citoyens s'attendent à trouver les services publics offerts dans le contexte et selon les conditions que permettent désormais les technologies de l'information. L'obligation désormais incontournable de faire mieux avec moins de ressources. Or, « challengée par le secteur marchand, l'administration doit s'aligner sur les modèles qui ont prouvé leur efficacité » (Weibel, p. 10). Tout comme les entreprises qui utilisent les applications Web 2.0 pour être en relation permanente avec leurs clientèles et leurs partenaires, plusieurs avancent que l'administration publique des prochaines années « reposera en grande partie, dans sa transformation à venir, sur les enjeux de l'Internet 2.0 » à savoir la connectivité, les nouvelles relations citoyennes, les nouveaux partenariats, les nouvelles responsabilités, les impératifs de transparence, de dialogue, l'individualisation des services.

Or, le passage d'une logique d'administration constituée en forme de hiérarchie e dans laquelle le moindre agent est censé agir au nom et aux ordres du ministre présente des défis majeurs au plan des exigences juridiques inhérentes l'administration publique. L'évolution vers ne « administration 2.0 » suppose une relecture et dans plusieurs cas, une réinterprétation de plusieurs principes juridiques fondamentaux présidant à la détermination des droits et obligations de l'Administration et des citoyens.

1.2.1 Les ajustements du cadre juridique

Dans le modèle du Ministère des services gouvernementaux du Québec, le volet relatif aux politiques sur le e-gouvernement désigné par l'expression « société de l'information » vise le développement et l'amélioration des relations sociales avec l'ensemble des parties prenantes de la société civile : groupes de pression, associations sans but lucratif, etc. Il revêt un caractère général. Il concerne l'ensemble de politiques et initiatives destinées à accroître les bénéfices susceptibles de découler du recours accru aux technologies de l'information pour soutenir le fonctionnement des services publics.

1.2.1.1 Les initiatives législatives et les changements aux principes juridiques

Les initiatives législatives visent généralement à assurer que le cadre juridique ne fait pas obstacle au recours aux technologies de l'information. S'agissant du e-gouvernement, il y a des initiatives générales d'ajustement du droit commun. Ces ajustements prennent souvent une grande importance dans le cadre des relations État-citoyen ou État-entreprises puisque tous, y inclus l'État ont besoin d'un cadre juridique qui confirme la validité des interactions réalisées en ligne[41]. D'autres changements, plus immédiatement relié à l'établissement de services en ligne

---

[41] John D. GREGORY, « Solving Legal Issues in Electronic Government: Authority and Authentication, » [2002] 1 *Canadian Journal of Law & Technology*, < http://cjlt.dal.ca/vol1_no2/TOC_set.html >.

s'inscrivent dans une logique de modernisation de l'État, de ses processus et de son fonctionnement. De telles modifications s'expriment par des changements de structures, par la constitution d'entités ayant pour mission de devenir le guichet unique de services conçus en fonction des besoins du citoyen plutôt que reflétant les structures gouvernementales. Enfin, un autre ensemble de changement s'observe au niveau des normes et pratiques, manifestant l'importance que prend la vision managériale de l'administration publique.

Le développement du e-gouvernement est largement tributaire de l'existence d'un cadre juridique qui admet la validité des interactions via les moyens en ligne. Le déroulement d'interactions emportant des conséquences juridiques entre l'État et les citoyens ou entre l'État et les entreprises nécessite un cadre juridique reflétant les caractéristiques du cyberespace.

En droit canadien, l'adaptation du droit commun aux impératifs des transactions en ligne a emprunté la voie indiquée par les lois modèles de la Commission Nations-Unies pour le droit commercial international (CNUDCI). Les textes sur le commerce électronique[42] de même que sur la signature électronique[43] ont inspiré les rédacteurs canadiens. Gregory observe que la Loi modèle des Nations Unies est le standard international au regard de la suppression des barrières juridiques au développement des transactions électroniques[44].

La transposition en droit canadien des principes de la Loi modèle des Nations Unies a emprunté la voie de l'élaboration d'une loi modèle canadienne par la Conférence canadienne sur l'uniformisation du droit[45]. Le texte a été adopté en septembre 1999. Il a le statut d'une recommandation à l'endroit des législateurs des provinces et territoires de même que du Parlement fédéral.

La *Loi uniforme sur le commerce électronique* s'applique à l'ensemble des situations juridiques sauf à celles qui en sont expressément exclues. Son but est de permettre le recours aux documents électroniques sans procéder à la modification de tous et chacun des textes qui pourraient exclure le recours aux documents électroniques ou laisser planer des doutes sur leur validité. La Loi uniforme sur le commerce électronique n'entend pas résoudre toutes les difficultés ni réformer les règles substantives qui trouvent application dans divers secteurs d'activité. Le texte de la Loi uniforme sur le commerce électronique introduit des définitions destinées à assurer la validité et l'acceptabilité juridique des documents établis sur des supports

---

42 *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation*, revisée 1998, http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/1996Model.html .

43 *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation*, 2001, http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/2001Model_signatures.html.

44 John D. GREGORY, « Canadian Electronic Commerce Legislation, » [2002] 17 *Banking & Finance Law Review*, 277, p. 282.

45 CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, *Loi uniforme sur le commerce électronique*, < http://www.ulcc.ca/fr/us/index.cfm?sec=1&sub=1u1>, ci-après désigné par « loi uniforme sur le commerce électronique ».

électroniques, il comporte des dispositions relativement aux conditions de fourniture et de conservation de l'information ainsi que des règles à l'égard de la communication de doc uments électroniques. Il en va de même pour la Loi uniforme sur la preuve électronique[46].

Au Québec La *Loi concernant le cadre juridique des technologies de l'information* vient préciser le droit relatif aux documents consignés sur support papier ou sur d'autres supports comme ceux qui reposent sur le recours aux technologies de l'information. Elle apporte des ajustements à plusieurs notions fondamentales du droit civil québécois afin de rendre celui-ci pleinement compatible avec l'usage sécuritaire des technologies de l'information. La *Loi concernant le cadre juridique des technologies de l'information* met en place un cadre pour la gestion de l'ensemble des documents peu importe le type de support sur lequel ils sont consignés[47].

1.2.1.2 Les principes directeurs

Les lois de régulation — plutôt que les lois de réglementation — paraissent à bien des égards caractéristiques de la société de l'information. Ce sont souvent des lois rédigées en forme de principes directeurs. Ce recours aux principes directeurs de préférence aux règles fixes d'explique par plusieurs facteurs. Par exemple, la partie 2 de la *Loi sur la protection des renseignements personnels et des documents électroniques* énonce ainsi à son article 32 les objets qu'elle vise :

> ***32.*** *La présente partie a pour objet de prévoir l'utilisation de moyens électroniques, de la manière prévue dans la présente partie, dans les cas où les textes législatifs envisagent l'utilisation d'un support papier pour enregistrer ou communiquer de l'information ou des transactions*.

Les principes directeurs se révèlent souvent les seuls capables d'assurer la compatibilité des valeurs et intérêts complémentaires et contradictoires. Ils sont régis par le principe de la non-contradiction : il est possible d'affirmer dans la même loi de principes qui pourraient, dans certaines de leurs applications se trouver en contradiction. Alors l'interprète aura à faire les raisonnements qui délimiteront la portée de l'un et de l'autre des principes. Le recours à des règles fixes se révèle souvent plus difficile pour le législateur qui doit tenir compte d'un ensemble de valeurs risquant à tout instant de se contrecarrer. Dans de telles situations, les principes directeurs permettent des législations très dissemblables protégeant des valeurs et intérêts parfois divergents.

Charles-Albert Morand constate à l'égard des principes généraux qu'ils sont *« Garants d'une interlégalité horizontale entre plusieurs législations finalisées, les principes directeurs assurent*

---

[46] CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, *Loi uniforme sur la preuve électronique*, < http://www.ulcc.ca/fr/us/index.cfm?sec=1&sub=1u2 > ci-après désignée par « loi uniforme sur la preuve ».

[47] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1 ; Pierre TRUDEL, « Notions nouvelles pour encadrer l'information à l'ère numérique : l'approche de la Loi concernant le cadre juridique des technologies de l'information, » [2004] 106 *Revue du notariat*, 287-339.

aussi l'internormativité entre les politiques publiques supranationales, nationales et infranationales. »[48] Tandis que les règles fixes se présentent comme des « portes » donnant ouverture directement à des droits et obligations, les principes directeurs sont des ponts permettant de relier plusieurs territoires normatifs, plusieurs régulations établies suivant des logiques différentes et sans souci de coordination. Les principes directeurs, à l'instar des réseaux de neurones, permettent au droit d'accroître sa complexité en procurant des liens avec d'autres univers normatifs qui permettent la mise en rapport de normes très diverses entre elles.

Dans la société de l'information, les principes directeurs sont multiples : l'introduction de notions indéterminées à l'intérieur de règles fixes crée une ouverture sur les autres normes. Ainsi, la *Loi concernant le cadre juridique des technologies de l'information* procède d'un certain nombre de principes directeurs. Les principes du caractère volontaire du recours aux outils en ligne de même que l'équivalence fonctionnelle et la « neutralité technologique » ont vocation à présider aux transitions qu'il est nécessaire d'effectuer dans les cadres juridiques et les façons de faire qui en résultent.

a) Le caractère volontaire du recours aux outils en ligne

La législation canadienne, telle que le préconise la *Loi uniforme sur le commerce électronique* n'impose pas le recours aux moyens électroniques. Les ajustements apportés au cadre juridique visent à permettre les transactions par voie électronique, non de forcer le recours à ces environnements. John D. Gregory remarque à ce sujet que :

> *The consent rule is absolutely fundamental in a technology-neutral statute, i.e., one that does not prescribe the technology to be used to create legal effects. The proposed user of electronic communications can decide if the technology to be used for the communications is sufficiently reliable fort his or her purposes. Only the proposed user can make that judgment for his or or her purposes.*[49]

Ainsi, la *Loi sur la protection des renseignements personnels et des documents électroniques* pose le principe suivant à l'égard des paiements qui doivent être versés au Gouvernement du Canada :

> *Tout paiement qui doit être remis au gouvernement du Canada peut être fait sous forme électronique, de la manière que le receveur général précise*[50].

En raison même de ce caractère volontaire des communications électroniques, il faut que les outils mis en place soient dignes de confiance. Les protagonistes doivent avoir la conviction qu'ils sont sécuritaires et fiables. C'est sans doute pour ce type de raison que l'on attache tant d'importance à la confiance dans les conditions du succès des environnements proposant des

---

48 Charles-Albert MORAND , *Le droit néo-moderne des politiques publiques*, Paris, LGDJ, 1999, p. 190.

49 John D. GREGORY, « Canadian Electronic Commerce Legislation, » [2002] 17 *Banking & Finance Law Review*, 277, p. 288.

50 *Loi sur la protection des renseignements personnels et des documents électroniques,* L.C., 2000, c. 5, art 34.

actes juridiques en ligne. Ainsi, l'article 6 (1) de la *Loi uniforme sur le commerce électronique* énonce que : « (1) La présente partie n'exige pas qu'une personne utilise ou accepte de l'information sous forme d'un document électronique, mais son consentement peut être déduit par ses actes. »

Au Québec, l'article 2 de la *Loi concernant le cadre juridique des technologies de l'information* énonce le principe général de la liberté des personnes quant au choix des supports qui servent à produire des documents. Cette liberté de choix est conditionnée par l'obligation de respecter les règles de droit. De même, la valeur juridique d'un document n'est ni augmentée ni diminuée pour la seule raison qu'un support ou un autre a été choisi. Plusieurs articles de la loi viennent préciser la portée du principe. Ainsi, l'article 29 énonce 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 par une convention. » La liberté de choix des supports ne peut être limitée que par la loi. Soit que la loi exige l'emploi exclusif d'un support ou d'une technologie spécifique soit que la loi limite les possibilités de choix. Car la liberté du choix des supports est assujettie à la condition du respect des règles de droit, notamment celles prévues au Code civil. De plus, les personnes peuvent avoir par contrat convenu d'utiliser un support particulier. Alors, le choix ainsi fait par convention s'impose au co-contractant. Ainsi, des lois particulières peuvent imposer l'usage d'un support ou d'une technologie spécifique.

b) L'équivalence fonctionnelle

L'expression «équivalence fonctionnelle » concerne l 'équivalence quant aux fonctions accomplies par des technologies différentes. Par exemple, la signature d'un document a pour fonction de marquer le consentement du signataire et d'identifier celui-ci. Alors, la loi précise comment on obtient cette identification et cette expression de consentement lorsqu'on fait usage de documents technologiques. La Loi uniforme sur le commerce électronique couvre l'ensemble des documents et pose que lorsqu'une règle de droit requiert qu'un document soit établi sur support-papier, cette exigence peut être satisfaite par le recours à un document électronique moyennant le respect de certaines conditions.

L'équivalence fonctionnelle entre l'écrit sur support-papier et les autres documents fait également figure de principe directeur des législations sur les interactions dans le cyberespace. L'expression «équivalence fonctionnelle» vise l'équivalence quant aux fonctions accomplies. Par exemple, la signature d'un document a pour fonction de marquer le consentement du signataire et d'identifier, établir un lien avec celui-ci. Alors, la loi précise comment on obtient ce lien lorsqu'on fait usage de documents technologiques. Tous les procédés, mécanismes ou objets capables d'accomplir une fonction déterminée se voient reconnaître un statut équivalent. Par exemple, l'article 9 de la la Loi modèle prescrit les exigences pour que la fourniture d'informations dans un formulaire électronique soit réputé validement accomplie :

> *9. L'exigence d'une règle de droit [d'une juridiction compétente] qu'une personne fournisse de l'information à une autre personne dans un formulaire prévu mais sous une forme autre qu'électronique est satisfaite avec la fourniture de l'information dans un document électronique :*

a) si l'information est fournie dans le formulaire ou dans un formulaire similaire, et l'autre personne a accès au document électronique et peut le conserver de façon à ce qu'il soit utilisable pour consultation ultérieure;

b) lorsque l'information est destinée au gouvernement si :

(i) le gouvernement ou une de ses parties auquel on doit fournir l'information a consenti d'accepter les documents électroniques à cette fin;

(ii) le document électronique s'accorde aux normes relatives à la technologie de l'information et aux règles sur l'accusé de réception, s'il y en a, établies par le gouvernement ou une de ses parties, selon le cas.

La loi n'entend pas privilégier une technologie particulière ou établir une hiérarchie entre les divers documents ou les supports. La voie est ainsi laissée libre à l'innovation car la loi prescrit les conditions que devront respecter les différents procédés techniques existants ou qui pourront exister dans l'avenir. Tous ces moyens doivent procurer les fonctionnalités nécessaires afin de mener des transactions avec le niveau de sécurité requis, compte tenu des enjeux des transactions et des exigences des diverses lois qui peuvent régir ces transactions.

À son article premier, la Loi québécoise pose aussi le principe de l'équivalence fonctionnelle laquelle est assurée entre l'écrit sur support-papier et les autres types de documents. Lorsque son intégrité est préservée, un document a pleine valeur juridique peu importe son support. La loi énonce les conditions pour établir des originaux et des copies de documents technologiques et ainsi que les équivalents technologiques pour d'autres fonctions utilisées dans les transactions comme les mécanismes servant à établir des liens entre une personne et un document, les mécanismes servant à identifier une personne etc.

c) La neutralité technologique

Les législations visant l'ajustement du droit aux contextes des environnements électroniques visent la neutralité technologique. La Loi uniforme sur le commerce électronique ne spécifie pas la technologie qui doit être installée pour la réalisation d'un résultat. Le législateur demeure impartial par rapport aux standards et aux normes technologiques sur lesquels les intervenants ont porté leur choix[51].

La loi exprime, le plus souvent, sous la forme de préceptes généraux, les qualités que doivent posséder les documents et processus utilisés pour les transactions ou les communications. Lorsque les documents possèdent les qualités requises par la loi, ils ont pleine valeur juridique; ils peuvent notamment être utilisés en preuve devant les tribunaux. La loi prescrit les conditions que devront respecter les différents procédés techniques existants ou qui pourront exister dans l'avenir. Tous ces moyens doivent procurer les fonctionnalités nécessaires afin de mener des

---

[51] John D. GREGORY, « Solving Legal Issues in Electronic Government: Authority and Authentication, » [2002] 1 *Canadian Journal of Law & Technology*, < http://cjlt.dal.ca/vol1_no2/TOC_set.html >, p. 12.

transactions avec le niveau de sécurité requis, compte tenu des enjeux des transactions et des exigences des diverses lois qui peuvent régir ces transactions.

1.2.2 Les risques juridiques

Il existe des phénomènes contribuant à moduler les normativités énoncées par les États ou les divers acteurs d'Internet et qui empêchent leur application de bout en bout du réseau. Malgré le caractère global du réseau, les appréciations et les valeurs présentent encore d'importantes différences dans les multiples milieux culturels dans lesquels s'appliquent les règles[52]. De tels phénomènes préviennent l'application de règles qui pourraient être décontextuées par rapport aux situations ou au substrat culturel dans lequel la norme s'applique. L'un de ces phénomènes paraît bien être le risque juridique[53] : l'évaluation que font les acteurs des possibilités concrètes d'application effective de lois nationales ou d'autres règles à leurs activités permet d'expliquer que même si Internet est un réseau global, personne ne se sent tenu de se conformer à la totalité des lois nationales qui peuvent théoriquement trouver application.

Sur Internet, les usagers ont depuis longtemps la possibilité d'introduire des contenus en ligne. Par exemple, ce qui paraît caractéristique du web 2.0 au plan du droit est le rôle plus actif que jamais tenu par l'usager. La notion de web 2.0 renvoie à une kyrielle de situations juridiques dans lesquelles les rôles paraissent moins stables ou délimités[54].

Envisagée dans la logique du réseau[55], la régulation du e-gouvernement dans le contexte du web 2.0 s'exprime par une normativité résultant des décisions de gestion des risques prises par les régulateurs et les autres acteurs actifs sur le net. Sur Internet, les États, les usagers, les entreprises et les autres acteurs gèrent des risques. Par leurs décisions et leurs comportements, l'ensemble des producteurs de normativités créent et relaient les risques issus de la normativité qui leur est applicable à leurs cocontractants et partenaires. Les producteurs de normes ne peuvent prétendre à la souveraineté dans le cyberespace, mais ils conservent une pleine capacité de formuler des règles qui engendrent des risques pour les acteurs.

Ceux qui prennent part à des activités dans les environnements web 2.0 le font avec plus ou moins d'intensité selon qu'ils ont ou non conscience qu'ils auront à supporter plus ou moins de risques. Les configurations techniques, les modes de fonctionnement, les normes applicables et

---

52 Jack GOLDSMITH et Tim WU, *Who Controls the Internet ? Illusions of a Borderless World*, New York, Oxford University Press, 2006, chapitre 9 « Consequences of Borders ».

53 Voir, pour une méthodologie d'analyse des risques juridiques : Franck VERDUN, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, pp. 39 et ss.

54 Pierre TRUDEL, « La régulation du web 2.0» dans *Les nouveaux services de l'Internet face au droit, Regards croisés sur le web 2.0*, Actes du colloque organisé le 10 octobre 2008, [2008] 32 *R.D.T.I* 283.

55 Thomas SCHULTZ, *Réguler le commerce électronique par la résolution des litiges en ligne*, Bruxelles, Bruylant, 2005, p. 151. Cet auteur envisage le réseau comme un « méta-modèle de régulation ». Voir également dans le même sens, Philippe AMBLARD, *Régulation de l'internet – l'élaboration des règles de conduite par le dialogue internormatif*, Bruxelles, Bruylant , 2004.

les sujets concernés par un environnement web 2.0 sont autant de facteurs qui sont susceptibles d'engendrer, accroître ou limiter les risques des acteurs impliqués.

Bien qu'il paraisse impossible d'énumérer dans l'abstrait l'ensemble des enjeux et risques que peut poser l'exploitation d'un site web possédant les caractéristiques associées au web 2.0, il est possible d'identifier les principales catégories d'enjeux et de risques que la plupart des acteurs voudront considérer afin de calibrer leurs décisions. De façon générique, il est possible de reconnaître que les environnements dans lesquels se déroulent les prestations gouvernementales impliquent des risques de comportement ; ils peuvent présenter des risques du fait de leur configuration technique ou ergonomique et il y a des risques de régulation. Chacun de ces risques peut être géré en créant ou en accentuant les risques associés à l'une ou l'autre de ces catégories. C'est de cette façon que paraît fonctionner la normativité effectivement agissante dans les environnements en réseaux du e-gouvernement.

1.2 La normativité en réseaux

Les réseaux sont le résultat d'interactions répétées entre personnes poursuivant un but commun. Le phénomène de réseautage suppose l'émergence d'environnements interconnectés unissant les décideurs, les chercheurs, les régulateurs de même que les autres acteurs jouant un rôle dans la gouvernance des espaces de gouvernement en ligne[56]. Anne-Marie Slaughter observe que dans la mesure où ces réseaux ont de l'influence sur l'élaboration des politiques, ils doivent être envisagés comme participant à la gouvernance internationale.[57]

Un ensemble de systèmes de normes se discutent et s'appliquent dans l'espace de e-gouvernement. Aux réglementations étatiques et professionnelles s'ajoutent des processus ayant vocation à procurer les encadrements pour des activités qui ne peuvent être entièrement régies par les droits territoriaux. La technique et les contraintes qu'elle induit est aussi source de normativité dans les réseaux.

L'espace auquel on a affaire est un ensemble interconnecté constitué de pôles interagissants de normativités. Il est constitué d'espaces dans lesquels prévalent en tout ou en partie des normes qui s'imposent aux usagers. Les normes peuvent s'imposer soit en raison de leur capacité à définir, même implicitement, les conditions de l'exercice des activités, soit parce qu'un État est en mesure d'exercer une autorité. Cet espace est aussi constitué de relais par lesquels s'explicitent et se diffusent les normativités et les conséquences de celles-ci. Les règles émanant des pôles de normativité se relayent et se diffusent dans les différents espaces virtuels. Elles coexistent soit en

56 Manuel CASTELLS, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998; François OST, et Michel de KERCHOVE, *De la pyramide au réseau : pour une théorie dialectique du droit*, Bruxelles, Publications des facultés universitaires Saint-Louis, 2002.

57 Anne-Marie SLAUGHTER, « The Real New World Order, » (1997) 76 *Foreign Affairs*, 183-184.

complémentarité avec d'autres règles soit en concurrence, se proposant à la place de celles qui sont issues d'autres pôles normatifs[58].

1.3.1 Les noeuds de normativité

Dans les environnements de e-gouvernement, les normativités sont définies au sein de pôles diversifiés. Les **États** continuent évidemment de régir les activités se déroulant dans les réseaux sur une base territoriale, mais étant donné que le cyberespace fait abstraction des frontières, des limites pratiques d'application se font de plus en plus sentir. Les limites fixées par le droit territorial s'appliquent dans un espace spécifique. Le droit d'une entité étatique peut trouver application ailleurs dans la mesure où il n'est pas incompatible avec le droit de cet autre territoire.

Dans le réseau, les coordonnées spatio-temporelles se présentent comme un problème toujours posé. Les lieux et les rôles s'y redéfinissent et se redistribuent en fonction des contraintes et circonstances n'obéissant pas à un modèle prévisible. Ces phénomènes résultent des caractéristiques des environnements électroniques tels que l'immatérialité des situations juridiques et les difficultés de preuve qui en découlent, le caractère transfrontière des activités : un acte juridique considéré comme licite dans un lieu peut s'avérer problématique ailleurs.

Le caractère virtuel de plusieurs interactions inhérentes au e-gouvernement soulève des problèmes qui ne peuvent être complètement résolus par les lois ou règlements des États. Il faut envisager la perspective d'une accentuation des mouvements vers l'uniformisation et l'harmonisation des règles régissant les interactions. S'agissant du e-gouvernement, les autorités ont énoncé des principes directeurs prescrivant de quelle façon les exigences des lois territoriales devraient trouver application dans les principales situations se présentant dans le cyberespace.

Les **normes et pratiques des réseaux** constituent un autre pôle de normativité : on observe l'émergence de communautés, ainsi que celle de frontières séparant, non plus des territoires, mais des « domaines », des réseaux, des groupes de travail, etc. Les modalités de l'adoption et de l'administration des normes trouvant application dans les réseaux doivent être examinées, de même que les mesures qui serviront à en garantir l'application.

La **normativité découlant de la technique** doit aussi être considérée. L'architecture technique, soit l'ensemble des éléments ou artefacts, tels les matériels, les logiciels, les standards et les configurations qui déterminent l'accès et les droits d'utilisation des ressources du réseau. Ces objets ont un effet régulateur se présentant suivant diverses formes. L'architecture technique permet ou interdit *de facto*. Elle peut accentuer certains risques ou en atténuer d'autres.

Le e-gouvernement se situe en grande partie dans un environnement construit par la technique. La plupart des environnements résultent de protocoles et autres fonctionnalités définis dans des standards techniques élaborés par des instances professionnelles, commerciales, étatiques ou

---

58 Pierre TRUDEL, « Un 'droit en réseau ' pour le réseau : le contrôle des communications et la responsabilité sur Internet, » dans INSTITUT CANADIEN D'ÉTUDES JURIDIQUES SUPÉRIEURES, *Droits de la personne : Éthique et mondialisation,* Cowansville, Éditions Yvon Blais, 2004, pp. 221-262.

industrielles. Certaines de ces règles ne découlent pas de l'activité d'institutions constituées comme telles : elles résultent des comportements suivis et espérés des acteurs. Par exemple, l'ensemble des éléments ou artefacts techniques sont formulés dans des forums multiples. Comme une part significative des décisions relatives à l'architecture technique relève d'autorités non-étatiques, il devient nécessaire d'organiser l'arrimage entre ces forums qui définissent les règles, les instances du système de santé et les activités se déroulant en réseau. C'est dire à quel point des relais sont nécessaires afin d'assurer les arrimages entre les normativités multiples.

1.3.2 Les relais de la normativité

Les relais sont les différents moyens par lesquels les acteurs d'un environnement en réseau reçoivent et appliquent effectivement les normes perçues par eux comme relevantes ou obligatoires. C'est un mécanisme majeur des processus de gouvernance dans les réseaux.

Les relais peuvent être vus comme une incarnation du concept de co-régulation. Ils résultent d'un processus de dialogue entre les divers pôles de normativité. Ce sont les moyens via lesquels les acteurs peuvent prendre acte, reconnaître les règles qui sont impératives et les relayer, d'en combler les interstices afin d'en assurer une application concrète et effective. Dans le champ du e-gouvernement, les normativités propres à l'appareil gouvernemental constituent d'importants relais des normativités.

L'un des relais majeurs entre les pôles étatiques de normativité et les acteurs des réseaux découle des **régimes de responsabilité**. Pour les acteurs, la responsabilité est source d'incertitude : ceux qui prennent part à des activités le font avec plus ou moins d'intensité selon qu'ils ont ou non conscience qu'ils auront à en supporter la responsabilité. C'est dire l'importance que prennent les mécanismes répartissant les responsabilités entre les acteurs. À ce titre, ils représentent un important relais des normativités susceptibles de s'appliquer à un ensemble d'activités.

Lorsqu'un préjudice est causé à l'occasion d'une activité menée en réseau, que se pose la question de rechercher une sanction et une réparation, la normativité étatique est souvent appelée en renfort. La responsabilité est le lieu où se joue le processus d'articulation entre les valeurs contradictoires que recèlent les droits et libertés. Les régimes de responsabilité contribuent à procurer les différentes hiérarchies et préséances entre les droits fondamentaux.

Du côté de la plupart des acteurs du e-gouvernement, la responsabilité se présente comme un ensemble de risques à gérer. Les personnes et organismes publics doivent s'assurer que leurs pratiques sont conformes aux exigences des dispositions des lois susceptibles de trouver application et d'engager leur responsabilité. Ils chercheront à maîtriser les risques découlant de leurs activités en prenant les précautions susceptibles de garantir qu'elles s'en tiennent uniquement à un rôle compatible avec les responsabilités qu'elles sont prêtes à assumer.

Pour gérer adéquatement les risques, il faut souvent anticiper les conflits et identifier, de façon contextuée, comment seront relayées les exigences issues du droit ou des normativités qui risquent de trouver application. Pour gérer les risques associés aux possibles conflits, il revient aux acteurs d'expliciter leur compréhension des normativités. Les processus d'**autorégulation** et de **co-régulation** sont les principaux relais des normativités encadrant les activités se déroulant

dans le cyberespace. On opère ainsi l'actualisation, l'adaptation et la particularisation des règles considérées comme relevantes à un environnement.

2. Comment les changements techniques modifient le droit?

Les changements techniques ne changent pas le droit de façon directe. Les lois et les décisions de justice ne se modifient pas du seul fait que se manifestent des évolutions techniques. Les changements dans les technologies se situent plutôt en amont : elles modifient les rationalités du droit, c'est-à-dire les perceptions des enjeux, des problèmes, des valeurs, et de ce qui paraît « rationnel » de régir par le droit.

Les technologies contribuent à provoquer la désuétude de certaines règles qui paraissent moins pertinentes; elles contribuent à remettre en cause ce qui fonde les règles de droit, leur légitimité. Les changements techniques entraînent aussi la remise en question des mécanismes par lesquels s'exprime et s'applique le droit c'est-à-dire les techniques de réglementation.

Dans cette section, on explique les relations entre le droit et le changement technologique.

Le droit se justifie par un ensemble de rationalités, c'est-à-dire de raisons, de motifs et de finalités qui rendent « rationnelles » les règles de droit, qui contribuent à en asseoir la légitimité. Par exemple, dans un contexte historique où tous les déplacements se font à pied ou à cheval, il paraît irrationnel de faire des lois prescrivant des limites de vitesse à 100 kilomètres heure!

L'encadrement juridique est tributaire des valeurs, souvent contradictoires, qu'on essaie d'y refléter. Il ne peut être analysé en faisant abstraction de ces valeurs. Connaître les dimensions juridiques d'un phénomène, c'est en bonne partie connaître les raisons qui poussent à l'adoption des règles, qui rendent « rationnelles » les règles adoptées afin d'encadrer le fonctionnement d'un ensemble d'activités. Lorsque les environnements technologiques se modifient, cela peut emporter des changements dans les perceptions de ce qui est bon ou mauvais, de ce qui est possible, nécessaire ou impossible, de ce qui est risqué ou désormais sans conséquences.

Les rationalités ne font pas toujours consensus : elle sont l'objet de débats et connaissent des légitimités variables selon les pays et les époques. Ce phénomène est plus visible avec la généralisation d'Internet et des autres environnements ayant le potentiel de rendre disponibles les informations sans égard à l'espace et même au temps.

Ce qui rend les cadres juridiques obsolètes, ce sont les mutations des rationalités. Les technologies modifient les conditions de la production et de la circulation de l'information. Elles peuvent accentuer les perceptions à l'égard des dangers ou des risques associés à certaines activités. Du coup, cela peut se manifester par une demande de nouvelles règles de droit. Par exemple, la diffusion à la grandeur du réseau des textes des décisions judiciaires peut susciter des inquiétudes qui n'étaient pas pensables lorsque les décisions étaient seulement accessibles dans les dossiers des greffes.

Les décisions des autorités publiques en application des politiques peuvent s'exprimer par plusieurs techniques. Nous appelons « techniques de réglementation » les diverses techniques utilisées par ceux qui veulent imposer des normes de conduite à ceux qui prennent part à une

activité. En adoptant une technique plutôt qu'une autre ou une combinaison de techniques de réglementation, les instances chargées de mettre au point les politiques parviennent à définir et à prévoir les modes d'articulation entre les droits, les obligations et les intérêts des diverses parties impliquées dans une activité. C'est de ce processus qu'émanent les règles de droit ou les autres normes visant à prescrire des comportements aux entreprises ou aux personnes. Or, les évolutions dans les technologies peuvent rendre inefficaces les techniques de réglementation utilisées à ce jour.

Les changements techniques entraînent des modifications dans ce qui est tenu pour « rationnel » de régir par le droit. Les changements peuvent aussi déclasser les méthodes par lesquelles on avait l'habitude d'énoncer et d'appliquer les règles de conduite.

2.1 La « cyberspatialisation » et les mutations du droit

Au regard du droit, la cyberspatialisation[59] est un phénomène multiforme : elle se manifeste au niveau des représentations à l'égard de ce qu'elle permet ou facilite. C'est de ces multiples façons qu'elle contribue à modifier les façons de voir. Les représentations étant modifiées, les dysfonctions pourront paraître amplifiées. Il en va ainsi des règles de droit régissant le déroulement des processus gouvernementaux. Ceux-ci supposent en effet des échanges d'information. Lorsqu'ils ont lieu dans le cyberespace, les enjeux qu'ils posent seront influencés par les caractéristiques associées à la numérisation[60].

Les mutations dans les conditions des échanges d'information ne peuvent manquer d'avoir des effets sur la façon d'envisager le droit. Le droit appréhende les réalités à travers des catégories et des qualifications. Le développement de technologies de l'information engendre des transformations qui remettent en cause les catégories par lesquelles on avait l'habitude de définir leur cadre juridique. Les technologies de l'information changent les façons de faire et peuvent entraîner des modifications dans la perception et les représentations des enjeux et la qualification des situations.

La numérisation et la généralisation des réseaux paraissent avoir une influence de mutation et une influence d'amplification de tendances. On peut parler d'une influence de mutation lorsque les changements induisent une rupture dans les logiques, les façons de faire et les perceptions. On parlera d'une influence d'amplification lorsqu'il n'y a pas de changement radical dans les logiques et les façons de faire mais modification dans la perception des risques ou des enjeux.

L'influence de l'environnement cyberspatial sur le droit paraît s'incarner en des mutations des perceptions sur ce qui est à la portée du droit, de ce qu'il est légitime d'encadrer de même que par l'amplification des enjeux, de leur portée et des conséquences.

---

59 On entend par cette notion le déroulement en tout ou en partie d'activités dans l'espace qui semble découler des connections des environnements informatiques tel que cela se fait par Internet.

60 Pierre TRUDEL, « L'influence d'Internet sur la production du droit », dans Georges CHATILLON (éd.), *Le droit international de l'Internet*, Bruxelles, Bruylant, 2003, 88-101.

2.1.1 Les mutations

Par les changements qu'il induit dans les processus de production et de circulation de l'information, le phénomène de numérisation recèle un important potentiel de mutation sur les fondements de plusieurs règles juridiques. De telles mutations affectent les rationalités sous-tendant les règles encadrant les activités se déroulant en tout ou en partie dans le cyberespace. Elles peuvent aussi affecter l'efficacité des techniques par lesquelles s'appliquent les règles présidant au déroulement des processus décisionnels en général et des processus délibératifs en particulier.

La numérisation contribue à modifier les représentations des acteurs et des décideurs au sujet des réalités auxquelles il importe de faire face au moyen du droit. Les changements dans les conditions de production et de circulation de l'information modifient les représentations à partir desquelles se pensent les cadres juridiques. Ces changements se manifestent de façon différente au sein des divers systèmes juridiques. Ils affectent les perceptions et les points de vue au sujet de ce qui fonde l'intervention du droit, sur ce qui est à la portée de son champ d'intervention ou ce qui paraît lui échapper.

La façon dont le droit est compris et appliqué est en partie tributaire du médium par lequel il est communiqué. L'on considère que la place prise par les précédents dans le Common Law s'explique en grande partie par la disponibilité de textes imprimés. Avant que soient disponibles des publications imprimées des jugements, le rôle des précédents y était beaucoup moins manifeste.[61] On peut pareillement constater à quel point la diffusion de certaines décisions et pas d'autres peut influer sur la connaissance et la compréhension du droit qui peut prévaloir dans un milieu juridique donné.

Dans l'univers de l'écrit et de l'imprimé, il était relativement facile de départager les différents usages auxquels pouvait être vouée l'information. Internet modifie les conditions de la production et de la circulation de l'information. La numérisation a pour conséquence de rendre l'information disponible sur des supports susceptibles de servir à différentes finalités. La numérisation permet de fédérer les différentes fonctions de l'information jusqu'à tout récemment accomplies par des acteurs différents. Les différents médias ou environnements d'information sont aussi, du fait de la convergence technologique, fédérés en des lieux interchangeables.

Les changements dans les processus de production et de transmission de l'information engendrent des mutations dans les fondements du droit. Il en résulte que certaines règles paraissent devenir obsolètes soit qu'elles n'ont plus de raison d'être soit que leur efficacité est mise en doute.

2.1.2 L'amplification des dysfonctions du droit

Les changements dans les conditions techniques des échanges d'information se manifestent par l'amplification des problèmes ou des contradictions qu'ils semblent induire. Marie-Anne Frison-

61 Ethan KATSH, *The Electronic Media and the Transformation of Law*, New York, Oxford University Press, 1989.

Roche observe qu'Internet : « provoque une sorte d'hypertrophie des règles : les conseils deviennent hyperboliques. Ainsi, le principe de prudence comme celui d'information est formulé avec superlatif. Le client doit être particulièrement prudent. Le professionnel doit plus encore veiller à la bonne information de son client. On retrouve ici l'idée que, Internet ne faisant qu'accroître les phénomènes, la réponse juridique est dans l'amplification de ses prescriptions.[62] » C'est ainsi que l'on a vu des recommandations de redoubler de précautions. Devant la difficulté de prévoir les conséquences juridiques de faits et gestes ou de contrats intervenus sur Internet, certains en viennent même à recommander de se ménager des preuves sur support-papier!

Ce type de problèmes que l'on observe de plus en plus lorsqu'on entreprend la diffusion massive de certains corpus indique qu'Internet aurait un effet d'amplification des limites et des dysfonctions du droit.

Les problèmes paraissent amplifiés du fait du passage aux environnements en réseaux. Souvent c'est en réclamant une amplification des protections juridiques sans pour autant questionner les fondements de celles-ci que l'on tente d'ajuster le droit aux réalités inédites.

Toutefois, ce n'est pas nécessairement en persistant dans les paradigmes des règles existantes que l'on parvient à maîtriser effectivement les périls aux dimensions nouvelles qui accompagneraient l'émergence de l'État en réseau. Il faut souvent revoir les raisons qui justifiaient les règles de droit et surtout les moyens par lesquels ces dernières sont exprimées et appliquées.

2.2 Le droit de l'État post-moderne

Les phénomènes associés au e-gouvernement et au Web 2.0 se manifestent dans le contexte de l'État post-moderne. Ils sont plus rarement rencontrés dans les contextes hiérarchisés et plus formalisés du droit et de l'État moderne.

Lorsqu'il est question d'état et de droit post-moderne, on renvoie aux évolutions qui caractérisent l'État moderne. L'État moderne se caractérise en effet par un pouvoir institutionnalisé s'inscrivant dans un cadre général et collectif dépassant la personnalité contingente de ses détenteurs. La citoyenneté y est entendue comme un rapport exclusif, incompatible avec l'existence d'allégeances parallèles ou concurrentes; l'État possédant le monopole de la contrainte, censé dans l'espace de ses frontières exercer la pleine souveraineté, constituer l'unique source du droit. Cette notion de la modernité appliquée au droit et à l'État fait conclure que « Par tous ces éléments, la construction de l'État apparaît bien comme indissociable d'une modernité, dont elle est à la fois le reflet et le vecteur »[63]. La logique de la modernité est caractérisée par l'empire de la raison. Elle envisage l'État comme un artefact doté de la puissance souveraine expression de la puissance collective détenue par les citoyens. Plusieurs signes donnent à croire que les sociétés contemporaines sont entrées dans une logique nouvelle résumée

62 Jean-Marie CHEVALIER, Ivar EKELAND, Marie-Anne FRISON-ROCHE et Michel KALIKA, *Internet et nos fondamentaux*, Paris, PUF, 2000, p. 41-42.

63 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 17.

et condensée par le concept de post-modernité[64]. Chevallier observe que « l'État post-moderne est un État dont les traits restent précisément, et en tant que tel, marqués par l'incertitude, la complexité, l'indétermination; et ces éléments doivent être considérés comme des éléments structurels, constitutifs de l'État contemporain. »

Le passage à l'État post-moderne « implique une redéfinition de la nature du lien politique, c'est-à-dire du rapport entre gouvernants et gouvernés »[65]. Pour Chevallier :

> *Dès lors, les changements qui affectent la structure étatique doivent être rapportés à des évolutions plus globales qui affectent le politique : de même que l'État absolutiste est le reflet de la conception absolutiste de l'autorité du monarque sur ses sujets, l'État libéral s'appuie sur la représentation d'un pouvoir procédant de la volonté des citoyens et l'État-providence présuppose la vision d'un pouvoir préposé à la satisfaction des aspirations collectives; aussi le changement de la configuration étatique doit-elle être considéré comme le révélateur d'une réévaluation en profondeur de la logique démocratique*.[66]

L'évaluation de l'influence des environnements techniques sur le droit procède nécessairement d'une prise en considération des traits que présente le droit postmoderne. Dans cette section, on constate qu'il y a des changements importants dans la morphologie du droit ainsi qu'à l'égard de la place qu'il occupe. Ces changements ne résultent pas uniquement de la généralisation des technologies de l'information mais coïncident avec ce phénomène.

Les technologies de l'information tendent à s'inscrire et accentuer les mutations caractéristiques que connaît le droit de la modernité. Sans doute les mutations que connaît le droit ne résultent pas uniquement des changements dans les techniques de communication mais il paraît y avoir une grande coïncidence entre les mutations que les techniques connaissent et celles qui affectent l'État et le droit. Le passage d'un État et d'un droit moderne à un État et un droit post-moderne permet de saisir les mutations qui découlent des évolutions que connaît le contexte socio-technique et surtout, les impacts que cela peut avoir sur le droit, la place qu'il tient, sa morphologie et ses conditions de fonctionnement.

Les phénomènes de crise de l'architecture étatique, de la mondialisation, de droit en réseau sont au nombre de ceux qui prennent une importance renouvelée dans le contexte des services en ligne et du Web 2.0.

- On parle de la **crise de l'architecture étatique**[67] . Le modèle étatique hérité de la modernité est mis à mal dans les sociétés post-modernes. Il y a une réévaluation de la place de l'État. La crise de l'État providence paraît emblématique de cette tendance. Selon Jacques Chevallier, cette crise s'est développée en deux temps. Premièrement au niveau des représentations : à compter des années soixante-dix, il y a une érosion du système de représentation sur lequel

64 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 19.

65 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 139.

66 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 139.

67 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 21.

l'état avait pourtant bâti sa légitimité. Le thème de l'inefficacité de l'État porte plusieurs des remises en cause d'un modèle présenté de plus en plus comme interventionniste, déréglant les mécanismes du marché et limitant l'initiative. Mais c'est au niveau de la crise des politiques que la crise paraît plus importante. Dans la décennie 1980, se succèderont un ensemble de politiques visant à mettre un frein au processus de croissance étatique.

- La dynamique de la **mondialisation** tend aussi à affecter la capacité des instances nationales ou territoriales d'exercer une juridiction effective sur plusieurs phénomènes. Avec le passage à la société de l'information, il devient difficile contrôler les flux d'information. L'impossibilité de contrôler la circulation de ces flux d'information ne peut manquer de saper, non seulement les principes d'organisation traditionnels, à base de hiérarchie et de centralisation, mais encore les fondements mêmes de l'institution.[68]

- Les instances établies par les États sont de plus en plus concurrencées par d'autres entités productrices de normativités ou capables de gérer des conflits. Les opérateurs économiques, les ONG agissant localement ou dans des réseaux agissant suivant des logiques supra-nationales, s'engagent de plus en plus dans les processus de détermination des règles de régulation et de résolution des conflits. Les médias tendent de plus en plus à mobiliser une partie du pouvoir qu'ils sont en mesure d'exercer. À tel point qu'ils peuvent finir par être perçus comme des alternatives aux tribunaux afin de rétablir des équilibres ou réparer certains torts.

- Ces phénomènes contribuent à brouiller les repères spatio-temporels, atténuant la spécificité étatique et contribuant à la banalisation de plusieurs institutions publiques[69]. Ce dernier tend à devenir une entité parmi d'autres. Pour assurer l'application de ses normativités, il a de plus en plus l'obligation d'en démontrer le bien-fondé et l'efficacité.

- Dans le cyberespace[70], la normativité s'élabore de plus en plus dans les **réseaux**. Les réseaux sont le résultat d'interactions répétées entre personnes poursuivant un but commun. L'« internetisation » s'accompagne de l'émergence de réseaux unissant les décideurs, les chercheurs, les régulateurs de même que les autres acteurs jouant un rôle dans la normativité d'Internet.

- La technologie et les contraintes qu'elle induit est aussi source de normativité dans le cyberespace[71].

---

68 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 31.

69 Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2003, p. 65.

70 Pierre TRUDEL, « Quel droit et quelle régulation dans le cyberespace ?» *Sociologie et sociétés, vol. 32, no 2, automne 2000,* 189-209. < http://www.erudit.org/erudit/socsoc/v32n02/trudel/trudel.pdf >

71 Pierre TRUDEL, « L'architecture technique comme élément régulateur du cyberespace », [2000] *Media Lex* 187; Pierre TRUDEL, « La Lex Electronica », dans Charles-Albert MORAND (dir.), *Le droit saisi par la mondialisation*, Bruxelles, Éditions Bruylant, collection Droit international, 2001, pp. 221-268.

- Dans une société de réseaux, les normes sont pensées, élaborées et appliquées au sein de plusieurs pôles interagissants. Les problèmes et enjeux auxquels répondent les mesures étatiques, de même que les autres normativités, sont débattus et mis au jour dans plusieurs lieux. Ces lieux sont en dialogue : chacun peut, à un moment où l'autre, se trouver en situation de proposer une signification à un principe ou une mesure. Il peut arriver que les principes constitutionnels soient invoqués au soutien ou à l'encontre d'une mesure débattue. L'application du droit se déroulant de plus en plus dans un univers à pôles multiples et inter reliés, il en résulte une plus grande richesse dans les échanges et possiblement des règles mieux adaptées aux besoins de la société. Les processus délibératifs se déroulent de plus en plus suivant le modèle des réseaux plutôt qu'en pyramide[72].

- L'apparition d'un socle de valeurs souvent exprimées sous la forme de principes directeurs. Ces principes directeurs, exprimés en termes généraux et de manière à être admis en principe par tous sont ensuite relayés dans le système juridique. Une illustration de phénomène est fournie par l'importance que prennent les droits fondamentaux. Tous sont en principe en faveur des droits fondamentaux : mais c'est souvent au niveau des conséquences pratiques de ces derniers que se rompent les consensus. Par exemple, il y a un va-et-vient entre les principes constitutionnels, les lois et les décisions qui sont prises en leur nom. Énoncés, dans un texte constitutionnel, les principes deviennent autant d'arguments, de justifications, de légitimations pour préconiser des lois ou appuyer des décisions. Mais en retour, ces mesures mises en place dans le déroulement de la vie sociale influent sur le sens des principes constitutionnels et sur les dialogues entre les différents pôles qui prennent part à l'application et à l'interprétation des règles.

- Dans les sociétés post-modernes, les principes et les droits n'ont pas un sens univoque. Le sens de la plupart des droits est déterminé, dans un contexte donné et dans le cadre de processus délibératifs. Les principes fondamentaux d'une politique, les droits et libertés ont beau connaître leur sens immédiatement obligatoire dans le système juridique, d'autres systèmes contribuent à dégager le sens des règles et des droits. La généralisation des espaces en réseaux accentue le constat de Philippe Jestaz selon lequel « le droit avec son réseau serré de règles et d'institutions, est un système compact, de surcroît imbriqué avec d'autres systèmes sociaux »[73]. Parmi ces systèmes sociaux qui participent à la construction du sens des règles et principes, il y a le système politique, les institutions politiques et juridiques, les mœurs, les usages... le juge. Dans ce cadre, il existe une pluralité de communautés d'interprétation au sein desquelles se dégage le sens des principes constitutionnels, des droits et libertés, qui génère les repères permettant de résoudre les contradictions. Le sens des règles se discute et se définit aussi dans les systèmes plus diffus, la morale, l'idéologie, les croyances communes ou communément admises. Le réseau génère lui aussi ses référents culturels, ses mythes, des croyances, ses coutumes.

---

72 François OST et Michel van de KERCHOVE, *De la pyramide au réseau? Pour une théorie dialectique du droit*, Bruxelles, Publications des Facultés universitaires Saint-Louis, 2002.

73 Philippe JESTAZ, *Le droit*, 4e édition, Paris, Dalloz, coll. Connaissance du droit, p. 25.

Les conséquences de la numérisation sont démultipliées par l'hypertextualisation caractéristique des environnements-réseaux constitués par Internet ou les supports multimédias. Cela permet de mobiliser un important potentiel de synergie entre les différents lieux dans lesquels se discute et s'applique le droit.

L'environnement-réseau induit une certaine instabilité de la règle de droit. L'écrit n'est plus fixé dans l'imprimé. L'information paraît de plus en plus fluide et en continuel ré-ajustement et actualisation. Le droit se présente de plus en plus comme une résultante continuellement provisoire d'un ensemble de décisions emportant des conséquences normatives. D'où une mutation allant dans le sens d'un élargissement des sources jugées pertinentes lors de la prise de décision.

En somme, dans l'État postmoderne, les processus sont moins centralisés. Ils se déploient de plus en plus en réseaux plutôt qu'en pyramide. Les réseaux ont des frontières fluctuantes. Le droit - constitué de principes généraux se confondant souvent avec les valeurs largement admises - est exprimé dans des pôles de normativité en concurrence les uns avec les autres. Les principes généraux connaissent des significations variables selon les divers lieux et parties du réseau où la normativité est déployée et relayée. En fin de compte, il est de plus en plus difficile de concevoir les règles menant aux décisions collectives comme prescrivant un processus par lequel une autorité répond à une question et en impose la réponse.

Au nombre des sources qui pourront être sollicitées lors du déroulement des processus décisionnels, il y a les acteurs impliqués, les clientèles ou leurs représentants. On trouvera souvent opportun de mettre en œuvre des mécanismes formels et informels afin de mesurer les enjeux et prendre en compte la diversité des intérêts. Souvent, s'instaure un processus de régulation dans le cadre duquel les parties impliquées en viennent à négocier l'application concrète des règles formelles. Par exemple, le respect de plusieurs droits fondamentaux requiert la mise en place d'accommodements raisonnables qui pourront être identifiés à l'issue d'un processus de négociation impliquant l'ensemble des parties concernées.

3. Les obligations selon le cycle de vie des documents

L'administration électronique suppose la circulation accrue d'informations. La circulation de l'information se présente comme une donnée majeure du contexte dans lequel se déploie le gouvernement en ligne. L'information qui circule est de l'information qui se déplace, qui va d'un lieu à l'autre. Et de fait, l'avènement des services en ligne nécessite la circulation accrue de l'information. La circulation et le partage des informations permettent d'améliorer la qualité et la célérité des prestations. Or, dans les environnements en réseaux, la circulation des informations s'effectue par le déplacement de « documents ».

3.1 La notion de « document »

Le droit québécois dispose d'une définition générique de la notion de « document ». En vertu de l'article 3 de la *Loi concernant le cadre juridique des technologies de l'information*, les documents technologiques sont des documents dont le support fait appel aux technologies de l'information. La disposition se lit ainsi :

> ***3.*** *Un document est constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.*
>
> *Pour l'application de la présente loi, est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.*
>
> *Un dossier peut être composé d'un ou de plusieurs documents.*
>
> *Les documents sur des supports faisant appel aux technologies de l'information visées au paragraphe 2° de l'article 1 sont qualifiés dans la présente loi de documents technologiques.*

La loi est construite à partir de la notion de document car c'est l'élément commun entre l'univers du papier et celui des technologies de l'information. Afin de mettre en place un environnement juridique qui pourra s'appliquer quelles que soient les technologies utilisées, on a retenu une définition générique de la notion de document. Cette notion est en effet l'élément commun au monde papier et à celui des technologies de l'information.

Lorsque l'information circule, elle passe d'un lieu à l'autre. Ces passages d'un lieu à l'autre s'effectuent selon des phases différentes. Mais dans le processus de circulation, l'information peut venir en possession d'une entité, voire d'une personne sans être connue de ceux-ci. C'est que la circulation de l'information nécessite qu'elle passe entre les mains d'entités qui n'ont que la charge de l'acheminer ou de l'entreposer dans le cadre d'un processus d'acheminement. Dans un réseau, l'information qui circule n'est pas nécessairement sous l'entier contrôle de l'entité qui se trouve à avoir la possession physique du support.

3.2 Le cycle de vie des documents

La circulation de l'information se présente comme un processus au cours duquel l'information passe entre diverses mains. Ce processus doit être sécurisé de bout en bout. Mais au plan du degré de maîtrise juridique, du contrôle de l'information, la circulation comporte des épisodes différents. Typiquement, une information est créée, puis transmise à une âtre personne qui en reçoit communication. La circulation de l'information s'effectuera selon des phases au cours desquelles on peut reconnaître la transmission via un transmetteur, l'entreposage dans un répertoire mettant le message à la disposition de son destinataire et enfin, la communication au destinataire, lorsque celui-ci prend contrôle et connaissance du message.

On peut considérer que les principaux épisodes du cycle de vie d'un document sont :

- La création
- La modification
- La communication

- Le transfert de l'information
- La consultation
- La transmission
- La conservation
- L'archivage ou destruction

La *Loi concernant le cadre juridique des technologies de l'information* prescrit les obligations incombant aux personnes qui sont responsables de documents lors des différents épisodes de leur cycle de vie. Par exemple, afin qu'il puisse conserver sa valeur juridique, l'intégrité du document doit être maintenue durant tout son cycle de vie[74]. La *Loi* prévoit ainsi les objectifs à atteindre et les mesures à prendre, afin d'assurer le maintien de l'intégrité du document tout au long de son cycle de vie. C'est-à-dire, lors du transfert de l'information vers un autre support, lors de la conservation du document, lors de sa consultation et lors de sa transmission.

La *Loi* impose également des obligations quant à la protection des renseignements personnels et confidentiels à chaque phase du cycle de vie du document, notamment lors de sa conservation, lors de sa consultation et lors de sa transmission. En matière de consultation, elle renforce le droit d'accès aux documents. Enfin, la *Loi* pose les principes de la responsabilité des différents prestataires de services qui prennent part à la conservation, à l'archivage ou à la communication des documents.

3.3 Les rôles des entités en réseau à l'égard des documents qui circulent

Dans les réseaux, il y a des entités qui contrôlent l'information, peuvent y accéder et les communiquer à d'autres tandis qu'il y a des entités qui assurent des fonctions d'intermédiaires, assurant le traitement des informations sans pour autant avoir le contrôle sur celles-ci.

La personne qui exerce le contrôle sur un document ou se comporte de manière à exercer un contrôle sur la diffusion de celui-ci en assume la responsabilité. Ainsi, mettre des informations en ligne, c'est assumer une fonction éditoriale. L'éditeur publie les informations. Publier signifie communiquer de l'information à des tiers en sachant que cette information sera lue, vue ou entendue. La publication s'effectuant de manière volontaire suppose une connaissance de la teneur de l'information transmise[75]. Dans le contexte d'Internet, la publication peut résulter de la transmission de fichiers, de discussions dans le cadre de conférences électroniques, de l'envoi d'un courriel à un nombre indéterminé de personnes ou encore par la mise à disposition d'information dans des fichiers de documents pouvant être transférés via le réseau. Dans l'échange de personne à personne, la personne qui exerce un contrôle sur une information peut la

---

74 Article 6, alinéa 2.

75 Pierre TRUDEL, «Responsibilities in the Context of the Global Information Infrastructure», [1997] 29 *International Information & Library Review*, 479-482.

Loftus E. BECKER Jr., « The Liability of Computer Bulletin Board Operators for Defamation Posted by Others », (1989) 22 *Connecticut Law Review* 203-239, 217.

communiquer ou accorder différentes permissions à l'égard de cette information. Or, dans le contexte du Web 2.0, la personne qui exerce le contrôle d'un document peut-être un client, un organisme ou un tiers.

L'exercice du contrôle à l'égard de la diffusion d'une information s'assimile à l'exercice de la fonction éditoriale. Celle-ci implique le pouvoir de choisir ce qui sera diffusé, de décider de le diffuser et de décider à qui ou auprès de qui l'information sera diffusée. Ainsi, un fournisseur d'accès Internet qui examinerait tous les messages avant de les retransmettre et se réserverait le droit de n'acheminer que les messages qu'il juge conformes à ses politiques, se comporterait comme un éditeur. Dans de pareilles situations, il est une constante : la décision de publier appartient à l'éditeur. Il s'agit pour lui d'une faculté : il n'a pas d'obligation de publier. Dans le monde de la presse et de l'édition, il est usuel de tenir que le directeur de publication est en mesure de contrôler les informations qui circulent du fait de son entreprise[76]. De ce pouvoir de contrôle découle la responsabilité pour la transmission d'informations.

Dans le contexte des réseaux comme Internet, les intermédiaires sont des personnes, entreprises ou organismes qui interviennent dans l'accomplissement d'une tâche effectuée entre le point d'expédition d'une transmission de document et le point de réception final. Le trait commun à tous ces intervenants, c'est qu'ils n'exercent pas de droit de regard sur l'information qui transite dans leurs environnements technologiques. Ainsi, les intermédiaires peuvent être des services de conservation de documents technologiques[77], des hébergeurs, des services de référence à des documents technologiques, des moteurs de recherche, des fournisseurs de services sur un réseau de communication. Il peut également s'agir d'entreprises offrant des services de conservation ou de transmission de documents technologiques, de services de transmission de documents technologiques ou de services de conservation sur un réseau de communication de documents technologiques fournis par un client.

Le statut des intermédiaires varie à l'infini. Sur Internet, une entité peut accomplir une ou plusieurs des fonctions nécessaires à la communication ou à la transmission d'informations. Les désignations que se donnent les acteurs telles que « fournisseur d'accès à Internet », fournisseur de connectivité, simple transporteur ne recouvrent pas toujours les mêmes activités. Il faut donc, pour chaque situation, examiner soigneusement ce que fait l'intermédiaire visé afin de le qualifier adéquatement au plan de la responsabilité qu'il assume.

Par exemple, certains services communs mis en place par les gouvernements tiennent un rôle d'intermédiaires. Ils prennent part au traitement des informations qui circulent dans les réseaux ou qui y sont déposé sans avoir, en principe, la maîtrise, le contrôle de celles-ci.

---

76 Pierre TRUDEL, « Liability in Cyberspace », in Theresa FUENTES-CAMACHO, *The International Dimensions of Cyberspace Law*, Aldershot Ashgate Publishing, UNESCO, 2000, p. 189-211. David R. JOHNSON et Kevin A. MARKS, « Mapping Electronic Data Communications onto Existing Legal Metaphors : Should We Let Our Conscience (and Our Contracts) be Our Guide? », (1993) 38 *Vill. L. Rev.* 487, 492.

77 Selon l'article 3 de la *Loi concernant le cadre juridique des technologies de l'information*, les documents technologiques sont des documents dont le support fait appel aux technologies de l'information.

3.3.1 Le contrôle de l'information

Pour être tenu à des obligations en matière de renseignements personnels, il faut être en position de contrôle à l'égard des documents qui comportent de tels renseignements. Cela est évident dans le monde des dossiers consignés uniquement sur support papier. Il en va de même pour les documents technologiques, ceux qui sont sur des supports faisant appel aux technologies de l'information.

Dans son sens premier, contrôler, c'est exercer un rôle et avoir une capacité de surveillance, de vérification. Contrôler, c'est maîtriser.

Contrôler l'information, c'est exercer à son égard, les prérogatives qui autorisent à s'approprier les attributs qu'elle comporte. Par exemple, celui qui, dans un environnement en ligne reçoit un vidéo qu'il télécharge et lit au moyen d'un logiciel approprié dispose d'un contrôle sur l'information.

Le contrôle d'une information implique un pouvoir d'en prendre connaissance. C'est pouvoir l'utiliser pour des fins déterminées ou pour des fins indéterminées. Par exemple, la propriété intellectuelle peut limiter le droit de reproduire, communiquer au public Dans le contexte de secret, c'est avoir l'obligation d'en assurer la confidentialité en dehors du secret, c'est pouvoir la transmettre à d'autres.

Le contrôle de l'information peut être un contrôle *de facto* : une personne obtient un fichier, le reproduit et le diffuse à d'autres sans détenir les autorisation aux termes des lois sur le droit d'auteur ou sur la protection des renseignements personnels.

Mais le contrôle de l'information peut être *de jure* : une personne dispose d'un droit exclusif d'interdire la diffusion d'un fichier.

Dans un réseau, une personne peut momentanément être en contrôle d'une information de facto sans l'être au regard du droit : j'obtiens par des manœuvres illicites, la photo d'une personne et décide de la diffuser sur des sites de réseautage social sans avoir demandé la permission.

C'est dans le cadre de ces catégories qu'il est utile d'aborde la signification des notions du droit de la protection de l'information personnelle dans le contexte des réseaux. Cela permettra de mieux situer le sens de notions de communication, collecte, transmission, conservation et autres éléments du cycle de circulation des renseignements personnels.

Les obligations de ceux qui n'ont pas le contrôle de l'information

Les entités qui n'ont pas le contrôle effectif de l'information peuvent avoir certains devoirs. Ainsi, l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*[78] dispose que :

---

[78] L.R.Q. c. C-1.1, disponible à http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html.

> *« **25.** 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. »*

Des obligations incombent aux prestataires qui n'ont pas comme tel le contrôle de l'information qui est entre leurs mains; toutefois, ces obligations ne sont pas les mêmes que celles auxquelles sont tenus les entités qui ont effectivement le contrôle sur des documents technologiques. Ainsi, les entités qui ne font que détenir physiquement des documents n'ont pas nécessairement le droit d'en prendre connaissance à moins que les documents comportent des informations qui sont publiques par nature. L'article 26 de la Loi concernant le cadre juridique des technologies de l'information[79] fait obligation à quiconque qui confie le document à un prestataire de services pour en assurer la garde d'informer ce dernier de la protection que requiert le document. Il lui faut donner des informations adéquates sur les mesures de protection de la confidentialité que le document nécessite. Il faut pareillement indiquer quelles sont les personnes habilitées à en prendre connaissance. De son côté, le prestataire de services doit faire en sorte que les moyens technologiques convenus d'un commun accord avec la personne qui lui a confié le document soient mis en place durant toute la période pendant laquelle il en la garde.

Ainsi, il est tenu, durant la période où il en a la garde, de voir à ce que les moyens technologiques soient mis en place pour en assurer la sécurité en préserver l'intégrité et le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Au surplus, le prestataire a l'obligation de respecter toute autre obligation prévue dans une loi relativement à la conservation d'un document.

Aux termes de l'article 27 de la *Loi concernant le cadre juridique des technologies de l'information*[80], l'intermédiaire qui fournit des services sur un réseau de communication ou qui y conserve ou y transporte des documents technologiques n'est pas tenu d'en surveiller l'information. Par contre, il 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, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions.

Ces dispositions qui explicitent les obligations incombant aux intermédiaires sur un réseau font bien voir que ceux-ci ne sont pas dans une position où ils exercent un contrôle sur les documents technologiques qui viennent en leur possession physique. Il ne viendrait pas à l'esprit de considérer que le facteur ou l'entreposeur de courrier dans le monde du support papier dispose du

---

79 L.R.Q. c. C-1.1, disponible à http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html.

80 L.R.Q. c. C-1.1, disponible à http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html.

contrôle sur l'information contenue dans les lettres entreposées : la situations des intermédiaires est fonctionnellement analogue.

Pour déterminer les rôles, droits et devoirs des divers acteurs qui prennent part à la transmission d'une information dans un réseau, il faut examiner sa relation avec le support de même qu'avec le contenu du message transmis[81]. Ce critère de contrôle serait même un pré-requis à l'imputation de toute responsabilité, y compris celle qui découle du traitement de renseignements personnels. Henry H. Perritt explique en effet que:

> *In all three categories of tort liability (defamation, copyright infringement and invasion of privacy), the requisite fault cannot be proven without showing either that the actor and potential tort feasor exercised some actual control over content or that it was feasible for it to control content and that it could foresee the possibility of harm if it did not control content*. [82]

L'objet et la portée des droits et responsabilités des différents acteurs qui interviennent dans la communication électronique tient au degré de contrôle et de maîtrise qu'ils exercent ou qu'ils sont réputés exercer sur l'information et les communications qui se déroulent dans les réseaux. L'imputation de la responsabilité à une entité suppose la possibilité d'identifier les acteurs qui ont la maîtrise de l'information dans les divers lieux de cet environnement virtuel.[83] Dès 1993, Eric Schlachter écrivait à cet égard que:

> *There is a sliding scale of control in relation to forced access. At one end of the scale are primary publishers, who have virtually unrestrained discretion over what they print or to whom they give access to disseminate information. Also on this end are owners of private property, who are similarly protected from mandatory or forced access. (...) At the other end of the sliding scale from primary publishers are common carriers who by definition must be available to all comers and cannot refuse to provide service in a discriminatory fashion*.[84]

Cette échelle mobile concerne aussi bien les droits d'accès aux informations que l'ensemble des autres relations qui peuvent exister entre un acteur donné et l'information qui transite dans un réseau. C'est à partir de ce constat que la doctrine et les tribunaux ont développé les principes relatifs à la responsabilité des acteurs dans un réseau. C'est à ces principes qu'il faut se référer lorsque vient le temps de départager la nature et l'intensité des obligations à l'égard des

---

81 Pierre TRUDEL, « Liability in Cyberspace » dans Theresa FUENTES-CAMACHO, *The International Dimensions of Cyberspace Law,* UNESCO Press et Ashgate Publishing, 2000, 189-211.

82 Henry H. PERRITT JR., «Tort Liability, the First Amendment and Equal Access to Electronic Networks», (1992) 5 *Harvard J. of L. & Tech*. 65, 110-111.

83 Voir Pierre TRUDEL, «La protection des droits et des valeurs dans la gestion des réseaux ouverts», dans CRDP, *Les autoroutes électroniques : usages, droit et promesses*, Montréal, Éditions Yvon Blais, 1995, pp. 324 et 325.

84 Eric SCHLACHTER, «Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Board Functions», (1993) 16 *Hastings Comm/Ent L.J*., 113 et ss.

renseignements personnels. Schlachter relève à cet égard que «Those entities with more editorial control generally also have greater exposure to tort liability for the statements or actions of others. »[85] Le contrôle éditorial dont parle ici Schlachter doit être entendu en son sens générique : celui du contrôle sur l'information, c'est à dire l'exercice à l'égard de celle-ci des divers pouvoirs qui sont possibles. Par exemple, lorsque je donne un renseignement me concernant, j'exerce une fonction de contrôle à l'égard de cette information. Ainsi, il est donc possible de caractériser l'intensité de la responsabilité à partir de l'intensité du contrôle qu'une personne exerce effectivement sur l'information dans une situation déterminée.

C'est d'ailleurs en tenant compte de l'intensité du contrôle exercé sur un document que fut développé le cadre juridique présidant à la détermination des droits et des responsabilités relatives aux informations circulant dans les réseaux. Plus on a le contrôle sur un document, plus on en répond.

3.3.2 L'intensité du contrôle

Dans un réseau, tout comme dans le monde physique, l'information voyage entre les mains d'une pluralité de prestataires qui, tout en contribuant à déplacer l'information n'acquièrent sur celle-ci qu'un contrôle strictement physique : le postier qui livre une lettre à certes le contrôle physique sur celle-ci pendant le déroulement de ses opérations de livraison, il n'a aucun contrôle qui lui permettrait de prendre connaissance des renseignements qu'elle contient.

Pour rendre compte du régime juridique applicable à la protection des renseignements personnels dans un réseau et calibrer de façon adéquate les droits et les obligations de ceux qui interviennent dans les diverses opérations de traitement de ces documents technologiques, il est nécessaire de caractériser plus précisément les types de maîtrise et de contrôles qui sont exercés sur les documents.

Au Québec, la *Loi concernant le cadre juridique des technologies de l'information* énonce les principes qui permettent de mieux qualifier les différents participants à des activités de communication en ligne. Ainsi, le prestataire visé à l'article 22**,** celui qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci.

Ce principe a un caractère général : il marque la distinction entre le prestataire qui exerce le contrôle sur un document et l'intermédiaire qui, bien que pouvant se trouver en possession du document n'a pas de contrôle sur celui-ci. Le second alinéa de l'article 22 explicite le processus par lequel le prestataire peut engager sa responsabilité. L'article 22 pose qu' « il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent

---

85 Eric SCHLACHTER, «Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Board Functions», (1993) 16 Hastings Comm/Ent L.J., 113 et ss.

apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité. » Ce principe aide à déterminer à quel moment naît une obligation de se comporter à l'égard d'un document comme si on en avait acquis le contrôle.

S'agissant du prestataire visé à l'article 22, la connaissance est la condition nécessaire afin que naissent pour lui des obligations à l'égard de l'information qu'il conserve. Par exemple, aux termes de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information,* le prestataire qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier. Ainsi, lorsque le prestataire-intermédiaire propose une plateforme dans laquelle il est loisible aux usagers de déposer des informations afin que celles-ci soient rendues disponibles à des tiers, le prestataire qui offre de tels services de conservation n'acquiert pas le contrôle sur les documents ainsi traités. Ces documents ne lui sont pas communiqués : ils sont rendus publics par l'usager qui choisit de le faire via la plateforme. C'est l'usager qui contrôle les documents et décide de les transmettre à un tiers.

Plusieurs cas de figure découlent s'envisagent dans une telle situation. Un usager peut utiliser une plateforme de conservation de documents technologiques pour communiquer avec un prestataire afin que celui-ci lui fournisse des renseignements. Par exemple, l'usager peut exercer son droit d'accéder à ses renseignements personnels à partir d'une plateforme. Il appelle donc à lui ses renseignements qu'il conserve dans le répertoire offert par le prestataire de services de conservation. Là encore ce prestataire n'a pas eu communication des documents.

Certaines plateformes peuvent servir à la réalisation d'une opération préalable à la réalisation d'une transaction. Par exemple, afin de s'identifier auprès d'un prestataire de services gouvernementaux, un usager pourra choisir d'accéder à ses renseignements personnels détenus par un organisme public à partir de la plateforme du prestataire de services de conservation. Ayant reçu ses renseignements, l'usager pourra décider de les acheminer à un autre organisme public. Dans un tel schéma, l'intermédiaire n'a pas reçu communication des renseignements personnels traités par l'usager. C'est plutôt l'usager qui a reçu communication des renseignements. Par la suite, l'usager a décidé de communiquer ces renseignements à un autre organisme. La communication a été faite uniquement à l'organisme auquel l'usager à transmis ses renseignements personnels.

La principe énoncé à l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information* pose que le prestataire qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier. Nous sommes ici dans des situations où le prestataire-intermédiaire n'a aucunement connaissance de ces informations. Il n'a pas vocation à avoir connaissance des ces documents ni en fait ni en droit. Certes, il est techniquement possible pour ce prestataire de prendre connaissance du document et s'il le fait, il pourra devoir en être responsable. Mais comment peut-on le rendre responsable tant qu'il ne prend pas connaissance du document?

Ces situations sont fonctionnellement équivalentes aux dépôts de conservation de documents.

La situation est la même à l'égard de la responsabilité de l'intermédiaire passif qui transporte les documents technologiques tel que l'intermédiaire visé à l'article 36 de la *Loi concernant le cadre juridique des technologies de l'information*[86] n'agit que comme transmetteur. Cet intermédiaire n'est pas, en principe, responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité. Mais il peut engager sa responsabilité dans les situations mentionnées à l'article 36.

Lorsque le prestataire a un contrôle accru sur le document, sa responsabilité à l'égard du document augmente. Ainsi, le prestataire qui est à l'origine de la transmission du document est en quelque sorte considéré avoir lui-même décidé de le transmettre. Alors, il n'est plus vraiment un intermédiaire passif. Il joue un rôle actif dans la décision de transmettre, ce qui est de la nature de l'exercice d'un contrôle sur la teneur du document.

Le prestataire qui sélectionne ou modifie l'information du document exerce une fonction éditoriale. Il devient la personne qui prend la décision de formuler ou de faire circuler un document. Il est alors considéré avoir participé à la décision de produire le document dans l'état où il est. Du coup, il en répond.

Le prestataire qui sélectionne la personne qui transmet le document, qui le reçoit ou qui y a accès fait plus que simplement le transmettre. Il décide des personnes qui transmettent, reçoivent ou peuvent accéder à un document. Le prestataire qui sélectionne la personne qui transmet décide lui-même de la transmission : il n'en est plus un agent passif. Il en va de même s'il sélectionne le récipiendaire ou celle qui peut y accéder.

Le prestataire qui conserve le document plus longtemps que nécessaire pour sa transmission se trouve à être en possession du document et exerce sur celui-ci un contrôle accru qui dépasse ce qui est nécessaire afin d'assurer la transmission. Ce peut être par exemple, s'il intercepte le document. Le contrôle physique effectif est alors exercé par une personne qui, sachant qu'elle contribue à la diffusion d'un document, a la possibilité de le retirer ce message et mettre un terme à sa circulation.

Par contraste, lorsque toutes ces décisions sont prises par l'usager, c'est celui-ci qui effectue la communication, non le prestataire de services qui procure à l'usager une plateforme afin de lui permettre d'effectuer la communication de renseignements personnels ou de tout autre document technologique.

Ces principes étant rappelés et contextualisés dans le cadre étendu de la communication en ligne, ils permettent d'éclairer le sens et la portée de notions cruciales dans le processus de communication de documents, y compris ceux qui comportent des renseignements personnels. Ces principes mettent également en lumière le fait que des degrés différenciés de contrôle te de maîtrise peuvent être exercés à l'égard de l'information circulant dans les environnements en réseaux.

---

86 L.R.Q. c. C-1.1, disponible à http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html.

Dans un environnement en réseau, l'information circule d'un point à l'autre. Mais la circulation de l'information n'emporte pas sa communication à chacun des points dans lesquels elle est relayée. Personne n'irait prétendre qu'un postier en possession physique pendant quelques temps d'une lettre comportant des renseignements personnels s'est vu communiquer ces renseignements. Il y a en effet dans le cycle de traitement de l'information personnelle, et particulièrement, dans le traitement des documents technologiques pouvant comporter de tels renseignements, des situations qui ne constituent pas une « communication ».

Par exemple, lorsque l'usager effectue une opération sur un site, il demande de l'information à un organisme, il prend connaissance d'information puis l'achemine à un autre organisme, cette opération n'emporte pas que le site acquiert le contrôle sur l'information ainsi transitée. Le site tient alors un rôle d'intermédiaire technique. Selon la Cour de cassation belge, citée par Montero, l'intermédiaire est « celui dont l'activité revêt un caractère purement technique, automatique et passif, ce qui implique qu'il ne connaît pas et n'exerce pas de contrôle sur l'information qui est transmise et stockée. »[87] C'est dire l'importance de situer avec plus de précision les lieux où s'exercent effectivement le contrôle de l'information dans un réseau.

3.4 Les droits de produire de l'information

Le droit de produire de l'information en élevé au rang de droit constitutionnel au Canada. Les libertés expressives sont garanties par les textes constitutionnels. Cela découle des garanties constitutionnelles de la liberté d'expression, de la liberté de la presse et des autres moyens de communication énoncés à l'article 2b) de la *Charte canadienne des droits et libertés*[88]. La liberté éditoriale possède une valeur constitutionnelle au Canada : elle ne peut être écartée que par une règle de droit et dans la mesure où cela est raisonnable et justifiable dans une société libre et démocratique.

La liberté éditoriale est la forme que prend la liberté d'expression lorsqu'elle s'applique aux médias comme entité[89]. Depuis longtemps, on reconnaît que les autorités gouvernementales n'ont pas la faculté de s'ingérer dans les décisions relatives à la production et à la transmission de l'information. La liberté éditoriale est protégée car elle constitue l'une des meilleures façons de garantir au public un accès aux informations et à la diversité des points de vue.

La liberté éditoriale suppose une autonomie de principe dans les décisions relatives aux choix, au traitement et à la diffusion des informations. Elle a pour contrepartie la responsabilité : les détenteurs de la liberté éditoriale répondent, devant les tiers, des informations diffusées à l'exclusion de tout autre personne. Ainsi, celui qui exerce sa liberté de produire de l'information,

---

87 Étienne MONTERO, « Les responsabilités liées au Web 2.0 », [2008] *R.D.T.I.,* 363 p. 367.

88 Partie I de la *Loi constitutionnelle de 1982*, [Annexe B de la *Loi de 1982 sur le Canada* (1982, R.-U., c. 11)].

89 Susan D. CHARKES, « Editorial Discretion of State Public Broadcasting Licensees », (1982) 82 *Columbia L. Rev*. 1161, 1172.

est libre de véhiculer la signification qui lui convient. Mais il supporte les conséquences de ces choix. C'est à ce niveau qu'interviennent les

3.4.1 La protection des personnes

Il est évidemment licite de parler d'une personne. Le principe général est qu'il est loisible à tous d'exprimer leur point de vue à l'égard d'une personne, de ses agissements et des différents aspects de son activité. Il y a cependant des limites à cette liberté. Ces limites découlent du fait que les personnes ont le droit de protéger leur réputation, leur vie privée et leur image. Il existe aussi des règles les protégeant contre le harcèlement.

Dès lors que l'on décide de recueillir des informations personnelles, il faut le faire en respectant un ensemble de dispositions spécifiques. La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* impose en effet des obligations aux « organismes publics »[90]. Ces derniers doivent limiter leur collecte de renseignements personnels aux seules fins nécessaires à la fourniture des services offerts. Des exigences strictes existent aussi pour la conservation ou l'utilisation qui peut être faite de ces renseignements.

Le droit à la protection des renseignements personnels constitue une facette des régimes de protection de la vie privée[91]. Des dispositions garantissant la protection des renseignements personnels en droit québécois se retrouvent dans 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*.

Ces lois consacrent le caractère confidentiel des renseignements personnels[92]. Ainsi, il est prévu un ensemble de mesures visant à encadrer la cueillette, l'utilisation, la conservation et la communication de renseignements personnels. Un renseignement personnel est un renseignement qui concerne une personne et permet de l'identifier.

La législation québécoise sur la protection des renseignements personnels limite le droit d'un organisme public ou d'une entreprise de recueillir des informations personnelles. De telles informations ne peuvent être recueillies qu'auprès de la personne concernée ou d'un tiers, en certaines circonstances spécifiques[93].

---

90 Aux termes de l'article 3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q., c. A-2.1, ci-après citée *Loi sur l'accès*), les organismes publics sont : le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères, les organismes gouvernementaux, les organismes municipaux, les organismes scolaires et les établissements de santé ou de services sociaux.

91 Raymond DORAY, « Le respect de la vie privée et la protection des renseignements personnels dans un contexte de commerce électronique », dans Vincent GAUTRAIS, (éd.) *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 303-361.

92 *Loi sur le secteur privé*, art. 10; *Loi sur l'accès*, art. 53; voir aussi le *Code civil du Québec*, art. 35 à 41.

93 *Loi sur l'accès*, art. 65; *Loi sur le secteur privé*, art. 6.

En général, pour collecter licitement des renseignements personnels, il faut être en mesure de démontrer la nécessité des renseignements demandés. Pour l'organisme du secteur public, il est licite de recueillir un renseignement personnel seulement si cela est nécessaire à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. Dans le secteur privé, il faut pouvoir démontrer la nécessité de la collecte compte tenu de l'activité visée.

Les renseignements personnels ne peuvent être utilisés que pour les fins pour lesquels ils ont été recueillis. Si de nouvelles finalités apparaissent, il faut s'assurer d'obtenir le consentement approprié de l'intéressé avant de faire usage des renseignements personnels.

La communication de renseignements personnels à des tiers est interdite sauf avec le consentement de la personne concernée ou dans certaines circonstances prévues par la loi ou lorsque cela est nécessaire à l'application d'une loi[94].

Par exemple, la divulgation ou la transmission des renseignements aux tiers est possible si cela est nécessaire : à l'exécution du contrat entre les parties, au respect d'une obligation légale imposée par une autorité, à la sauvegarde de l'intérêt vital de la personne, à l'exécution d'une mission d'intérêt public, à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement.

Autrement, les renseignements personnels ne peuvent pas être divulgués, ni transmis à des tiers qu'avec le consentement de la personne concernée ou lorsqu'une règle de droit le permet.

Les renseignements personnels ne doivent être détenus que dans la mesure où ils sont nécessaires à l'accomplissement de la fin pour laquelle ils ont été recueillis. C'est pourquoi il faut en tout temps être en mesure d'indiquer quelles sont les utilisations qui sont faites des informations personnelles demandées et détenues.

L'usager doit être en mesure de déterminer facilement l'existence et la nature des renseignements personnels collectés et détenus et les finalités de leur utilisation[95]. Il faut expliquer de façon claire et simple quel type de renseignement personnel est recueilli, dans quel but et expliquer la manière dont cette information est traitée[96]. L'usager ne doit pas être laissé dans un état d'incertitude quant à la politique du site concernant la protection des renseignements personnels. Ainsi le concepteur d'un environnement doit éviter que soient recueillies des informations personnelles sans que les usagers soient informés au préalable de la façon dont ces renseignements seront traités et utilisés.

L'usager qui se fait demander des renseignements personnels dont on n'a pas démontré la nécessité, compte tenu du bien ou du service concerné, doit s'interroger si les risques qu'il prend à l'égard de la protection des renseignements personnels ne sont pas trop élevés.

---

94 *Loi sur l'accès*, art. 59, 67; *Loi sur le secteur privé*, art. 13, 18.

95 *Loi sur le secteur privé*, art. 8 et 27; *Loi sur l'accès*, art. 65 et 83.

96 AUSTRALIAN PRIVACY COMMISSIONER'S, *Guidelines for Federal and ACT Government Websites*, < http://www.privacy.gov.au/internet/web/index.html >.

Celui qui procède ou fait procéder au traitement des renseignements personnels assume la responsabilité qui en découle. Il lui incombe de prendre toutes les mesures requises afin que les principes relatifs à la protection des renseignements personnels aient plein effet.

La personne concernée a un droit d'accès à son dossier[97]. Cela emporte l'obligation de permettre l'accès à ce dossier d'une manière simple et facile. Le plus souvent, on cherchera à assurer les accès à ces dossiers par un mécanisme en ligne.

En outre, la personne concernée doit avoir la possibilité de corriger ou effacer les informations erronées ou incomplètes la concernant[98]. Elle dispose d'un droit de recours auprès de la Commission d'accès à l'information lorsque ces droits lui sont niés[99].

3.4.2 Liberté de s'approprier l'information

Une fois produite, l'information est susceptible de certains droits tendant à son appropriation. Les règles de la propriété intellectuelle visent précisément à déterminer la portée des droits exclusifs que l'on peut exercer à l'égard d'un bien informationnel. La propriété intellectuelle désigne la relation juridique intime qui existe entre un créateur et son œuvre et rend compte du caractère exclusif de celle-ci. Le professeur Kerever écrit :

> *Ce qu'on appelle « propriété intellectuelle », c'est un faisceau de droits légaux, permettant à l'auteur, ou au propriétaire de l'œuvre immatérielle, d'interdire à des tiers d'utiliser et d'exploiter son œuvre sans son autorisation, le défaut d'autorisation engageant la responsabilité civile et pénale de l'utilisateur non autorisé. Il en résulte que la jouissance et l'exercice de ces droits bien particuliers sont subordonnés à l'édiction de lois, de normes obligatoires s'imposant à tous les membres de la société, de tribunaux pour assurer (l'application) de ces lois en sanctionnant civilement et pénalement les contrevenants, de policiers pour rechercher les infractions.*[100]

La propriété intellectuelle et la reconnaissance de droits subjectifs par voie législative poursuivent plusieurs finalités. On peut même penser que la propriété intellectuelle participe, dans une certaine mesure, à la promotion de la dignité humaine et contribue à l'identité culturelle. En effet, l'article 27 de la *Déclaration universelle des droits de l'homme* de 1948 énonce que chacun a *« droit à la protection des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur »*.

---

97 Voir les articles 38 à 40 du C.c.Q; *Loi sur le secteur privé*, art. 27 et ss.; *Loi sur l'accès*, art. 83 et ss.

98 *Loi sur l'accès*, art. 89 et ss.; *Loi sur le secteur privé*, art. 28; art. 40 C.c.Q.

99 *Loi sur le secteur privé*, art. 42 à 53; *Loi sur l'accès*, art. 135 et ss.

100 André KEREVER, « Propriété intellectuelle : La détermination de la loi applicable aux transmissions numérisées », dans Jacques FRÉMONT et Jean-Paul DUCASSE (dir.), *Les autoroutes de l'information : Enjeux et défis*, *Actes du Colloque tenu dans le cadre des Huitièmes entretiens Centre Jacques Cartier*, 5 au 8 décembre 1995, Rhône-Alpes, Les chemins de la recherche, 1996, p. 254.

C'est minimalement cette production qui est protégée par la propriété intellectuelle. Autrement dit, la propriété intellectuelle récompense les créateurs en leur reconnaissant des droits privatifs sur leurs réalisations et en condamnant les utilisations non autorisées de celles-ci par des tiers. En un sens, ces droits privatifs viennent limiter la liberté de circulation des informations. C'est pourquoi cette protection a une durée limitée dans le temps, au terme de laquelle l'œuvre tombe dans le « domaine public » et redevient ainsi de libre parcours.

L'importance de la propriété intellectuelle dans la nouvelle économie ne fait plus de doute[101]. Le régime des droits d'auteur y contribue de façon substantielle. En effet, à l'heure des sociétés de l'information, le droit d'auteur apparaît comme l'un des principaux outils de développement culturel et de croissance économique. D'ailleurs, le développement des inforoutes a amené la plupart des États à s'interroger sur l'adéquation de leur cadre juridique, en matière de droit d'auteur et de propriété intellectuelle, pour rencontrer les exigences et défis de la société de l'information[102].

3.5 Les libertés relatives aux supports

La *Loi concernant le cadre juridique des technologies de l'information* prévoit des règles relativement à l'établissement de documents sur divers supports, au transfert de l'information d'un document d'un support à un autre, aux conditions de l'intégrité des documents tout au long de leur vie, au lien entre une personne et un document, ainsi qu'à la certification.

---

101 Voir Silke von LEWINSKI, « Le rôle du droit d'auteur dans le commerce international aujourd'hui » (1994) 161 *R.I.D.A.* 4-98, qui explique que depuis 1988, l'approche à l'égard du droit d'auteur a été considérablementa changée, passant de négative (une mesure qui limite la libre circulation) à positive (qui la favorise), venant ainsi insister sur la nécessité d'intégrer l'obligation de la protection des droits d'auteur dans le cadre des accords commerciaux multilatéraux et bilatéraux. Voir aussi Victor NABHAN, « L'Accord de libre-échange et le droit d'auteur : Perspective canadienne » (1994) 161 *R.I.D.A.* 99-159 et Ronald K.L. COLLINS et David M. SKOVER, « Essay : Commerce & Communication » (1993) 71 *Texas Law Review* 697-746.

102 Voir notamment les rapports suivants : des États-Unis, le WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, *Intellectual Property and the National Information Infrastructure - The Report*, Bruce A. Lehman (Chair), Washington, 1995, (également désigné comme le *Livre blanc* américain); de la France, MINISTÈRE DE LA CULTURE ET DE LA FRANCOPHONIE, *Industries culturelles et nouvelles techniques*, Rapport de la Commission présidée par Pierre Sirinelli, Paris, Juin 1994; du Japon, AGENCY FOR CULTURAL AFFAIRS OF JAPAN, Green Paper of Japan, Report of Discussions by the Working Group of the Subcommittee on Multimedia of the Copyright Council, « Summary », February 1995; de la Commission des Communautés européennes, COMMISSION DES COMMUNAUTÉS EUROPÉENNES, *Le droit d'auteur et les droits voisins dans la Société de l'Information*, (également désigné comme le *Livre vert* de la Commission des Communautés européennes, COM (95) 382 final; et enfin, au Canada, COMITÉ CONSULTATIF SUR L'AUTOROUTE DE L'INFORMATION, *Le droit d'auteur et l'autoroute de l'information*, Rapport final du Sous-comité sur le droit d'auteur, Ottawa, mars 1995 et COMITÉ CONSULTATIF SUR L'AUTOROUTE DE L'INFORMATION, *Contact, Communauté, Contenu : Le défi de l'autoroute de l'information*, Rapport final du Comité consultatif sur l'autoroute de l'information, Ottawa, 1995, p. 131 (ci-après « Rapport final du CCAI »). Voir pour un résumé des principales propositions : ALAI-Canada, *Multimédia, inforoutes, droits d'auteur et droits voisins*, Actes de la journée d'étude du 23 février 1996 à Montréal (à paraître en 1997).

Le cycle de vie du document commence à sa création. Comme un document peut être consigné sur différents supports, se pose la question de savoir qui décide du choix du support?

L'article 2 énonce le principe général de la liberté des personnes quant au choix des supports qui servent à produire des documents.

Cette liberté de choix est conditionnée par l'obligation de respecter les règles de droit. De même, la valeur juridique d'un document n'est ni augmentée ni diminuée pour la seule raison qu'un support ou un autre a été choisi. Ce principe est d'ailleurs mentionné à l'article 5.

Ainsi, à moins qu'une règle de droit impose le recours à un support spécifique, le principe de la liberté de choix du support est celui qui prévaut.

3.6 La communication

Communiquer un renseignement ou un document implique de conférer un droit de prendre connaissance de la teneur du document ou du renseignement. Si le document est mis en possession physique ou juridique d'une entité, cela ne signifie pas que celle-ci ait obtenu communication du document ou du renseignement.

La définition même du mot communication suppose que l'information est portée à la connaissance d'une personne. Dans son vocabulaire juridique, Gérard Cornu définit ainsi le mot « communication : « Fait de porter un événement ou un élément d'information à la connaissance d'une personne déterminée d'un groupe d'intéressés ou du public. » Gérard Cornu, *Vocabulaire juridique*.

Dans le *Dictionnaire de droit québécois et canadien* de Hubert Reid, le mot communication est défini comme étant l'«action de porter un fait ou un élément d'information à la connaissance de quelqu'un ».

Dans Henry Campbell BLACK, *A dictionary of law*, New York (NY), Lawbook Exchange, 1891. La définition suivante de « Communication » est donnée : « Information given; the sharing of knowledge by one with another; conference; consultation or bargaining preparatory to making a contract. Also intercourse; connection. »

Dans l'édition de 2004 du Bryan A. GARNER (dir.), *Black's law dictionary*, 8e éd., St. Paul (Minn.), Thomson/West, 2004 : « Communication » 1. The expression or exchange of information by speech, writing, gestures, or conduct; the process of bringing an idea to another's perception. 2. The information so expressed or exchanged.

La jurisprudence confirme le sens donné au mot communication. Dans *Goldman c. R.*, [1980] 1 S.C.R. 976, le juge Mcintyre écrit aux pages *994 et 995* que :

> *Il est élémentaire de dire que les cours doivent dégager l'intention du législateur et l'appliquer quand elles interprètent les lois. C'est en examinant les mots employés dans la loi que l'on doit dégager l'intention, car c'est à l'intention exprimée par le législateur qu'il faut donner effet. C'est pour cela qu'il faut examiner le sens des termes de la loi et faire parfois de subtiles distinctions. A mon avis, la différence entre le mot conversation*

> *et le mot communication est importante dans le contexte de cette disposition. Une communication comprend la transmission de pensées, d'idées, de mots ou de renseignements d'une personne à une autre. Le terme conversation est plus large et inclurait, comme toutes les conversations, l'échange d'une série de communications distinctes.*

Communiquer un document implique de conférer un contrôle sur celui-ci. Cela suppose de permettre à l'entité à qui l'on communique de prendre connaissance du document.

Cette distinction permet de rendre compte du fait qu'on ne songe pas à rendre une entité qui ne fait que déplacer un document d'un point d'expédition à un autre point acquiert le contrôle sur ce document. Par exemple, le facteur qui livre une lettre a beau être en pleine possession de celle-ci, il n'a pas le contrôle du document puisqu'il n'a pas le droit d'en prendre connaissance. Ainsi, lorsqu'une personne en possession physique d'un document n'a pas le droit de l'utiliser, celui-ci ne lui est pas communiqué.

Par exemple, aux termes de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information,* le prestataire qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier. Ainsi, lorsque le prestataire-intermédiaire propose une plateforme dans laquelle il est loisible aux usagers de commander des informations, par exemple en actionnant un lien pour ensuite les acheminer à un tiers, le prestataire qui offre de tels services de conservation n'acquiert pas le contrôle sur les documents ainsi traités. Ces documents ne lui sont pas communiqués. C'est l'usager qui se fait communiquer des documents et décide de les transmettre à un tiers.

La communication se distingue de la « mise à disposition » qui consiste à rendre disponible un document pour une communication. Tant que le document n'est qu'à disposition, il n'est pas effectivement communiqué. Par contre, la mise à disposition se présente habituellement comme une situation ayant vocation à mener à la communication du document. C'est pourquoi il est habituellement nécessaire d'avoir le droit de communiquer pour pouvoir mettre à disposition.

L'utilisation de l'information suppose que celle-ci a été communiquée. Utiliser de l'information, c'est forcément exercer un certain contrôle sur celle-ci, c'est en prendre connaissance.

Utiliser des renseignements personnels implique d'en avoir connaissance et de décider à la lumière de la connaissance que ces renseignements confèrent.

Pour utiliser des renseignements personnels, il faut généralement en avoir connaissance. Il faut donc que ceux-ci nous aient été communiqués en tout ou en partie. L'on fait usage d'information afin de décider. Soit que l'on doit disposer d'un certain degré de certitude ou que l'on a besoin d'établir des faits qui donnent ouverture à une décision.

3.7 La collecte de l'information

La collecte est une forme de communication de documents. Elle est régie par d'un encadrement particulier dans les lois sur la protection des renseignements personnels[103]. Collecter de l'information, c'est non seulement acquérir une nouvelle information mais de surcroît disposer sur celle-ci d'un contrôle effectif. Ainsi, la collecte de renseignements personnels s'entend donc comme une opération par laquelle des renseignements sont placés sous le contrôle d'une entité qui du fait de cette opération acquiert, à l'égard des documents ou renseignements, un droit d'en prendre connaissance. Pour qu'il y ait « collecte » de renseignements ou de documents, il faut que ces documents ou renseignements aient été communiqués à une entité, à une personne qui en prend connaissance.

Il ne peut y avoir collecte sur une information que l'on possède déjà. Cette interprétation tient presque d'une lapalissade tant il apparaît évident que la définition semble associer à la notion de « cueillir » (de même étymologie que le verbe collecter), voire même à cette notion de « première fois ». Terme de première fois qui apparaît d'ailleurs dans la lettre même de l'article 65 de la *Loi sur l'accès*, où on envisage expressément l'hypothèse de la cueillette initiale[104]. Pourtant, il importe de le rappeler ici dans la mesure où il est des situations où la question se pose. Au regard des trois illustrations vues plus tôt, il est notamment possible de citer l'hypothèse numéro 1, concernant l'identification des usagers, où ne serait pas considéré comme étant une collecte la situation par laquelle une administration reçoit des renseignements personnels d'un usager, renseignements que ce dernier serait uniquement porté à donner afin qu'un service commun puisse reconnaître l'identité de la personne.

La collecte implique soit d'avoir connaissance des renseignements personnels en cause soit de disposer du droit d'en prendre connaissance. Le fait d'être en possession physique d'un support comportant une information ne constitue pas forcément une collecte. Par exemple, le livreur qui est chargé de transporter une caisse de documents comportant des renseignements personnels ne collecte pas de renseignements personnels. Il n'a à l'égard de ces informations, aucun droit d'en prendre connaissance mais par contre, il a une obligation de traiter ces documents de façon conséquente selon les directives ou indications que lui a donnée l'entité qui lui en a confié la garde[105]. Également, le fait qu'il ait la capacité physique de le faire n'implique pas forcément une qualification différente de l'opération. Simplement, des règles de responsabilités sont envisageables s'il devait contourner ses obligations.

---

103 Dans la LAPRPSP, on peut notamment référer aux articles 63.1, 64, 65. Dans la Loi sur le Ministère du Revenu, on peut identifier l'article 69.

104 Art. 65 LAPRPSP : « Quiconque, au nom d'un organisme public, recueille verbalement un renseignement personnel auprès de la personne concernée doit se nommer et, lors de la première collecte de renseignements et par la suite sur demande, l'informer: (…) »

105 Art 26, Loi concernant le cadre juridique des technologies de l'information, L.R.Q. c. C-1.1, disponible à http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html.

Pour être tenu à des obligations associées à une collecte de renseignements personnels, il faut nécessairement que l'on ait acquis le contrôle de l'information concernée, à savoir, les renseignements personnels, qu'on ait le droit et la possibilité technique d'en prendre connaissance.

3.8 La détention de l'information

Le détenteur est la personne qui est en possession d'une chose. La possession est un fait : celui d'être en contrôle d'un bien. Strictement, la détention s'applique au support sur lequel est consigné l'information. L'information est connaissance. Lorsqu'on détient de l'information, c'est qu'on a connaissance de celle-ci, c'est donc que l'information nous a été communiquée.

Par contre dans le déroulement des différentes phases de la circulation de l'information, il peut arriver qu'un acteur en particulier soit simplement détenteur d'un support comportant de l'information.

Ainsi, La détention des renseignements personnels est la situation dans laquelle une entité est en possession physique du support sur lequel est consigné un renseignement personnel.

3.9 Le droit d'accéder et de consulter

Accéder et consulter un document ou un renseignement implique de se le faire communiquer. Le droit d'accéder aux documents ne va pas de soi. Il est prévu par des lois qui en délimitent la portée. La *Loi concernant le cadre juridique des technologies de l'information* a adapté le droit d'accès aux documents au contexte des technologies de l'information et entoure la consultation de documents technologiques de mesures de protection des renseignements personnels et confidentiels.

Lorsqu'une personne a accès à un document, celui-ci doit être consultable directement ou en faisant appel aux technologies de l'information (Article 23). Ainsi, un document peut être examiné par l'accès à une copie du document, à un document résultant d'un transfert ou à une copie de ce dernier. Toutefois, il doit y avoir un équilibre réaliste entre le choix d'une personne quant au support ou la technologie permettant l'accès au document et la possibilité —ou la capacité— de répondre à ce choix.

La possibilité de consultation d'un document à distance qu'offrent les technologies de l'information est prévue dans la loi (par exemple, les articles 40, 50 et 60 de la *Loi concernant le cadre juridique des technologies de l'information*). De plus la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., chapitre A-2.1) permet l'accès aux documents des organismes publics à distance de même qu'elle prévoit la consultation sur place ou par obtention d'une copie (articles 82, 83, 84, 85).

Lorsqu'une personne a droit d'accès à un document, celui-ci doit être consultable directement ou en faisant appel aux technologies de l'information (article 23). Ainsi, un document peut être examiné par l'accès à une copie du document, à un document résultant d'un transfert ou à une copie de ce dernier. Toutefois, il doit exister un équilibre réaliste entre le choix d'une personne quant au support ou la technologie permettant l'accès au document et la possibilité — ou la

capacité — de répondre à ce choix. La personne responsable de l'accès à un document technologique doit prendre des mesures de sécurité propres à assurer la confidentialité des renseignements (article 25).

Une personne, qui confie un document technologique à un prestataire qui doit en assurer la garde, doit informer ce prestataire des protections que requiert le document en ce qui a trait à la confidentialité de l'information. Le prestataire est tenu d'en assurer la sécurité, d'en préserver l'intégrité et d'en protéger la confidentialité (article 26).

Dans le cas des documents contenant des renseignements personnels et qui sont rendus publics pour une finalité particulière, les fonctions de recherche extensives doivent être restreintes à cette finalité (article 24).

3.10 L'obligation de diffuser certains documents

L'article 4 du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*[106] énumère une série de documents que certains organismes publics ont l'obligation de diffuser dans un site internet dans la mesure où ces documents sont accessibles en vertu de la loi. Ainsi, les paragraphes 7 et 8 visent :

> *les études, les rapports de recherches ou de statistiques, produits par l'organisme public ou pour son compte dont la diffusion présente un intérêt pour l'information du public ;*
>
> *les documents transmis dans le cadre d'une demande d'accès dont la diffusion présente un intérêt pour l'information du public ;*

Dans tous les cas visé par l'article 4 du Règlement, il s'agit de documents qui sont accessibles en vertu de la *Loi sur l'accès*. La question ne se pose donc pas de savoir s'il est licite ou non de diffuser ces documents. C'est le caractère accessible aux termes de la loi qui est le facteur déclenchant l'application de l'obligation visée à l'article 4 du Règlement. Les paragraphes 7 et 8 de l'article 4 obligent l'organisme détenteur à le diffuser sur un site internet dès lors que celui-ci « présente un intérêt pour l'information du public ».

La notion d'intérêt public, à l'instar de la plupart des notions juridiques renvoyant à des valeurs fondamentales est susceptible d'une pluralité de sens. Dans les sociétés démocratiques, il existe un vaste ensemble de conceptions de ce qui correspond à l'intérêt public. Chacune des significations qui sont données à la notion peut revendiquer une certaine part de légitimité. C'est pourquoi une règle énoncée au moyen d'un standard comme celui-là devient le siège des enjeux opposant les divers groupes d'intérêt dans la société civile.

Il n'y a pas un seul sens à la notion d'intérêt public. Il est rare que les définitions qui en sont données fassent l'unanimité. Lorsqu'une telle unanimité existe, il devient souvent plus aisé

---

106 Décret 408-2008, 23 avril 2008, GOQ, 14 mai 2008, 140e année, no. 20, p. 2081.

d'exprimer a priori et de manière plus détaillée, les différents droits et obligations des acteurs de même que leurs limites respectives.

Mais lorsque l'unanimité n'existe pas, il est plus facile d'énoncer une règle en renvoyant l'interprète à l'appréciation de l'intérêt public. Cela suppose le recours à un standard qui guidera les décideurs dans leur mission d'évaluation. On déterminera alors le sens de la notion d'intérêt public au fil des situations concrètes, en considérant les divers éléments du contexte propre à la situation à laquelle on est confronté.

L'appréciation de l'intérêt du public est un exercice d'évaluation. Cette évaluation sera forcément – à un certain point - tributaire des valeurs de la personne qui l'effectue. Déterminer ce qui « présente un intérêt pour l'information du public » revient à faire une évaluation du document concerné de même qu'une appréciation du contexte dans lequel serait diffusé le document.

On peut déceler une approche large de la notion d'intérêt pour le public et une approche plus étroite, qui insiste sur les conséquences présumément adverses de la diffusion.

L'approche large de l'intérêt public

On peut anticiper que certains interprètes opteront pour une approche large de la notion : sera d'intérêt public ce qui représente un intérêt pour une partie de celui-ci. Dans la logique des paradigmes du « marché des idées » (*marketplace of ideas*) en droit américain, l'on postule que si une partie du public trouve de l'intérêt dans une question, c'est que celle-ci est d'intérêt public. Suivant une telle logique, l'intérêt public est déterminé par un processus analogue au « marché » : si une idée recueille de l'intérêt elle sera tenue pour avoir de la valeur et inversement, si une idée ne recueille que peu d'intérêt, elle sera réputé avoir peu de valeur. C'est une conception libérale de l'intérêt pour l'information du public : suivant une telle conception, dès lors qu'il est constaté que le document suscite l'attention, il présente un intérêt pour le public.

Appliquée à l'analyse d'un document accessible au sens de la Loi, cela reviendrait à poser que dès lors qu'un document est susceptible d'intéresser une personne, il est présumé être d'intérêt public de le rendre disponible sur le site web.

L'approche « conséquentialiste »

Au Québec, comme dans plusieurs autres sociétés développées, il existe une conception de l'intérêt public qui attache une plus grande importance aux conséquences prévues, escomptées ou prévisibles d'une situation afin de déterminer ce qui correspond à l'intérêt public. Selon ces conceptions « conséquentialistes » : on juge de l'intérêt pour le public à partir d'une évaluation des possibles conséquences que pourrait engendrer sa diffusion. L'anticipation d'une conséquence adverse d'une décision constitue, dans ce schéma de raisonnement, un motif pertinent afin de déterminer ce qui peut être tenu pour aller dans le sens de l'intérêt public.

Certaines dispositions des lois semblent rédigées en fonction d'une approche accordant de l'importance aux conséquences qui pourraient découler de la diffusion d'un document. Par exemple, l'article 55 de la *Loi sur l'accès* prévoit que :

> *« Un renseignement personnel qui a un caractère public en vertu de la loi n'est pas soumis aux règles de protection des renseignements personnels prévues par le présent chapitre.*
>
> *Cependant, un organisme public qui détient un fichier de tels renseignements peut en refuser l'accès, en tout ou en partie, ou n'en permettre que la consultation sur place si le responsable a des motifs raisonnables de croire que les renseignements seront utilisés à des fins illégitimes. » (les soulignements ont été ajoutés)*

L'article 55 introduit la possibilité, exceptionnelle dans le domaine de l'accès aux documents des organismes publics, de prendre en considération les motivations de la personne qui demande d'accéder à un document. Il autorise de porter un jugement de valeur sur les utilisations possibles des renseignements. Avant même que ces utilisations soient faites, l'organisme public peut anticiper – en somme, faire un procès d'intention, à l'égard des utilisations qui pourraient être faites des renseignements. Au surplus, l'organisme peut refuser l'accès à ces renseignements, pourtant à caractère publics, en posant un jugement sur la « légitimité » des utilisations que l'on pourrait anticiper. Voilà un exemple d'une disposition qui autorise à porter un jugement fondé sur les conséquences d'une diffusion de renseignements.

L'approche conséquentialiste, accorde un poids important aux possibles conséquences qui pourraient résulter de la diffusion d'un document. Une telle approche suppose forcément un jugement de valeur à l'égard de ce qui pourrait advenir de la diffusion du document. De ce jugement de valeur, découle une évaluation de l'intérêt que présente la diffusion pour le public en relation avec les possibles conséquences adverses de la diffusion.

Par exemple, un décideur pourrait anticiper les conséquences de la diffusion d'un document qui contredit les prétentions du premier dirigeant de l'organisme. Il pourrait déterminer que la diffusion du document engendre de la confusion sur ce qui constitue effectivement la position du ministère et estimer que cela ne sert pas l'intérêt public.

Les dangers d'une approche fondée sur les conséquences de la diffusion sautent aux yeux. Il est en effet parfois difficile de faire la distinction entre ce qui va dans le sens de l'intérêt de l'organisme ou de ses dirigeants et ce qui constitue l'intérêt public.

Est-ce l'alinéa 7 et 8 donnent ouverture à l'analyse conséquentialiste ?

Plusieurs arguments peuvent être invoqués à l'encontre du recours à une approche conséquentialiste pour appliquer les aliéas 7 et 8 de l'article 4. Le plus important tient au contexte dans lequel s'inscrit le règlement lui-même. Celui-ci vise à assurer la diffusion de documents qui sont accessibles au sens de la Loi. Il est donc légitime de postuler que les arbitrages de valeurs qui doivent forcément avoir lieu afin de déterminer si un document devrait circuler ont été faits par le Parlement. Les documents qui sont visés par une exception au principe de l'accès ne sont pas concernés par ces dispositions du Règlement. Les motifs qui pouvaient exister afin de s'opposer à la diffusion du document ne sont donc pas applicables.

Il ne reste que les motifs fondés sur les conséquences quantitatives et qualitatives découlant de la diffusion sur Internet. Il est devenu courant de considérer que la diffusion sur Internet emporte des enjeux qui peuvent différer de ceux qu'implique la diffusion hors-ligne. La diffusion en ligne

suppose en effet une portée beaucoup plus considérable. Un document public accessible auprès de l'archiviste d'un ministère bénéficie d'un potentiel de diffusion infiniment moindre que lorsqu'il est disponible sur Internet. Il en découlerait des enjeux qui ne seraient pas présents lorsque la diffusion demeure tributaire d'une démarche dans un lieu physique déterminé.

Il n'y a cependant pas beaucoup de données empiriques qui permettraient de vérifier la mesure dans laquelle la disponibilité sur Internet emporte des conséquences aussi importantes qu'on le craint parfois.

Éléments d'une grille d'évaluation de l'intérêt public

Il est possible d'identifier les éléments d'une grille d'analyse des documents afin de déterminer dans quelle mesure ils sont susceptibles de représenter un intérêt pour l'information du public.

Il s'agit, rappelons –le des « les études, les rapports de recherches ou de statistiques, produits par l'organisme public ou pour son compte dont la diffusion présente un intérêt pour l'information du public ;

> *«*
>
> *Est-ce que le document serait ou est accessible ?*
>
> *Est-ce que le document peut intéresser une personne ? Si le document a déjà fait l'objet d'une demande d'accès, il faut forcément répondre par l'affirmative.*
>
> *Il faut garder à l'esprit que ces dispositions concernent des documents qui sont accessibles. Donc, les intérêts qui auraient à être préservés par la non-divulgation sont déjà pris en compte par le législateur.*
>
> *Est-ce que par son sujet ou par sa forme, il existe une raison pour prétendre qu'il ne présente pas d'intérêt pour l'information du public.*
>
> *Pour répondre à cette question, certains facteurs pourront être considérés :*
>
> *Le document présente des carences au plan de la forme.*
>
> *Le document a fait l'objet d'évaluations négatives au regard de sa validité technique ou scientifique…*
>
> *Le document pourrait-il induire en erreur ? Est-ce que ces erreurs circulant dans le public seraient nuisibles à l'intérêt public ?*
>
> *Le document est-il conforme aux standards de qualité linguistique ?*

Voilà les principaux repères afin d'appliquer les paragraphes 7 et 8 de l'article 4 du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels.*

3.11 La conservation

La conservation est l'action de maintenir intact, dans le même état. Dès lors qu'une personne est tenue de conserver un document, elle a le devoir d'en assurer l'intégrité et l'accessibilité. Elle doit voir à la disponibilité du matériel permettant de le rendre accessible et de l'utiliser aux fins auxquelles il est destiné (article 19 *Loi concernant le cadre juridique des technologies de l'information*). Donc, dans certaines situations, le devoir de conserver peut comporter un devoir de préserver l'intégrité d'un document.

Des devoirs stricts incombent aux entités impliquées dans la conservation d'un document. Ainsi, l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*, la personne responsable de l'accès à un document technologique portant un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité.

Aux termes de l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* la personne qui confie le document à un prestataire de services pour en assurer la garde a l'obligation d'informer ce dernier de la protection que requiert le document lors de la remise du document. Il lui faut donner des informations adéquates sur les mesures de protection de la confidentialité que le document nécessite. Il faut pareillement indiquer quelles sont les personnes habilitées à en prendre connaissance.

De son côté, le prestataire de services doit faire en sorte que les moyens technologiques convenus d'un commun accord avec la personne qui lui a confié le document soient mis en place durant toute la période pendant laquelle il en la garde. Ainsi, il est tenu, durant la période où il en a la garde, de voir à ce que les moyens technologiques soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Au surplus, le prestataire a l'obligation de respecter toute autre obligation prévue dans une loi relativement à la conservation d'un document.

Quant la personne responsable de l'accès à un document technologique portant un renseignement confidentiel, elle a l'obligation, aux termes de l'article 25 de la Loi concernant le cadre juridique des technologies de l'information de « 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. »

La conservation d'un document est donc une opération distincte de sa communication : ce n'est pas parce qu'une entité conserve un document, exerce la garde de celui-ci qu'elle a le droit d'y accéder ou de le communiquer. Si un document confidentiel tel un document comportant des renseignements personnels est confié à une entité, celle-ci a l'obligation de s'assurer que la consultation du document ne soit réservée qu'aux personnes qui ont le droit de se voir communiquer le document.

Le seul fait de confier un document à une entité pour qu'elle le conserve n'emporte pas le droit de le communiquer s'il comporte des renseignements confidentiels ou des renseignements auxquels une personne n'a pas le droit d'accéder.

Le fait qu'une personne soit en possession physique d'un support comportant un document confidentiel ne lui confère pas le droit d'en prendre connaissance. Au contraire, la Loi lui impose plutôt l'obligation de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité.

On relève ici une différence entre un certain « sens commun » qui porte à penser que dès lors qu'on est mis en possession physique d'un document, on a le droit d'en prendre connaissance. Cela est vrai lorsque le possesseur d'un document n'est pas informé du caractère confidentiel du document et des mesures de protection qu'un tel statut requiert.

Dès lors qu'une personne est tenue de conserver un document, elle a le devoir d'en assurer l'intégrité et l'accessibilité. Elle doit voir à la disponibilité du matériel permettant de le rendre accessible et de l'utiliser aux fins auxquelles il est destiné (article 19 de la *Loi concernant le cadre juridique des technologies de l'information*). Par exemple, elle doit disposer du logiciel ou du matériel nécessaire pour que l'on puisse prendre connaissance du document.

L'article 20 de la *Loi concernant le cadre juridique des technologies de l'information* précise le droit de détruire le document dont l'information a été transférée. Il prévoit selon quelles conditions une personne peut détruire les documents, dont la *Loi* exige la conservation et qui ont fait l'objet d'un transfert.

Lorsqu'un document technologique est modifié, durant la période pendant laquelle il doit être conservé, des conditions doivent être respectées afin d'en préserver la valeur juridique en dépit de la modification (article 21). Si ces conditions n'étaient pas observées, il pourrait être considéré que la modification de l'information constitue une altération du document, ce qui lui ferait perdre son intégrité, qui fonde sa valeur juridique.

3.12 La transmission

Transmettre n'est pas communiquer. Transmettre un document, c'est l'expédier d'un point d'expédition à un point de réception. C'est le faire passer d'un point à l'autre. La notion de transmission est absente de la *Loi sur l'accès* et autres lois sur la protection des renseignements personnels. Plus exactement, les 25 occurrences dans la *Loi sur l'accès* référant au terme de transmission, ou à une de ses variantes, concernent généralement l'envoi de documents d'une personne à une autre[107]. En revanche, la *Loi concernant le cadre juridique des technologies de l'information*[108] réfère à cette notion de manière plus explicite.

---

107 On peut citer par exemple l'envoi d'avis à la Commission d'accès à l'information (articles 8, 64, 68.1), de l'envoi d'un document par un organisme public suite à une demande d'accès (article 11, 43), etc.

108 L.R.Q. c. C-1.1, disponible à http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html. 2, en ligne avec annotations à < http://www.msg.gouv.qc.ca/gel/cadre_juridique_intro.html > (site visité le 15 octobre 2008); Pierre TRUDEL, « Notions nouvelles pour encadrer l'information à l'ère du numérique : l'approche de la *Loi concernant le cadre juridique des technologies de l'information* », [2004] 106 *Revue du notariat*, 287-339.

L'article 28 de cette loi précise qu'un document peut être transmis, envoyé ou expédié par tout mode de transmission approprié à son support, à moins que la loi n'exige l'emploi exclusif d'un mode spécifique de transmission. Transmettre un document, c'est l'expédier d'un point d'expédition à un point de réception. C'est le faire passer d'un point à l'autre.

La transmission s'analyse comme une opération technique pouvant emporter communication, ou mise à disposition ou simple possession physique du document.

Le caractère confidentiel d'un document emporte évidemment des obligations lors de la transmission, l'article 34 de la *Loi concernant le cadre juridique des technologies de l'information*[109] dispose que lorsque la loi déclare confidentiels des renseignements que comporte un document, la confidentialité de ces derniers doit être protégée par un moyen approprié au mode de transmission et cela y compris sur les réseaux de communication.

La transmission doit s'effectuer de façon à protéger la confidentialité des renseignements. Le choix des moyens quant à la façon d'assurer la protection des renseignements confidentiels lors de la transmission d'un document est laissé à ceux qui en ont la responsabilité. Ceux-ci doivent cependant être en mesure de fournir, au besoin, la documentation expliquant comment les moyens pris permettent d'assurer la protection de la confidentialité. Cette documentation pourra établir, si requis, que la confidentialité a été maintenue lors de la transmission.

La transmission n'est pas en soi une situation emportant la communication d'un document. Seul le destinataire, celui à qui est effectivement destiné le document, a communication de celui-ci. Les autres prestataires impliqués dans le processus de transmission ont pour leur part une obligation de mettre en œuvre les moyens conséquents au mode de transmission afin de garantir la confidentialité de l'information transmise.

3.13 Le transfert de l'information

Les articles 17 et 18 de la *Loi concernant le cadre juridique des technologies de l'information* traitent du processus de changement du support de l'information (par exemple : transférer une photo sur support-papier vers un CD, transférer l'information contenue sur une bande sonore vers un disque CD, imprimer sur papier un document numérique…).

Il est possible de transférer l'information d'un document vers un support faisant appel à une technologie différente sans que le document perde sa valeur juridique.

Pour assurer le maintien de la valeur juridique d'un document lors d'un transfert, celui-ci doit être documenté; il faut être en mesure de démontrer, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée (article 17). L'article 18 de la *Loi concernant le cadre juridique des technologies de l'information* vient faciliter l'admission en preuve des documents résultant de transfert.

---

109 L.R.Q. c. C-1.1, disponible à http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html.

3.14 L'archivage

La *Loi sur les archives* prévoit l'établissement de calendriers de conservation. Le plus souvent, ces calendriers sont établis par règlement.

Tout document présentant une valeur archivistique, historique ou patrimoniale doit être conservé sur son support d'origine.

L'objectif visé est de préserver la mémoire collective. En effet, un document manuscrit peut avoir une grande valeur historique ou patrimoniale. Cela justifie de le conserver sur son support original même si son contenu a été numérisé afin d'en améliorer l'accessibilité.

Les critères déterminant si le document possède une valeur archivistique, historique ou patrimoniale sont élaborés par le gouvernement aux termes du premier paragraphe de l'article 69.

3.15 La destruction

L'article 20 de la *Loi concernant le cadre juridique des technologies de l'information* précise le droit de détruire le document dont l'information a été transférée. Il prévoit selon quelles conditions une personne peut détruire les documents dont la loi exige la conservation et qui ont fait l'objet d'un transfert. La destruction des documents pour lesquels la loi n'exige pas de conservation relève du bon vouloir de leur propriétaire. Mais cette liberté peut avoir été limitée par un contrat obligeant à la conservation. L'article indique les conditions de destruction :

- préparer et de tenir à jour des règles préalables à la destruction des documents ayant fait l'objet d'un transfert; Cette exigence ne vise pas les particuliers. Elle concerne les entreprises et l'État. De telles règles doivent êtres préparées et tenues à jour selon les règles de l'art;

- s'assurer de la protection des renseignements confidentiels et personnels que peuvent comporter les documents devant être détruits;

- la destruction ne doit pas mettre en péril la confidentialité. Par exemple, les documents détruits qui comporteraient des renseignements personnels doivent l'être de manière à éviter qu'ils soient fortuitement entre les mains de personnes susceptibles d'en prendre connaissance.

Dans le cas des documents en la possession de l'État ou d'une personne morale de droit public, il y obligation de s'assurer que la destruction est faite selon le calendrier de conservation établi conformément à la *Loi sur les archives*.

4. Le droit à la vie privée : étendue et limites

La *Charte des droits et libertés de la personne*[110] assure la protection des droits fondamentaux au Québec. À la différence de la *Charte canadienne des droits et libertés*, la *Charte* québécoise s'applique non seulement aux rapports des citoyens et de l'État, mais aussi aux rapports privés. Tant les individus que les sociétés commerciales sont touchés et se doivent de respecter ses prescriptions.

Si, pendant les premières années de son existence, la *Charte* québécoise fut surtout considérée comme un instrument permettant d'interpréter les droits législativement garantis par ailleurs, l'évolution récente de la jurisprudence a fait de la *Charte* un instrument normatif régissant et structurant les rapports tant privés que publics.

Qui plus est, le caractère solennel et proclamatif de cet acte de l'Assemblée nationale du Québec, ainsi que les mécanismes permettant de faire prévaloir les dispositions de la *Charte des droits et libertés de la personne* sur celles des lois dites ordinaires[111], ont permis au tribunaux de conclure que cet instrument législatif a un caractère supralégal, obligeant, compte tenu de sa « suprématie de principe »[112], d'interpréter toute loi, règlement ou autre règle en fonction des prescriptions de *la Charte des droits et libertés de la personne*[113]. Par ailleurs, la *Charte* québécoise doit s'interpréter à la lumière des interprétations données aux dispositions équivalentes contenues dans la *Charte canadienne des droits et libertés* dont elle constitue, en quelque sorte, le pendant au Québec[114].

L'article 9.1 de la *Charte* au même titre que l'article premier de la *Charte canadienne des droits et libertés*, permet de pondérer des droits concurrents présents dans la plupart des situations. Cet article est formulé ainsi :

> *Art. 9.1 : Les libertés et droits fondamentaux s'exercent dans le respect des valeurs démocratiques, de l'ordre public et du bien-être général des citoyens du Québec.*
>
> *La loi peut, à cet égard, en fixer la portée et en aménager l'exercice.*

---

110 *Charte des droits et libertés de la personne*, L.R.Q. c. C-12.

111 L'article 52 de la *Charte* prévoit : *Aucune disposition d'une loi, même postérieure à la Charte, ne peut déroger aux articles 1 à 38, sauf dans la mesure prévue par ces articles, à moins que cette loi n'énonce expressément que cette disposition s'applique malgré la Charte.*

112 *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Montréal (Ville)*, [2000] 1 R.C.S. 665, 683.

113 *Béliveau-Saint-Jacques* c. *Fédération des employées et employés des services publics Inc.*, [1996] 2 R.C.S. 345, 358 (la juge L'Heureux-Dubé et La Forest, dissident sur une autre question; 402 (le juge Gonthier, pour la majorité); *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Montréal (Ville)*, [2000] 1 R.C.S. 665

114 *Vrend* c. *Alberta*, [1998] 1 R.C.S. 493; *Colombie-Britannique (Public Service Employee Relations Commission)* c. *BCGSEU*, [1999] 3 R.C.S. 3; *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Montréal (Ville)*, [2000] 1 R.C.S. 665, 688; *Lac d'Amiante du Québec Ltée* c. *2858-0702 Québec Inc.*, [2001] 2 R.C.S. 743.

L'État peut législativement restreindre un droit garanti par la *Charte des droits et libertés de la personne*. Mais alors, il doit pouvoir justifier cette atteinte à un droit fondamental, en montrant que la mesure se justifie dans une société libre et démocratique, que les valeurs qui sous-tendent son intervention législative, et qui s'articulent autour de l'ordre public et le bien-être général des citoyens, doivent avoir préséance sur les droits énoncés dans la *Charte des droits et libertés de la personne*. Par exemple, la bonne administration de la justice peut aussi justifier que le droit à la vie privée soit restreint dans certains cas[115]. Une fois encore, cette disposition vise à confier aux tribunaux, en dernière analyse, la latitude voulue pour arbitrer les conflits de droits.

En ce qui concerne la protection de la vie privée, ce droit est garanti par divers articles de la *Charte des droits et libertés de la personne*. Ainsi, l'article 5 énonce :

> *Art. 5. Toute personne a droit au respect de sa vie privée.*

D'autres dispositions de la *Charte* québécoise assurent aussi le respect de volets spécifiques du droit à la vie privée. C'est le cas de l'article 6, qui assure la jouissance paisible des biens[116], de l'article 7, qui protège l'inviolabilité de la demeure[117], et de l'article 4, qui assure à chaque personne le droit à la sauvegarde de sa dignité, de son honneur et de sa réputation[118]. Récemment, la Cour d'appel du Québec a toutefois insisté sur le caractère distinct des droits apparaissant aux articles 4 et 5 de la *Charte* québécoise[119]. D'autres dispositions, comme celles assurant le respect du secret professionnel, entreront aussi en ligne de compte dans la protection des renseignements personnels.

Le droit à la protection de la vie privée est aussi consacré à l'article 35 du *Code civil du Québec*[120]. Cet article dispose que :

> *35. Toute personne a droit au respect de sa réputation et de sa vie privée.*
>
> *Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise.*

Par ailleurs, des dispositions de la *Charte* peuvent entrer en concurrence ou limiter les garanties dont disposent les attentes raisonnables en matière de vie privée. C'est le cas de l'article 2, qui

---

115 *Raymond, Chabot, SST Inc.* c. *Groupe AST (1993) Inc.*, [2002] R.J.Q. 2715 (C.A.).

116 L'article 6 énonce : *Toute personne a droit à la jouissance paisible et à la libre disposition de ses biens, sauf dans la mesure prévue par la loi.*

117 L'article 7 se lit ainsi : *La demeure est inviolable.*

118 L'article 4 dispose : *Toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation.* Voir *Bergeron* c. *Saint-Aubin*, J.E. 2002-2153 (C.Q.). Voir aussi les arrêts *Aubry* c.*Éditions Vice-Versa Inc.* , [1998] 1 R.C.S. 591 et *Falcon* c. *Cournoyer*, [2000] A.J.D.Q. 3093 (C.S.).

119 *Journal de Québec (Le), division de Communications Quebecor Inc.* c. *Beaulieu-Marquis*, J.E. 2002-1722, AZ-50143036.

120 L.Q. 1991, c. 64.

assure le droit au secours[121], de l'article 35, qui assure à tout accusé le droit à une défense pleine et entière[122], et de l'article 44, qui affirme le droit à l'information[123].

4.1 L'étendue de la protection

Pour cerner l'étendue de la protection résultant du droit à la vie privée, il faut considérer les éléments d'information protégés par le droit de même que les limites découlant d'autres intérêts qui doivent forcément être pris en compte dans un univers juridique où sont garantis une pluralité de droits pouvant parfois se contredire.

4.1.1 Les éléments protégés

La protection offerte par la *Charte des droits et libertés de la personne* et par le *Code civil du Québec* concerne plusieurs volets du droit à la vie privée.

La jurisprudence civile ayant examiné le droit à la vie privée a statué qu'il s'agit d'un droit de la personnalité et qu'il se divise en deux principales composantes. Il y aurait d'abord le droit à la solitude et au respect de son intimité. Le droit à la protection du domicile ferait partie de cette composante. La deuxième composante serait le droit à l'anonymat[124].

Il faut donner une interprétation large et libérale au droit à la vie privée protégé par la *Charte des droits et libertés de la personne* et le *Code civil du Québec*, et une interprétation étroite et restrictive des dispositions qui y portent atteinte[125].

Par ailleurs, le droit à la vie privée protégé par la *Charte des droits et libertés de la personne* et par le *Code civil du Québec* touche autant les sociétés et personnes morales que les personnes physiques[126]. Toutefois, il semble bien que la protection des attentes légitimes de vie privée des sociétés soit moins étendue que celle des personnes physiques. Ainsi, il fut considéré « qu'il était loin d'être évident » que la publication d'une adresse de courrier électronique d'un dirigeant de

---

121 L'article 2 énonce : *Tout être humain dont la vie est en péril a droit au secours.*

Toute personne doit porter secours à celui dont la vie est en péril, personnellement ou en obtenant du secours, en lui apportant l'aide physique nécessaire ou immédiate, à moins d'un risque pour elle ou pour les tiers ou d'un autre motif raisonnable.

122 L'article 35 est ainsi formulé : *Tout accusé a droit à une défense pleine et entière et a le droit d'interroger et de contre-interroger les témoins.*

123 L'article 44 dispose : *Toute personne a droit à l'information, dans la mesure prévue par la loi.*

124 Sur ces questions, *Thomas* c. *Publications Photo-police Inc.*, [1997] R.J.Q. 2321 (C.Q.*); Courtemanche* c. *Société Radio-Canada,* [1999] A.J.D.Q. 760 (C.S.).

125 *Lirette* c. *M. (C.)*, [1997] R.J.Q. 1794 (C.Q.); *Tellier* c. *De Michele et al*, [2000] R.J.Q. 2012 (C.S.).

126 *Payette* c. *Beaulieu*, [1994] A.J.D.Q. 2783 (C.S.); *Jardins du Mont Inc.* c. *Provigo distribution Inc.*, [1994] A.J.D.Q. 2243 (C.S.); *Tobin* c. *De Lanauze*, [2000] R.J.Q. 2596 (C.S.); *Leblanc* c. *Turpin*, [2001] A.J.D.Q. 3569 (C.S.).

société constituait une attente à la vie privée[127]. Rappelons aussi que les sociétés qui agissent dans un domaine réglementé ont forcément des attentes en matière de vie privée plus limitées[128]. La *Charte des droits et libertés de la personne* du Québec ne s'applique toutefois pas à une entreprise relevant de la juridiction fédérale[129].

Le contexte est un élément important pour saisir le niveau de protection offert par la *Charte des droits et libertés de la personne*. La nature des renseignements qu'on veut protéger, l'endroit où ils se trouvent, les attentes subjectives en matière de vie privée, etc., constituent des facteurs pertinents pour juger du degré de protection dont jouissent les renseignements personnels[130]. De même, il est clair que la protection à l'égard de documents ou de renseignements qui ont déjà été révélés publiquement sera beaucoup moins importante, si tant est qu'elle existe encore[131].

En matière civile, une violation du droit à la vie privée peut entraîner l'obligation de compenser ou de réparer financièrement le préjudice subi[132]. Il en est ainsi d'une attitude négligente ou non-sécuritaire à l'égard de la protection des renseignements personnels[133]. Des dommages punitifs pourront même être accordés en cas de violation intentionnelle ou délibérée des obligations en matière de vie privée.

La protection du domicile constitue l'un des volets les plus importants de la protection de la vie privée assurée par la *Charte des droits et libertés de la personne* et par les dispositions de l'article 35 du *Code civil du Québec*. Le domicile jouit donc d'un très haut degré de protection[134]. Un représentant de l'État ne peut forcer l'entrée du domicile d'une personne qu'avec l'accord d'un juge ou seulement quand la vie ou la sécurité de la personne est menacée, à défaut de quoi on considérera qu'il y a violation du droit à la vie privée[135], cette obligation s'étend aussi aux personnes privées. Ainsi, un locateur ne peut agir de façon telle que cela constituerait une atteinte au droit à la vie privée de ses locataires[136]. Le locateur a aussi droit au respect de sa vie privée, à l'égard des activités de ses locataires[137]. Un certain nombre d'arrêts des tribunaux concernent aussi les troubles de voisinage. Une personne ne peut agir à l'égard de son voisin de manière à porter atteinte à sa vie privée. Elle ne peut donc procéder à la surveillance continue des voisins,

---

127 *Wyeth-Ayert Canada Inc*. c. *Phaneuf*, [2002] R.J.Q. 949 (C.S.).

128 *Supra*, Onglet III.

129 *Kealty* c. *Société internationale de télécommunications aéronautique (Sita) Inc*., [1991] R.J.Q. 397 (C.S.).

130 *Srivastava* c. *Hindu Mission of Canada (Québec) Inc*., [2001] A.J.D.Q. 2866 (C.A.).

131 *Tobin* c. *De Lanauze*, [2000] R.J.Q. 2596 (C.S.).

132 *R. (H.)* c. *B. (G.)*, [1998] R.J.Q. 3065 (C.S.).

133 *Stacey* c. *Sauvé Plymouth Chrysler (1991) Inc*., [2002] R.J.Q. 1779 (C.Q.).

134 *Samson* c. *Québec (Procureur général)*, [2000] A.J.D.Q. 3097 (C.Q.); *Syndicat canadien de la fonction publique, section 302* c. *Verdun (Ville)*, [2000] A.J.D.Q. 3403 (C.A.).

135 *R*. c. *Trépanier*, [1988] R.J.Q. 607 (C.M. de Montréal); *R*. c. *Feeney*, [1997] 2 R.C.S. 13.

136 *Béchard* c. *Desjardins*, [1992] A.J.D.Q. 1586 (C.Q.); *Commission des droits de la personne du Québec* c. *S. (G.)*, J.E. 94-252 (T.D.P.Q.).

137 *Cheung* c. *Québec (Procureur général)*, [2001] A.J.D.Q. 1336 (C.S.).

limiter leur vision, empiéter sur leur propriété, etc.[138]. Une personne ne peut entrer sur une propriété dans le but de filmer ou de photographier une maison sans violer le droit à la vie privée du propriétaire de cette maison[139]. La question de la prise de photos ou le tournage d'un vidéo à l'insu d'une personne, alors qu'elle se trouve dans sa propriété, mais alors les scènes captées peuvent l'être sans entrer sur la propriété ou violer son domicile et que des raisons sérieuses justifient l'utilisation de ces procédés est cependant plus controversée[140]. Retenons toutefois que, de façon générale, une personne ne peut pas entrer sur la propriété d'autrui ou dans son domicile, alors qu'elle n'y est pas invitée, sans violer le droit à la vie privée de cette personne. Il en est de même d'un employeur à l'égard du domicile de ses salariés[141]. Un officier public, agissant sans mandat valide, viole aussi le droit à la vie privée des personnes, s'il pénètre dans leur domicile sans droit ou sous un faux prétexte[142]. Si les municipalités peuvent validement adopter des règlements qui limitent le droit de propriété, au nom de la sécurité de tous[143] ou pour voir à la vérification de l'application des règlements municipaux[144], ils ne peuvent aller jusqu'à barricader et interdire l'accès à cette propriété[145].

Les règlements municipaux qui interdisent la sollicitation, au nom du respect de la vie privée, ne peuvent s'appliquer dans les cas de sollicitations à des fins religieuses ou d'évangélisation[146]. On a aussi jugé que le piquetage secondaire illégal fait devant une résidence constitue une violation du droit à la vie privée[147]. Mais si le choix du lieu de sa résidence constitue une composante du

---

138 Pour des exemples de ces situations, consulter *Maheux c. Boutin*, [1996] A.J.D.Q. 288 (C.Q.); *Côté* c. *Auclair*, [1996] A.J.D.Q. 288 (C.S.); *Gauthier* c. *Roy*, [1999] A.J.D.Q. 221; *M. (M.)* c. *V. (S.)*, [1999] A.J.D.Q. 759 (C.S.).

139 *Courtemanche* c. *Société Radio-Canada*, [1999] A.J.D.Q. 760 (C.S.); *Société Radio-Canada* c. *Courtemanche*, [1999] A.J.D.Q. 761 (C.A.).

140 Sur cette question, voir: *Ville de Mascouche* c. *Houle*, [1999] R.J.Q. 1894 (C.A.); *Syndicat des travailleurs et travailleuses de Bridgestone (C.S.N.)* c. *Trudeau*, [1999] R.J.Q. 2229 (C.A.); *Syndicat des travailleuses et travailleurs de l'abattoir de volailles de Saint-Jean-Baptiste* c. *Corriveau*, [1999] R.J.Q. 2065; *Éppelé* c. *CSST*, [2000] C.A.I. 194; *Lacombe* c. *April (Succession d')*, [2002] R.J.Q. 2335 (C.S.).

141 *Marcotte* c. *Maison Lacouline Inc.*, [2000] A.J.D.Q. 3463 (C.S.).

142 *Palacios* c. *Côté*, [1996] A.J.D.Q. 3803 (C.Q.); *Bélisle* c. *Dion*, [1999] A.J.D.Q. 3031 (C.Q.); *Gagnon-Paquette* c. *Paquette*, [1999] A.J.D.Q. 2596 (C.S.).

143 *Dorval (Ville)* c. *Provost*, [1994] A.J.D.Q. 1671 (C.A.); *Mercier (Ville de)* c. *Fortin*, [1996] A.J.D.Q. 1830 (C.S.)

144 *Saint-Raymond (Ville)* c. *Plamondon*, [2001] A.J.D.Q. 2456 (C.S.).

145 *Oxford (Municipalité du canton d')* c. *Ferland*, [1996] A.J.D.Q. 861 (C.S.).

146 *Beauchemin* c. *Blainville (Ville)*, [2001] A.J.D.Q. 1809 (C.S.).

147 *Journal de Montréal, division du groupe Quebecor Inc.* c. *Syndicat canadien des communications, de l'énergie et du papier, section locale 4545*, [1994] A.J.D.Q. 3251 (C.S.).

droit à la vie privée[148], la notion de vie privée ne va pas jusqu'à interdire des transformations du cadre municipal par le législateur[149].

La notion de domicile doit aussi être mise en contexte pour établir l'étendue de la protection offerte. Ainsi, la jurisprudence a confirmé qu'un domicile peut constituer un lieu public pour le temps d'une réunion, ce qui réduit de façon considérable les attentes légitimes de vie privée dans un tel contexte[150].

Évidemment, le droit à la vie privée, surtout en matière civile, comprend aussi le droit à l'image et à la protection de sa voix[151], même si cette protection, comme nous le verrons, peut être moins importante dans un contexte judiciaire.

Le droit à la protection de la vie privée s'étend aussi à la correspondance d'une personne[152]. Une personne ne peut toutefois diffamer une autre personne dans sa correspondance privée ou publique (lettre aux médias, par exemple) ou dans ses propos privés ou publics sans engager sa responsabilité[153].

Mentionnons encore le droit à la confidentialité de son orientation sexuelle ou le droit de ne pas voir son orientation sexuelle ridiculisée publiquement[154]. Le harcèlement sexuel[155] et les

---

148 *Brasserie Labatt Ltd*. c. *Villa*, [1995] R.J.Q. 73 (C.A.); *Godbout c. Longueuil (Ville)*,[1997] 3 R.C.S. 844; *Dion* c. *Régie intermunicipale d'assainissement des eaux de Sainte-Thérèse et Blainville*, [1998] R.J.Q. 2731 (C.S.); *Rioux* c. *Rivière-du-Loup (Ville)*, [1999] A.J.D.Q. 773 (C.Q.).

149 *Westmount (Ville de)* c. *Québec (Procureur général)*, [2001] A.J.D.Q. 1822 (C.A.).

150 *Commission des droits de la personne et des droits de la jeunesse* c. *Bertrand*, [2001] R.J.Q. 1684 (T.D.P.Q.).

151 Sur cette question, voir: *Deschamps* c. *Renault Canada* [1977] A.J.Q. 1230 (C.S.); *Bagajewicz* c. *Sony of Canada Ltd*., [1995] A.J.D.Q. 656 (C.S.); *Aubry* c. *Vice-Versa*, [1998] 1 R.C.S. 591; *Pilon* c. *Saint-Pierre*, [1999] R.J.Q. 1825 (C.Q.); *Malo* c. *Laoun*, [2000] A.J.D.Q. 3095 (C.S.); *Beaulieu-Marquis* c. *Journal de Québec, division de Communications Quebecor Inc*., [2000] A.J.D.Q. 3094 (C.Q.); *J.L.* c. *S.B*., [2000] A.J.D.Q. 748 (C.S.); *176100 Canada Inc*. c. *Réseau des Appalaches FM Ltée*, [2001] R.J.Q. 1011 (C.S.); *Journal de Québec (Le), division de Communications Quebecor Inc*. c. *Beaulieu-Marquis*, J.E. 2002-1722, AZ-5014303 (C.A.); *Brisson* c. *Virtually Magazine*, J.E. 2002-1362, AZ-50135810 (C.S.).

152 *Droit de la famille –2181*, [1995] A.J.D.Q. 2339 (C.S.); *Gilles E. Néron Communication marketing Inc.,* c. *Chambre des notaires du Québec*, [2000] A.J.D.Q. 3092 (C.S.).

153 *Dumas* c. *Dauphin*, [1993] A.J.D.Q. 2805 (C.Q.); *Groupe R.C.M. Inc. c.Morin*, [1996] A.J.D.Q. 3783 (C.S.*); R. (H.)* c. *B. (G.)*, [1998] R.J.Q. 3065 (C.S.); *Marcotte* c. *Maison Lacouline Inc*., [2000]A.J.D.Q. 3463 (C.S.); *Falcon* c. *Cournoyer*, [2000] A.J.D.Q. 3093 (C.S.).

154 *Commission des droits de la personne et des droits de la jeunesse* c. *Michaud*, [1998] A.J.D.Q. 623 (T.D.P.Q.*); R. (H.)* c. *B. (G.)*, [1998] R.J.Q. 3065 (C.S.); *Commission des droits de la personne et des droits de la jeunesse* c. *Poulin*, [2001] A.J.D.Q. 712 (T.D.P.Q.). Dans l'affaire *Commission des droits de la personne et des droits de la jeunesse* c. *140998 Canada Inc*, J.E. 2002-1901 (T.D.P.Q.), le tribunal a préféré rattacher cette question au droit à la dignité.

155 *Jackson* c. *Bousquet*, [1996] A.J.D.Q. 745 (T.D.P.Q.); *Commission des droits de la personne et des droits de la jeunesse* c. *Virages santé mentales Inc*., [1998] A.J.D.Q. 620 (T.D.P.Q.).

agressions du même type[156] ont aussi été considérés comme des atteintes à la vie privée; certaines décisions ont plutôt rattaché cette protection au droit à la dignité de la personne[157].

Rappelons finalement que les attentes en matière de vie privée, associées à l'utilisation d'un téléphone, sont généralement très élevées, et ce, peu importe qu'il s'agisse d'un téléphone traditionnel ou d'un téléphone cellulaire. Ces attentes sont cependant moindres s'il s'agit d'un appareil situé dans les locaux de son employeur et qui sert à des fins liées à son emploi[158]. L'enregistrement de ses propres conversations téléphoniques ne constituera généralement pas une atteinte à la vie privée de la personne au détriment de qui cet enregistrement est réalisé, surtout en matière commerciale, avec un employeur, ou dans d'autres situations de ce type. Le procédé, quoique jugé inélégant, ne sera pas illégal et la preuve ainsi obtenue sera généralement admissible. À cet égard, l'introduction de l'article 35 du *Code civil du Québec* n'a pas changé le droit sur cette question[159].

Les renseignements sur la situation financière d'une personne sont aussi protégés par l'article 5 de la *Charte des droits et libertés de la personne* du Québec[160].

En matière commerciale, d'un point de vue civil comme d'un point de vue criminel ou administratif, l'attente en matière de vie privée est forcément moindre, surtout si les renseignements sont logés dans un lieu public[161]. Toutefois, il faut, une fois encore, mettre en contexte l'examen de cette question. Dans le domaine civil, la jurisprudence reconnaît que les procédures ne sont pas assujetties à des exigences aussi élevées qu'en matière criminelle, même si le droit à la vie privée est en cause[162]. Toutefois, le bureau d'un professionnel soumis aux obligations de secret professionnel, bénéficie d'un très haut niveau de protection des attentes en matière de vie privée[163].

---

156 *Larocque* c. *Côté*, [1996] R.J.Q. 1930 (C.S.).

157 *Commission des droits de la personne et des droits de la jeunesse* c. *Stiridis*, J.E. 2002-1208 (T.D.P.Q.).

158 Sur ces questions, voir: *R.* c. *Salomon*, [1996] R.J.Q. 1789 (C.A.); *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, [2001] A.J.D.Q. 2866 (C.A.).

159 Pour un aperçu de l'important contentieux que cette question a soulevé, voir: *Cadieux c. Le service de gaz naturel Laval Inc.*, [1991] R.J.Q. 2490 (C.A.); *Roy* c. *Saulnier*, [1992] R.J.Q. 2419 (C.A.); *167782 Canada Inc.* c. *Tenneco Canada Inc.*, [1994] A.J.D.Q. 392 (C.S.); *Droit de la famille –2206*, [1995] R.J.Q. 1419 (C.S.); *Compagnie d'assurances Standard Life* c. *Rouleau*, [1995] R.J.Q. 1407 (C.S.); *Wilson* c. *Bano*, [1995] R.J.Q. 787 (C.S.); *Droit de la famille –2474*, [1996] A.J.D.Q. 1078 (C.S.); *Commission des droits de la personne* c. *Systèmes internationaux de fret Dillon Reid Inc.*, [1996] A.J.D.Q. 733 (T.D.P.Q.); *Thibodeau* c. *Commission municipale du Québec*, [1996] R.J.Q. 1217 (C.S.); *Sept-Îles (Ville)* c. *Thibodeau*, [1997] R.J.Q. 2903 (C.A.); *Sejko* c. *Gabriel André Inc.*, [1999] A.J.D.Q. 2960 (C.Q.).

160 *Droit de la famille –2650*, [1997] R.J.Q. 1418 (C.S.).

161 *Comité paritaire de l'industrie de la chemise c. Potash*, [1994] 2 R.C.S. 406; 143471 *Canada Inc.* c. *Québec (Procureur général)*, [1994] 2 R.C.S. 339; *R.* c. *Salomon*, [1996] R.J.Q. 1789 (C.A.); *R.* c. *Morin*, [1996] R.J.Q. 1758 (C.Q.).

162 *Raymond Chabot SST Inc.* c. *Groupe AST (1993) Inc.*, [2002] R.J.Q. 2715 (C.A.); *Julien* c. *Québec Métal Recyclé (F.N.F.) Inc.*, [2002] R.J.Q. 1079 (C.S.).

163 *Leblanc* c. *Maranda*, [2001] R.J.Q. 2490 (C.A.).

Quant aux conséquences de l'introduction de l'article 35 du *Code civil du Québec*, rappelons que les tribunaux ont insisté sur la nécessité que l'interprétation de cette disposition se fasse à la lumière de la *Charte des droits et libertés de la personne*[164]. On peut donc considérer que la protection de la vie privée est confirmée et renforcée par l'adoption de ces dispositions[165].

4.1.2 Les limites découlant d'autres intérêts

Les tribunaux devront, à l'occasion, arbitrer entre des valeurs et droits contradictoires, et la protection de la vie privée doit donc parfois céder le pas à des droits ou des valeurs considérés prééminents ou primordiaux. Parmi les valeurs et droits souvent considérés prioritaires, mentionnons :

- Les intérêts de l'enfant[166].

- Les droits des salariés par rapport à ceux des usagers, en matière de sexualisation des postes de travail, par exemple[167].

- L'obligation de transparence en matière de procédures policières ou judiciaires[168] ou pour assurer la bonne administration de la justice[169]; toutefois, cette obligation de transparence peut parfois céder le pas à la nécessaire confidentialité de renseignements au bénéfice de la protection des jurés[170] ou de la personne agressée sexuellement[171], surtout dans les phases

---

164 *Lac d'Amiante du Québec Ltée*. c. *2858-0702 Québec Inc*., [2001] 2 R.C.S. 743.

165 *Godbout* c. *Longueuil (Ville)*, [1995] R.J.Q. 2561 (C.A.).

166 Pour des exemples de ces déterminations, voir *Protection des droits de la jeunesse –116*, [1984] A.J.Q. 1294 (T.J.); *Protection de la jeunesse –174*, [1985] A.J.Q. 1472 (T.J.); *Protection de la jeunesse –182*, [1986] A.J.Q. 2127 (C.S.); *Protection des droits de la jeunesse*, [1993] A.J.D.Q. 1116 (C.Q.); *Droit de la famille –2206*, [1995] R.J.Q. 1419 (C.S.); *Protection de la jeunesse –2474*, [1996] A.J.D.Q. 1078 (C.S.); *Protection de la jeunesse –808*, [1996] A.J.D.Q. 1240 (C.Q.).

167 *Dufour* c. *Centre hospitalier Saint-Joseph-de-la-Malbaie*, [1992] A.J.D.Q. 604 (T.D.P.Q.); *Commission des droits de la personne* c. *Centre d'accueil Villa-Plaisance*, [1996] A.J.D.Q. 741 (T.D.P.Q.).

168 *Duquette* c. *Sainte-Thérèse (Corporation municipale de la ville de)*, [1988] R.J.Q. 961 (C.A.); *Naessens* c. *Québec (Procureur général)*, [1992] A.J.D.Q. 2875 (C.S.); *Caron* c. *Publications Photo-police Inc*., [1993] A.J.D.Q. 2802 (C.S.).

169 *Sierra Club du Canada* c. *Canada (Ministre des finances)*, [2002] 2 R.C.S. 522; *Raymond Chabot SST Inc*. c. *Groupe AST (1993) Inc*, [2002] R.J.Q. 2715 (C.A.); *Julien* c. *Québec Métal Recyclé (F.N.F.) Inc*., [2002] R.J.Q. 1079 (C.S.).

170 *R*. c. *Sabourin*, [1999] A.J.D.Q. 2248 (C.S.).

171 *D. (J.L.)* c. *Vallée*, [1996] R.J.Q. 2480 (C.A.); *Commission des droits de la personne et des droits de la jeunesse* c. *Montréal (C.U.M.)*, [2000] A.J.D.Q. 941.

antérieures au procès lui-même[172]. Une personne ne peut non plus profiter de l'existence de procédures judiciaires pour diffamer l'autre partie[173].

- L'application régulière des lois générales, eu égard à la protection des intérêts privés et spécifiques[174], et les intérêts de l'État de vérifier l'admissibilité des personnes à des prestations sociales[175].

- L'intérêt public rattaché à l'existence d'une fonction publique neutre et impartiale l'emporte sur le droit du fonctionnaire de prendre, en plus de son emploi, des contrats privés en invoquant son droit à la vie privée[176].

- La sécurité nationale peut aussi justifier des atteintes à la vie privée[177].

- Le droit du public à l'information peut parfois prévaloir sur le droit à la vie privée des personnes[178]. Ainsi, le droit du public à l'information l'emportera généralement sur le droit à la vie privée des personnes exerçant une fonction élective et publique[179]. Toutefois, il ne faut pas confondre la curiosité malsaine et le mauvais goût avec l'intérêt public à avoir accès aux informations[180]. Cela ne veut pas dire que les personnes publiques n'ont pas droit au respect de leur propriété privée, comme composante de leur droit à la vie privée[181].

---

172 *Lac d'Amiante du Québec Ltée* c. *2858-0702 Québec Inc*, [2001] 2 R.C.S. 743.

173 *Droit de la famille –1936*, [1994] A.J.D.Q. 2353 (C.Q.); *Lecours* c. *Desjardins*, [1999] R.R.A. 865 (C.S.); *Théorêt* c. *K.M. Construction Inc,* [1999] R.R.A. 846 (C.S.)*; Programmed Communication Ltd.* c. *Ludgate,* [1999] R.R.A. 187 (C.S.); *French* c. *Groupe Quebecor Inc.*, [1999] A.J.D.Q. 2949 (C.S.); *Belisle-Heurtel* c. *Tardif*, [2000] R.J.Q. 2391 (C.S.); *Laliberté* c. *Guinta*, [2000] R.R.A. 498 (C.S.); 9078-0669 *Québec Inc.* c. *Gravel*, [2001] R.J.Q. 1669 (C.A.); *Corriveau* c. *Speer*, [2001] R.R.A. 1044 (C.S.); *D'Amour* c. *157569 Canada Ltée*, [2001] R.R.A. 1071 (C.S.); *Marquis* c. *Auxilium technologies Inc.*, [2001] R.R.A. 1051 (C.S.); *Setym International Inc.* c. *Belout*, [2001] R.R.A. 1048 (C.S.); *Entreprises Sompro Inc.* c. *Serge Bruyère Inc.*, [2001] R.R.A. 1044 (C.S.); *Gauthier* c. *Gauthier*, J.E. 2002-870 (C.S.); *Bernier* c. *Beauregard*, J.E. 2002-2046 (C.Q.).

174 *Slatery (Syndic de) c. Slatery*, [1993] 3 R.C.S. 430. Voir aussi la jurisprudence en matière de règlements municipaux.

175 *Smith* c. *Canada (Procureur général)*, [2001] 3 R.C.S. 902; *Charest* c. *Tribunal administratif du Québec*, J.E. 2002-628, AZ-50110836 (C.S.).

176 *Dubé* c. *Québec (Procureur général)*, [1999] A.J.D.Q. 3566 (C.S.).

177 *Ruby* c. *Canada (Solliciteur général*), [2002] 4 R.C.S. 3.

178 *Rouleau* c. *Groupe Quebecor Inc.*, [1992] A.J.D.Q. 2890 (C.S.); *Aubry* c. *Vice-versa*, [1998] 1 R.C.S. 591; *Beaulieu-Marquis* c. *Journal de Québec, division de Communications Quebecor Inc.*, [2000] A.J.D.Q. 3094 (C.Q.).

179 *Desrosiers* c. *Groupe Quebecor Inc.*, [1994] A.J.D.Q. 2773 (C.S.); *Bourque* c. *Saint-Romuald (Ville de) et autres*, [2000] R.J.Q. 546 (C.Q.); *Société Saint-Jean-Baptiste* c. *Hervieux-Payette*, [2002] R.J.Q. 1669 (C.A.); *Société Radio-Canada* c. *Guitoni*, [2002] R.J.Q. 2691 (C.A.).

180 *Thomas* c. *Publications Photo-Police Inc.*, [1997] R.J.Q. 2321 (C.Q.).

181 *Syndicat canadien de la fonction publique, section 302* c. *Verdun (Ville de)*, [2000] A.J.D.Q. 3403 (C.A.).

4.2 La protection des renseignements personnels et de la vie privée dans les environnements technologiques

Le recours aux technologies de l'information peut accentuer les risques de divulgation d'informations relatives aux personnes. Afin d'assurer la protection de la vie privée et de la dignité des personnes, lors de transactions réalisées au moyen de documents technologiques, la *Loi sur le cadre juridique des technologies de l'information* a prévu des dispositions pour garantir la protection et la confidentialité des renseignements personnels. Ces dispositions viennent compléter les exigences des lois générales relatives à la protection des renseignements personnels.

La *Loi* vise à organiser la protection de la vie privée dans le cycle de gestion des documents technologiques. Elle prévoit, à cette fin, les conditions d'utilisation des moyens susceptibles d'assurer le caractère confidentiel de documents.

Ainsi, il faut, lors de chaque phase du cycle de vie d'un document, prendre les précautions de nature à garantir la protection des renseignements personnels.

- La protection des renseignements personnels et confidentiels doit être assurée avant de détruire un document, dont la loi exige la conservation et qui a fait l'objet d'un transfert de support (article 20, paragraphe 2°).

- La consultation de documents publics comportant des renseignements personnels est limitée à ce qui est nécessaire afin d'assurer le respect de la finalité pour laquelle ces documents sont rendus publics. L'article 24 impose des restrictions aux fonctions de recherche extensive dans les banques de données publiques, afin de protéger la vie privée. On veut ainsi éviter, par exemple, les consultations de banques de données à l'aide de moteurs de recherche qui viseraient à repérer des renseignements personnels pour des fins autres que celles pour lesquelles ils ont été recueillis ou diffusés.

- La consultation de documents technologiques qui portent des renseignements confidentiels est également entourée de protection; la personne responsable de l'accès à ces documents doit prendre des mesures de sécurité propres à en assurer la confidentialité (article 25).

- La protection de la confidentialité d'un document technologique doit être maintenue, y compris dans un contexte où la garde du document est confiée à un prestataire de services (article 26).

- De même, les renseignements déclarés confidentiels par la loi doivent être protégés en cours de transmission d'un document, y compris sur les réseaux de communication, et ce, par un moyen approprié au mode de transmission retenu (article 34).

Des balises sont aussi édictées à l'égard de l'usage de mécanismes d'identification et de vérification de l'identité.

- Ces opérations doivent être accomplies dans le respect des lois (article 40, alinéa 2).

- Les renseignements personnels contenus dans un document ou un certificat confirmant l'identité d'une personne ou l'identification d'une association, d'une société ou de l'État doivent être protégés lors de sa transmission (article 40, alinéa 1).

- Un document technologique servant à identifier une personne doit être protégé contre l'interception rendant possible l'usurpation de l'identité de la personne visée, lorsqu'il est conservé ou transmis sur un réseau de communication. De même, sa confidentialité doit être assurée, et sa consultation journalisée (article 41).

- Il est interdit d'exiger que l'identité d'une personne soit établie au moyen d'un dispositif qui porte atteinte à son intégrité physique (article 43).

- Il est interdit d'exiger qu'une personne soit liée à un dispositif qui permet de la retracer, sauf si la loi le permet expressément en vue de protéger la santé des personnes ou la sécurité publique (article 43).

- Des contrôles sont prescrits pour l'utilisation des caractéristiques ou des mesures biométriques servant à identifier une personne (exemple : par l'empreinte digitale ou de l'iris). L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance. Les autres informations générées par des procédés biométriques ne peuvent être utilisées ni communiquées à d'autres que l'intéressé. La CAI se voit confier un droit de contrôler *a priori* et *a posteriori* les banques de caractéristiques et de mesures biométriques (articles 44 et 45).

Enfin, l'activité de certification comporte spécifiquement certaines mesures de protection de la vie privée et de contrôle de l'accès à de l'information jugée sensible.

- L'obtention de renseignements relatifs aux attributs d'une personne, et qui sont établis dans un certificat, n'est pas automatique. L'accès à ce certificat doit être autorisé par la personne concernée ou par une personne en autorité par rapport à elle (article 47, dernier alinéa).

- De même, le motif d'annulation ou de suspension d'un certificat ne doit pas être accessible par le répertoire; il ne peut l'être que sur autorisation de la personne qui l'a suspendu ou annulé (article 50, dernier alinéa). En effet, un certificat peut être annulé ou suspendu pour des raisons confidentielles ou pouvant porter atteinte à la réputation de la personne.

- L'usage d'un pseudonyme, au lieu du nom distinctif, est possible dans le cas de l'utilisation d'un certificat confirmant l'identité d'une personne physique, et ce, afin de préserver l'anonymat des personnes (article 48, dernier alinéa).

- La *Loi* oblige le prestataire de services de certification ou de répertoire, au moyen de l'énoncé de politique, d'informer les usagers, entre autres, sur sa politique de protection de la confidentialité des renseignements personnels reçus ou communiqués par lui (article 52, premier alinéa, paragraphe 7°).

- La *Loi* impose des obligations relativement à l'élément secret d'un dispositif qui permet d'identifier, de localiser ou d'indiquer un attribut d'une personne (par exemple, la clé privée

en matière de signature électronique). Le titulaire du dispositif doit en assurer la confidentialité et faire en sorte que le dispositif ne soit pas utilisé sans son autorisation. Le prestataire de services de certification, quant à lui, doit transmettre l'élément secret du dispositif de manière à ce que seul le titulaire visé en prenne connaissance et le reçoive. Ces obligations visent, entre autres, à éviter les conséquences d'une usurpation d'identité (article 57). L'article 58 vient préciser les obligations du titulaire d'un dispositif, lorsque cet appareil a été volé ou perdu ou lorsque des données confidentielles ont été compromises.

5. La protection des renseignements personnels selon la *Loi sur l'accès*

L'article 54 de la *Loi sur l'accès* définit la notion de renseignement personnel comme étant ceux qui concernent une personne physique et permettent de l'identifier. L'article 56 précise que le nom d'une personne n'est pas en soi un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement concernant cette personne ou lorsque la seule mention du nom de la personne révèlerait un renseignement nominatif concernant cette personne.

5.1 Le principe général de la protection des renseignements personnels

Les renseignements personnels sont confidentiels, sous réserve du consentement de la personne concernée à leur divulgation ou si cette divulgation concerne des renseignements obtenus dans le cadre des fonctions d'adjudication d'un organisme exerçant des fonctions quasi judiciaires et siégeant en public. Telles sont les dispositions apparaissant à l'article 53 de la *Loi sur l'accès*.

L'article 59 de la *Loi* prévoit aussi un certain nombre de situations où la divulgation peut être réalisée sans le consentement de la personne concernée. Toutefois, la jurisprudence a insisté sur l'interprétation restrictive devant être faite de ces dispositions, compte tenu qu'il s'agit d'exceptions au principe de la confidentialité des renseignements personnels. Par ailleurs, l'établissement ou l'organisme dispose d'un pouvoir discrétionnaire de divulguer ou non les renseignements en cause, puisqu'il s'agit d'une disposition facultative[182].

Ainsi, on a jugé que la lettre de démission d'un médecin adressée à un établissement ne saurait être divulguée sans l'accord du professionnel concerné. La personne qui a entrepris des procédures devant un organisme quasi judiciaire doit donc s'adresser à cet organisme pour obtenir une ordonnance de divulgation d'un tel renseignement, la CAI n'étant pas alors le tribunal compétent pour disposer de cette demande[183].

De même, un établissement ne saurait transmettre à un syndicat une liste de salariés comprenant outre les noms de ces personnes, leur prénom, leur adresse, leur date d'entrée en fonction, les services où ils oeuvrent, leur titre d'emploi, leur salaire, leur numéro d'assurance sociale, leur numéro de salarié dans l'établissement, leur statut et leur ancienneté dans l'établissement, alors que ces salariés sont couverts par un autre certificat d'accréditation et représentés par un autre syndicat, car il s'agit de renseignements nominatifs[184].

---

182 *Syndicat des travailleurs et travailleuses du Centre d'accueil Émilie Gamelin et de la Résidence Armand Lavergne* c. *Centre d'accueil Émilie Gamelin*, [1989] C.A.I. 410 (C.Q.) (Évocation rejetée par la Cour supérieure et par la Cour d'appel).

183 *Desrochers* c. *Centre hospitalier Robert-Giffard*, CAI, 29 avril 2002, Hélène Grenier.

184 *Dubé* c. *Centre hospitalier universitaire de Québec*, C.A.I., 15 mars 2002, Christiane Constant, Jennifer Stoddart et Michel Laporte.

Selon la jurisprudence de la CAI, les renseignements recueillis par une personne dans le cadre de ses fonctions ne constituent pas des renseignements nominatifs sur cette personne, car une activité, un geste posé ou une opinion émise dans le cadre d'une fonction constituent le prolongement de la fonction en cause[185].

5.2 Les renseignements publics en vertu de l'article 57 de la *Loi sur l'accès*

L'article 55 de la *Loi* prévoit qu'un renseignement qui a un caractère public en vertu de la loi n'est pas soumis aux règles de protection des renseignements personnels prévus aux articles 53 à 102.1 de la *Loi sur l'accès*. Cependant, au termes du second alinéa de l'article 55, « un organisme public qui détient un fichier de tels renseignements peut en refuser l'accès, en tout ou en partie, ou n'en permettre que la consultation sur place si le responsable a des motifs raisonnables de croire que les renseignements seront utilisés à des fins illégitimes ».

Par cette disposition, le responsable de l'accès se voit conférer le pouvoir de porter des jugements de valeur au sujet de tout un ensemble possible d'usages d'informations qui ont un caractère public. Les informations à caractère public sont ainsi censurées au motif qu'il existe des risques — le plus souvent hypothétiques — que certaines d'entre elles soient utilisées de manière fautive.

Cette tendance s'observe aussi dans la *Loi concernant le cadre juridique des technologies de l'information*[186] qui impose un mécanisme de censure des documents publics comportant des données personnelles. L'article 24 de cette loi se lit comme suit :

> *L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des données personnelles et qui, pour une finalité particulière est rendu public, doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. Elle peut, en outre, eu égard aux critères élaborés en vertu du paragraphe 2° de l'article 68, fixer des conditions pour l'utilisation de ces fonctions de recherche.*

Cette disposition vise des informations qui ont un caractère public; elle ne concerne pas les renseignements à caractère privé. Elle permet de restreindre l'utilisation des fonctions de recherche extensive à l'égard des documents technologiques comportant des données personnelles et rendues publiques pour une finalité particulière. On veut ainsi éviter, par exemple, les consultations de banques de données à l'aide de moteurs de recherche afin de repérer des données personnelles pour des fins autres que celles pour lesquelles elles ont été recueillies ou diffusées.

L'article 57 de la *Loi sur l'accès* affirme, quant à lui, le caractère public de certains renseignements. Il est formulé ainsi :

---

185 *Giroux* c. *Centre d'accueil la Cité des Prairies Inc.*, [1993] C.A.I. 53.

186 *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1,

57. Les renseignements suivants ont un caractère public:

1° le nom, le titre, la fonction, la classification, le traitement, l'adresse et le numéro de téléphone du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction et, dans le cas d'un ministère, d'un sous-ministre, de ses adjoints et de son personnel d'encadrement;

2° le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification, y compris l'échelle de traitement rattachée à cette classification, d'un membre du personnel d'un organisme public;

3° un renseignement concernant une personne en sa qualité de partie à un contrat de services conclu avec un organisme public, ainsi que les conditions de ce contrat;

4° le nom et l'adresse d'une personne qui bénéficie d'un avantage économique conféré par un organisme public en vertu d'un pouvoir discrétionnaire et tout renseignement sur la nature de cet avantage;

5° le nom et l'adresse de l'établissement du titulaire d'un permis délivré par un organisme public et dont la détention est requise en vertu de la loi pour exercer une activité ou une profession ou pour exploiter un commerce.

Toutefois, les renseignements personnels prévus au premier alinéa n'ont pas un caractère public si leur divulgation est de nature à nuire ou à entraver le travail d'un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime. De même, les renseignements personnels visés aux paragraphes 3° et 4° du premier alinéa n'ont pas un caractère public dans la mesure où la communication de cette information révélerait un renseignement dont la communication doit ou peut être refusée en vertu de la section II du chapitre II.

En outre, les renseignements prévus au paragraphe 2° ne peuvent avoir pour effet de révéler le traitement d'un membre du personnel d'un organisme public.

5.3 La collecte, la conservation et l'utilisation des renseignements personnels

Les renseignements personnels bénéficient d'une protection lors de chacune des phases de leur cycle de vie. Ainsi, la collecte, la conservation et l'utilisation de ces renseignements sont assujettis à des conditions.

5.3.1 La nécessité de la collecte pour réaliser les finalités de l'organisme

L'article 64 de la *Loi sur l'accès* limite la capacité des organismes publics d'obtenir, de conserver ou d'utiliser des informations personnelles à ce qui est nécessaire pour réaliser les finalités qu'elles cherchent à accomplir. Cette disposition est ainsi formulée :

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

> *Un organisme public peut toutefois recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en oeuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.*
>
> *La collecte visée au deuxième alinéa s'effectue dans le cadre d'une entente écrite transmise à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission.*

Avant l'entrée en vigueur des modifications de 2006, la notion de nécessité avait reçu une interprétation restrictive de la part de la CAI. Ainsi, le terme « nécessaire » a le sens d'indispensable, d'obligatoire, de primordial ou de *sine qua non*[187]. Certes, par la suite, la CAI a admis le caractère évolutif de cette notion : ce qui n'était pas nécessaire à une époque donnée peut le devenir ultérieurement et vice-versa[188]. Il revient à l'organisme de démontrer cette nécessité[189].

Si la notion de nécessité a reçu une interprétation restrictive, la notion « d'attribution » propre à un organisme a fait lui l'objet d'une interprétation large et généreuse. Ainsi, on a jugé que si la mission ou l'attribution première d'un établissement du réseau de la santé est d'abord de prodiguer des soins ou d'offrir des services, il faut aussi examiner ces attributions non seulement par rapport au public, mais également à l'égard des salariés de l'établissement, ce qui permet de justifier l'existence de nombreuses fonctions administratives[190].

La notion de nécessité retenue par la Commission[191] et la Cour du Québec[192] dans des décisions d'adjudication ne renvoie pas à une condition *sine qua non* pour l'accomplissement des devoirs et fonctions de l'organisme. Il suffit d'établir que le renseignement est raisonnablement requis, compte tenu de l'ensemble des contraintes dans lesquelles évolue l'organisme. Raymond Doray et François Charette concluent de ces décisions que « serait nécessaire au sens de l'article 64, un renseignement requis pour répondre aux besoins de l'organisme, c'est-à-dire à la bonne marche de ses attributions ou d'un programme dont il a la gestion »[193].

---

187 *Bellerose* c. *Université de Montréal*, [1986] C.A.I. 109; *Bellerose* c. *Université de Montréal*, [1988] C.A.I. 377 (C.Q.).

188 *Bayle* c. *Université Laval*, [1992] C.A.I. 240, 249.

189 *Tremblay* c. *Caisse populaire Desjardins de Saint-Thomas*, [2000] C.A.I. 154.

190 *Robillard* c. *Hôpital Sainte-Justine*, [1989] C.A.I. 296.

191 *Bellerose* c. *Université de Montréal*, [1986] C.A.I. 236.

192 *Bellerose* c. *Université de Montréal*, [1988] C.A.I. 377 (C.Q.).

193 Raymond DORAY et François CHARETTE, *Accès à l'information, loi annotée, jurisprudence , analyse et commentaires*, Cowansville, Éditions Yvon Blais, p. III/ 64-3.

Comme le mentionne le juge Claude Filion dans la décision *Société de transport de la Ville de Laval c. X*,[194] le principe d'interprétation […] « voulant que la nécessité doit être évaluée relativement aux fins pour lesquelles un renseignement est requis, est conforme à la lettre et à l'esprit de la loi. Il ne s'agit pas de déterminer ce qu'est la nécessité en soi, mais plutôt de chercher, dans le contexte de la protection des renseignements personnels, et pour chaque situation, ce qui est nécessaire à l'accomplissement de chaque fin particulière pour laquelle un organisme public plaide la nécessité. »

Mais avec les amendements apportés en 2006, il est expressément permis à un organisme public de recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en oeuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune. Mais alors la collecte de tels renseignements s'effectue dans le cadre d'une entente écrite transmise à la Commission. Une telle entente entre en vigueur 30 jours après sa réception par la Commission.

5.3.2 La communication d'un renseignement personnel sans l'accord de la personne afin d'assurer l'application d'une loi

Les dispositions de l'article 67 de la *Loi sur l'accès* prévoient qu'un organisme public peut communiquer, à toute personne ou à un autre organisme public, un renseignement nominatif, sans l'accord de la personne concernée, si cette divulgation est nécessaire pour l'application d'une loi.

Cette disposition est ainsi formulée :

> *67. Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou organisme si cette communication est nécessaire à l'application d'une loi au Québec, que cette communication soit ou non prévue expressément par la loi.*

Le libellé de cette disposition a été modifié en 2006 afin d'écarter l'interprétation étroite de la notion de nécessité qu'avait retenue la CAI[195].

---

194 *Société de transport de la Ville de Laval* c. *X, (2003-02-21) QCCQ 500-02-094423-014,* < http://www.canlii.org/qc/jug/qccq/2003/2003qccq11657.html >.

195 *Blais* c. *C.S.S.T.*, [2000] C.A.I. 1. Cette prise de position « dogmatique » n'a pas empêché la C.A.I. de rendre une décision pour le moins controversée dans cette affaire. En effet, en l'occurrence, il s'agissait d'un médecin-fonctionnaire de la C.S.S.T. qui, la veille d'une audition devant un tribunal administratif, appelle, sans le consentement de la personne concernée, le médecin de l'accidenté et obtient une opinion sur la relation entre la lésion du travailleur et son accident de travail. La C.A.I. a considéré que cette manœuvre louche était « nécessaire » à l'application de la *Loi sur les accidents de travail et les maladies professionnelles*, car il revenait au médecin-fonctionnaire de conseiller l'organisme sur la relation entre une lésion et un accident survenu au travail. Ce que cette décision néglige toutefois de prendre en compte c'est que l'organisme avait déjà tranché cette question, puisqu'on était rendu au stade de l'audition devant le Bureau de Révision paritaire, et que la relation entre une lésion et un travail n'est pas une question médicale, mais une question juridique, comme le reconnaît d'ailleurs unanimement la jurisprudence des tribunaux spécialisés en la matière.

5.3.3 La communication sans consentement de renseignements personnels lorsque c'est nécessaire à l'application d'une convention collective (art. 67.1 de la *Loi sur l'accès*)

Les dispositions de la *Loi sur l'accès* sont susceptibles d'entrer en interaction avec les dispositions des conventions collectives. Ce sont les dispositions de l'article 67.1 qui régissent ce type de rapport. Elles sont formulées ainsi :

> *67.1 Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou organisme si cette communication est nécessaire à l'application d'une convention collective, d'un décret, d'un arrêté, d'une directive ou d'un règlement qui établissent des conditions de travail.*

Dès 1986, la CAI a interprété cette disposition en indiquant que l'organisme dispose d'une faculté de transmettre ou non les renseignements en cause, mais qu'elle n'a aucune obligation à cet effet[196]. Partant du fait que le mot « peut » n'est pas univoque en droit, mais que son sens dépend d'un certain nombre de facteurs, la CAI s'est montrée sensible au fait que le contexte litigieux justifiant souvent les demandes en ce sens permet par ailleurs à l'organisme d'invoquer d'autres dispositions de la *Loi sur l'accès* (comme l'effet probable sur une procédure judiciaire) et qu'il fallait donc dégager une interprétation qui donne cohérence aux principes de protection des renseignements personnels. La Commission a aussi remarqué que le législateur a fait preuve de rigueur dans la formulation des obligations ou des facultés dans la loi et que lorsqu'il veut imposer une obligation, il utilise toujours le mot « doit ». Certes, le terme « nécessaire » doit recevoir la même interprétation restrictive que celle donnée généralement à ce terme dans la *Loi sur l'accès*. Toutefois, le fait qu'un syndicat considère que la divulgation de ces renseignements est nécessaire à l'application d'une convention collective ne veut pas dire que cela entraîne automatiquement une obligation corrélative pour l'organisme de les divulguer[197]. Ces interprétations ont ensuite été validées par la Cour du Québec et par la Cour supérieure[198].

Pour qu'un syndicat puisse s'autoriser de cette disposition pour réclamer la divulgation de ces renseignements, il faut encore que la convention collective contienne une disposition précise à cet effet[199]. Par ailleurs, certains renseignements recherchés par un syndicat à cet égard peuvent aussi être des renseignements qui sont publics, tel que le prévoit l'article 57. C'est le cas de certains

---

196 *Racette* c. *Centre hospitalier Le Gardeur*, [1986] C.A.I. 266; *Syndicat des travailleuses et travailleurs du Centre Émilie Gamelin et de la Résidence Armand Lavergne* c. *Centre d'accueil Émilie Gamelin*, [1988] C.A.I. 66.

197 *Centre hospitalier Saint-Joesph* c. *Université du Québec à Trois-Rivières*, [1993] C.A.I. 41.

198 *Syndicat des travailleuses et travailleurs du Centre Émilie Gamelin et de la Résidence Armand Lavergne* c. *Centre d'accueil Émilie Gamelin*, [1989] C.A.I. 410 (C.Q.); *Syndicat des travailleuses et travailleurs du Centre Émilie Gamelin et de la Résidence Armand Lavergne (C.S.N.)* c. *Centre d'accueil Émilie Gamelin*, [1990] C.A.I. 286 (C.S.); *Syndicat des travailleuses et travailleurs du Centre Émilie Gamelin et de la Résidence Armand Lavergne (C.S.N.)* c. *Centre d'accueil Émilie Gamelin,* C.A. Montréal, nº 500-09-001378-900, 1994-11-25.

199 *Bazin* c. *Centre hospitalier Cooke*, [1990] C.A.I. 12.

renseignements apparaissant sur la liste de rappel des salariés. L'organisme est alors tenu de les divulguer[200].

Finalement, si un renseignement a été communiqué par erreur à l'organisme et que celui-ci ne l'avait pas requis, la notion de « nécessaire à l'application d'une convention collective » ne saurait être invoquée[201].

5.3.4 La divulgation de renseignements personnels sans le consentement de la personne lorsque la communication est nécessaire à l'exercice d'un mandat confié par l'organisme (art. 67.2 de la *Loi sur l'accès*)

Les dispositions de l'article 67.2 de la *Loi sur l'accès* permettent à un organisme de communiquer des renseignements personnels sans l'autorisation de la personne concernée si cette divulgation est nécessaire à la mise en œuvre d'un mandat confié par l'organisme. La disposition se lit ainsi :

> *67.2 Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme.*
>
> *Dans ce cas, l'organisme public doit:*
>
> *1° confier le mandat ou le contrat par écrit;*
>
> *2° indiquer, dans le mandat ou le contrat, les dispositions de la présente loi qui s'appliquent au renseignement communiqué au mandataire ou à l'exécutant du contrat ainsi que les mesures qu'il doit prendre pour en assurer le caractère confidentiel, pour que ce renseignement ne soit utilisé que dans l'exercice de son mandat ou l'exécution de son contrat et pour qu'il ne le conserve pas après son expiration. En outre, l'organisme public doit, avant la communication, obtenir un engagement de confidentialité complété par toute personne à qui le renseignement peut être communiqué, à moins que le responsable de la protection des renseignements personnels estime que cela n'est pas nécessaire. Une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service visé au premier alinéa doit aviser sans délai le responsable de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué et doit également permettre au responsable d'effectuer toute vérification relative à cette confidentialité.*
>
> *Le deuxième alinéa ne s'applique pas lorsque le mandataire ou l'exécutant du contrat est un membre d'un ordre professionnel. De même, le paragraphe 2° du deuxième alinéa ne*

---

200 *Syndicat des travailleuses et travailleurs du Centre Émilie Gamelin et de la Résidence Armand Lavergne* c. *Centre d'accueil Émilie Gamelin*, [1988] C.A.I. 66.

201 *X.* c. *Commission scolaire des draveurs*, [1995] C.A.I. 43.

> *s'applique pas lorsque le mandataire ou l'exécutant du contrat est un autre organisme public*.

Un organisme public peut confier en tout ou en partie la gestion de renseignements personnels à un mandataire. Un tel mandat doit être encadré par un contrat conforme aux exigences de l'article 67.2 de la *loi sur l'accès* qui prévoit qu'un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme.

Dans un tel cas, le deuxième alinéa de l'article 67.2 de la *Loi sur l'accès* prévoit que l'organisme public doit confier un mandat par écrit et des mentions spécifiques doivent figurer dans un tel contrat. Les seuls renseignements personnels qui peuvent être communiqués sont ceux qui sont nécessaires à l'exercice du mandat ou du contrat de service.

Il faut indiquer, dans le mandat ou le contrat, les dispositions de la *Loi sur l'accès* qui s'appliquent au renseignement communiqué au mandataire ou à l'exécutant du contrat ainsi que les mesures qu'il doit prendre pour en assurer le caractère confidentiel, pour que ce renseignement ne soit utilisé que dans l'exercice de son mandat ou l'exécution de son contrat et pour qu'il ne le conserve pas après son expiration. Le mandat doit prévoir des mesures afin de s'assurer que les renseignements personnels ne demeurent pas en possession du mandataire une fois le mandat accompli et le contrat terminé.

En outre, l'organisme public doit, avant la communication, obtenir un engagement de confidentialité complété par toute personne à qui le renseignement peut être communiqué, à moins que le responsable de la protection des renseignements personnels de l'organisme public concerné estime que cela n'est pas nécessaire.

L'article 67.2 prévoit qu'une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service visé au premier alinéa doit aviser sans délai le responsable de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué et doit également permettre au responsable d'effectuer toute vérification relative à cette confidentialité.

De telles exigences ne s'appliquent pas lorsque le mandataire ou l'exécutant du contrat est un membre d'un ordre professionnel. De même, le paragraphe 2° du deuxième alinéa ne s'applique pas lorsque le mandataire ou l'exécutant du contrat est un autre organisme public.

Les dispositions de l'article 67.3 et 67.4 obligent également l'organisme qui communique de tels renseignements à établir un registre des renseignements transmis sans le consentement de la personne concernée, à justifier cette communication et à donner à la personne concernée l'accès à ce registre.

5.3.5 La divulgation de renseignements dictée par les obligations de l'organisme receveur ou par des circonstances exceptionnelles (article 68 de la *Loi sur l'accès*)

Un organisme peut transmettre des renseignements nominatifs sans le consentement de la personne dans un certain nombre de situations. L'article 68 de la *Loi sur l'accès* dispose que:

> *68. Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel:*
>
> *1° à un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en oeuvre d'un programme dont cet organisme a la gestion;*
>
> *1.1° à un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée;*
>
> *2° à une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient;*
>
> *3° à une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne.*
>
> *Cette communication s'effectue dans le cadre d'une entente écrite qui indique:*
>
> *1° l'identification de l'organisme public qui communique le renseignement et celle de la personne ou de l'organisme qui le recueille;*
>
> *2° les fins pour lesquelles le renseignement est communiqué;*
>
> *3° la nature du renseignement communiqué;*
>
> *4° le mode de communication utilisé;*
>
> *5° les mesures de sécurité propres à assurer la protection du renseignement personnel;*
>
> *6° la périodicité de la communication;*
>
> *7° la durée de l'entente.*

L'entente écrite doit être soumise à la CAI pour avis (art 70).

5.4 Communication d'un renseignement personnel aux fins de le comparer

L'article 68.1 permet à un organisme public, sans le consentement de la personne concernée, de communiquer un fichier de renseignements personnels aux fins de le comparer avec un fichier détenu par une personne ou un organisme si cette communication est nécessaire à l'application d'une loi au Québec, que cette communication soit ou non prévue expressément par la loi.

Lorsque la communication de renseignements personnels n'est pas prévue expressément par la loi, elle s'effectue dans le cadre d'une entente écrite qui doit être transmise pour avis à la Commission d'accès. Lorsque la communication est prévue expressément par la loi, elle s'effectue dans le cadre d'une entente écrite transmise à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission.

5.5 L'étude des ententes de partage de renseignements personnels par la Commission d'accès

L'article 70 de la *Loi sur l'accès* énonce les devoirs afférents à l'étude des ententes de communication de renseignements personnels. C'est ainsi qu'une entente visée à l'article 68 ou au deuxième alinéa de l'article 68.1 doit être soumise à la Commission pour avis.

Pour sa part, la Commission doit prendre en considération:

1° la conformité de l'entente aux conditions visées à l'article 68 ou à l'article 68.1;

2° l'impact de la communication du renseignement sur la vie privée de la personne concernée, le cas échéant, par rapport à la nécessité du renseignement pour l'organisme ou la personne qui en reçoit communication.

La Commission doit rendre un avis motivé dans un délai d'au plus 60 jours de la réception de la demande d'avis accompagnée de l'entente. Si la demande est modifiée pendant ce délai, celui-ci court à compter de la dernière demande. Si le traitement de la demande d'avis dans ce délai ne lui paraît pas possible sans nuire au déroulement normal des activités de la Commission, le président peut, avant l'expiration de ce délai, le prolonger d'une période n'excédant pas 20 jours. Il doit alors en donner avis aux parties à l'entente dans le délai de 60 jours.

L'entente entre en vigueur sur avis favorable de la Commission ou à toute date ultérieure prévue à l'entente. La Commission doit rendre publics cette entente ainsi que son avis. À défaut d'avis dans le délai prévu, les parties à l'entente sont autorisées à procéder à son exécution.

En cas d'avis défavorable de la Commission, le gouvernement peut, sur demande, approuver cette entente et fixer les conditions applicables. Avant d'approuver l'entente, le gouvernement publie à la Gazette officielle du Québec l'entente et, le cas échéant, les conditions qu'il entend fixer avec un avis qu'il pourra approuver l'entente à l'expiration d'un délai de 30 jours de cette publication et que tout intéressé peut, durant ce délai, transmettre des commentaires à la personne qui y est désignée. L'entente entre en vigueur le jour de son approbation ou à toute date ultérieure fixée par le gouvernement ou prévue à l'entente.

L'entente visée au cinquième alinéa ainsi que l'avis de la Commission et l'approbation du gouvernement sont déposés à l'Assemblée nationale dans les 30 jours de cette approbation si l'Assemblée est en session ou, si elle ne siège pas, dans les 30 jours de la reprise de ses travaux. Le gouvernement peut révoquer en tout temps une entente visée au cinquième alinéa.

Le processus d'approbation de la Commission est ainsi complété par un mécanisme permettant au gouvernement d'autoriser l'entente quitte à devoir justifier sa décision devant l'Assemblée nationale.

5.6 L'établissement et la gestion des fichiers de renseignements personnels et des fichiers confidentiels (articles 71-82 de la *Loi sur l'accès*)

Le législateur a normalisé la confection et la tenue des fichiers de renseignements personnels (articles 71-79). L'article 71 prévoit qu'un organisme public doit verser dans un fichier de renseignements personnels établi conformément à la cette sous-section de la Loi tout renseignement personnel qui: 1° est identifié ou se présente de façon à être retrouvé par référence au nom d'une personne ou à un signe ou symbole propre à celle-ci; ou 2° lui a servi ou est destiné à lui servir pour une décision concernant une personne.

La Loi autorise, dans certains cas déterminés, la constitution de fichiers confidentiels (articles 80-82).

L'article 72 fait obligation aux organismes publics de veiller à ce que les renseignements personnels qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés. Les principes dégagés de la *Loi* et de la jurisprudence sont à l'effet que les fichiers de renseignements personnels doivent, se présenter en référence au nom des personnes permettant ainsi de retrouver plus facilement les renseignements qui concernent une personne. L'organisme public ne peut les détruire qu'en conformité avec son calendrier de conservation. Selon la jurisprudence de la CAI, la conservation d'un renseignement qui n'est pas exact constitue une conservation non autorisée par la *Loi* et le renseignement doit être détruit, comme le permet le droit de rectification prévu à l'article 89[202].

L'article 73, qui prévoit la destruction des documents en conformité du calendrier de conservation, est une disposition d'ordre public[203]. Si le calendrier de conservation prévoit la conservation pour une période indéterminée du renseignement, l'organisme est fondé à le conserver indéfiniment[204]. L'établissement ou l'organisme doit aussi déclarer à la CAI l'ensemble des fichiers qu'il détient et cette déclaration doit être mise à jour, si des changements surviennent.

5.7 Le droit des personnes concernées par un renseignement nominatif

Divers droits sont accordés à la personne directement concernée et à ses ayants droit, des restrictions spécifiques touchent aussi à cet accès, en particulier si les renseignements touchent à des tiers, et un droit de rectification est aussi accordé, si les renseignements sont inexacts, incomplets ou équivoques.

---

202 *Thibert* c. *Centres d'accueil du Haut St-Laurent*, [1987] C.A.I. 340.

203 *Bédard* c. *Hôpital Saint-Luc*, [1992] C.A.I. 5.

204 *X.* c. *Régie de l'assurance-maladie du Québec*, [2000] C.A.I. 70.

5.7.1 Les droits d'accès de la personne concernée ou de ses ayants droit

L'article 83 consacre le droit d'une personne d'être informée de l'existence de renseignements personnels qui la concernent dans un fichier de renseignements personnels. Elle a aussi droit d'en recevoir communication, sauf s'il s'agit d'un mineur de moins de 14 ans et que les renseignements sont de nature médicale ou sociale.

Diverses autres restrictions à l'accès de la personne directement concernée par un renseignement personnel apparaissent aux articles 86, 86.1, 87 et 87.1 de la *Loi sur l'accès*. L'article 86.1 touche aux renseignements personnels contenus dans un avis ou une recommandation faite par un membre de l'organisme en cause et limite la discrétion de l'organisme jusqu'à ce qu'une décision finale soit rendue. À cet égard, la CAI a statué qu'une fois la décision de l'établissement prise, il ne peut plus invoquer les dispositions de l'article 86.1 et refuser de communiquer. Telle est le cas d'une expertise médicale qui statue sur la capacité de la personne d'exercer son emploi et sur laquelle l'établissement s'appuie pour décider du congédiement de la personne[205]. Par ailleurs, un organisme exerçant des fonctions de conseil auprès d'un organisme –employeur ne peut invoquer les dispositions de l'article 86.1 dans la mesure où ce n'est pas elle qui prend la décision, mais bien l'organisme-employeur[206]. Cet organisme est plutôt couvert par les dispositions de l'article 87 : il peut refuser de divulguer les renseignements pour les seuls motifs prévus à la section II du chapitre II. Or, ces dispositions nous renvoient aux articles 18 à 41 de la *Loi*.

5.7.2 Les renseignements qui concernent des tiers

La divulgation de renseignements qui révèle un renseignement concernant un tiers, qui est une personne physique, et qui est de nature à nuire sérieusement à ce dernier, ne peut être effectuée qu'avec le consentement de cette personne. Telles sont, en substance, les dispositions que l'on retrouve à l'article 88 de la *Loi sur l'accès*.

5.7.3 Le droit de rectification

Le droit est formulé dans ces termes par la loi :

> *89. Toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que le fichier soit rectifié.*
>
> *89.1 Un organisme public doit refuser d'accéder à une demande de rectification d'un renseignement personnel faite par le liquidateur de la succession, par le bénéficiaire d'une assurance-vie ou d'une indemnité de décès ou par l'héritier ou le successible de la personne concernée par ce renseignement, à moins que cette rectification ne mette en*

---

205 *Laurin* c. *Centre d'accueil Sénécal*, [1992] C.A.I. 30.

206 *Bernier* c. *C.A.R.R.A.*, [1992] C.A.I. 100.

cause ses intérêts ou ses droits à titre de liquidateur, de bénéficiaire, d'héritier ou de successible.

90. En cas de contestation relative à une demande de rectification, l'organisme public doit prouver que le fichier n'a pas à être rectifié, à moins que le renseignement en cause ne lui ait été communiqué par la personne concernée ou avec son accord.

91. Lorsque l'organisme public refuse en tout ou en partie d'accéder à une demande de rectification d'un fichier, la personne concernée peut exiger que cette demande soit enregistrée.

92. Un organisme public doit, lorsqu'il accède à une demande de rectification d'un fichier, délivrer sans frais à la personne qui l'a faite, une copie de tout renseignement personnel modifié ou ajouté, ou, selon le cas, une attestation du retrait d'un renseignement personnel.

93. Toute personne qui a demandé la rectification d'un fichier peut exiger que l'organisme public fasse parvenir une copie des documents prévus à l'article 92 ou, selon le cas, de l'enregistrement visé à l'article 91 à l'organisme de qui il a obtenu le renseignement ou à tout organisme à qui le renseignement a pu être communiqué dans le cadre d'une entente conclue suivant la présente loi.

La jurisprudence a énoncé plusieurs principes au sujet de l'application de ces exigences. Ainsi, il fut décidé que :

- Il revient à l'organisme public de montrer que les renseignements ne devraient pas être rectifiés, qu'ils ne sont pas équivoques ou ambigus. C'est lui qui a le fardeau de la preuve[207] et qui doit montrer que les éléments en cause ou les paroles prononcées correspondent à ce qui a été dit par la demanderesse ou avec son accord[208].

- Une fois que l'établissement a montré que le renseignement n'a pas à être rectifié, la destruction du document ne peut se faire que selon le calendrier de conservation prévu à la Loi sur les archives[209].

- Le droit à la rectification s'exerce sans égard à la date de consignation du document en cause. Il peut donc être antérieur à l'entrée en vigueur de la Loi sur l'accès[210].

- L'organisme public n'est que le dépositaire du document visé, mais il n'en est pas l'auteur. La CAI ne peut ordonner la rectification d'un document sans entendre le

---

207 Entre plusieurs autres, consultez les arrêts suivants : *Thibert* c. *Les centres d'accueil du Haut-Saint-Laurent*, [1987] C.A.I. 340; *X.* c. *Hôtel-Dieu de Montréal*, [1998] C.A.I. 244; *X.* c. *Centre hospitalier Fleury*, C.A.I., 19 juin 2003, Michel Laporte.

208 *Côté* c. *Centre hospitalier affilié universitaire de Québec (Pavillon Saint-Sacrement)*, [1999] C.A.I. 352.

209 *X.* c. *Hôpital Hôtel-Dieu de Montréal*, [1995] C.A.I. 37.

210 *X.* c. *Hôtel-Dieu de Montréal*, [1998] C.A.I. 244.

professionnel qui l'a rédigé, afin de vérifier sa position sur ladite rectification, sans commettre un excès de juridiction[211].

- Face à une demande de rectification s'inscrivant dans une procédure judiciaire en cours, la CAI doit faire preuve de prudence et doit éviter d'intervenir si le débat porte sur des versions contradictoires de certains faits. Elle devrait même dans certains cas décliner juridiction dans un tel contexte. Le fait qu'un document puisse être appelé à servir de preuve dans une instance judiciaire ne veut toutefois pas dire que le droit à la rectification n'existe pas à l'égard de tels documents[212] et la CAI ne peut s'abstenir et décliner juridiction pour la seule raison que l'objet de la rectification exigée risque de se retrouver au centre d'un différend devant être tranché par un autre tribunal[213].

- Dans l'interprétation des qualificatifs ambigu ou équivoque ou inexact qu'utilise la loi, il faut considérer que les faits doivent être patents pour que l'on puisse considérer qu'ils rencontrent les critères de la loi. On ne peut affirmer, par exemple, que tout renseignement qui ne correspond pas à la version du patient est inexact et qu'il doit être rectifié. En fait, une version contradictoire d'un même événement n'équivaut pas nécessairement à de l'inexactitude[214].

- Si la procédure régulière de l'organisme public impose que soient donnés un certain nombre de renseignements relatifs à une demande de soins, comme le fait de s'être présenté accompagné à l'organisme public, et que le formulaire qui prévoit un espace pour répondre à ces questions est laissé en blanc, on peut conclure qu'il s'agit d'un renseignement équivoque et incomplet au sens de la loi. Il doit donc être rectifié[215].

- Le personnel des organisme publics n'a pas à se livrer à une enquête policière lorsqu'il reçoit ou traite une personne sur les circonstances d'un accident. Il est donc normal que le dossier ne contienne pas tous les renseignements possibles sur les circonstances d'un tel événement. Cela ne justifie pas pour autant une rectification des renseignements consignés[216].

- Le droit de rectification porte sur des renseignements déjà existants et non à l'égard de renseignements n'apparaissant pas au dossier de l'usager. Le droit n'a pas pour effet d'obliger les organisme publics du réseau à consigner au dossier tous les renseignements qu'un demandeur juge pertinent. Il appartient au seul professionnel de juger de la

---

211 *Ouellet* c. *C.A.I.*, [2001] C.A.I. 504 (C.Q.).

212 *X.* c. *S.A.A.Q.*, [1991] C.A.I. 79; *Ouellet* c. *C.A.I.*, [2001] C.A.I. 504.

213 *X.* c. *Centre hospitalier affilié universitaire de Québec (Pavillon Enfant-Jésus) et Dr. Daniel Boulet*, C.A.I., 19 août 2003, Diane Boissinot, par. 48.

214 *Ouellet* c. *C.A.I.*, [2001] C.A.I. 504 (C.Q.).

215 *Dubois* c. *Hôtel-Dieu de Saint-Jérôme*, [1993] C.A.I. 11.

216 *Dubois* c. *Hôtel-Dieu de Saint-Jérôme*, [1993] C.A.I. 11.

pertinence de consigner certains renseignements au dossier[217]. Les inscriptions faites par le personnel infirmier à la demande expresse du médecin en charge des traitements et qui traduisent les perceptions et les constats réalisés et exprimés d'une manière détaillée, ne sauraient être rectifiées, d'autant qu'elles coïncident avec les appréciations du médecin lui-même[218].

- Il n'y a pas lieu de rectifier un renseignement consigné au dossier d'un usager s'il correspond à la version donnée par la personne, si équivoque ou ambiguë que puisse être cette version des faits[219]. Le droit de rectification n'est pas celui de voir le passé réécrit[220].

- Il y a lieu d'accepter de rectifier un renseignement apparaissant au dossier de l'usager, s'il appert que des problèmes de langues ont rendu la communication difficile et sont responsables des ambiguïtés dans le contenu du dossier[221].

- La rectification « ne vise que les faits objectivement vérifiables et non l'interprétation qu'une personne peut retenir du texte »[222]. Il faut donc distinguer entre les renseignements objectifs, les faits, qui sont rectifiables, des appréciations subjectives, qui sont de l'ordre de l'opinion, et qui ne peuvent être rectifiées sans l'accord de la personne qui a consigné ces renseignements. Des renseignements consignés, par des médecins, après leur examen de la patiente, et alors qu'ils ont noté leur impression diagnostique, ne sauraient être rectifiés, dans la mesure où ils traduisent la qualification donnée par un professionnel. Il s'agit donc de son opinion et elle ne peut être rectifiée sans son accord[223]. La CAI exprimera parfois l'opinion qu'elle n'a pas la compétence pour obliger la rectification d'une opinion médicale alors que le médecin refuse cette rectification[224]. Le refus de rectifier est d'autant plus justifié lorsqu'un autre médecin a révisé les résultats d'un examen et qu'il a confirmé l'opinion initiale du premier médecin et que celui-ci continue de refuser la rectification demandée de son impression diagnostique[225]. Le fait que les

---

217 *Lachance-Roy* c. *Centre local de services communautaires de l'Aquilon*, [1993] C.A.I. 22; *C.* c. *Hôpital Sainte-Justine*, [1993] C.A.I. 259; *X.* c. *Commission scolaire des Draveurs*, [1995] C.A.I. 43; *C.* c. *Centre hospitalier de Granby*, [2001] C.A.I. 280.

218 *X.* c. *Centre hospitalier régional de Trois-Rivières*, C.A.I., 4 février 2002, Hélène Grenier.

219 *Dubois* c. *Hôtel-Dieu de Saint-Jérôme*, [1993] C.A.I. 11.

220 *L.* c. *Centre hospitalier régional de l'Outaouais*, [1984-1986] 1 C.A.I. 123.

221 *Paul* c. *Hôpital général de Montréal*, [1989] C.A.I. 348; *X.* c. *S.A.A.Q.,* [1991] C.A.I. 79.

222 *X.* c. *Centre hospitalier universitaire de Sherbrooke*, C.A.I., 4 juin 2004, Michel Laporte, p. 4.

223 *M.* c. *Centre hospitalier régional de l'Outaouais*, (1984-1986) 1 C.A.I. 120; *L.* c. *Centre hospitalier régional de l'Outaouais*, (1984-1986) C.A.I. 123; *M.* c. *CLSC Normandie*, [1986] C.A.I.*X.* c. *Hôtel-Dieu de Montréal*, [1998] C.A.I. 244; *C.* c. *Centre hospitalier de Granby*, [2001] C.A.I. 280; *F.* c. *Centre hospitalier universitaire de Sherbrooke*, CAI, 23 octobre 2002, Michel Laporte; *X.* c. *Centre hospitalier régional de Trois-Rivières*, C.A.I., 4 février 2002, Hélène Grenier; *X.* c. *Centre hospitalier affilié universitaire de Québec (Pavillon Enfant-Jésus) et Dr. Daniel Boulet*, C.A.I., 19 août 2003, Diane Boissinot, par. 46.

224 *X.* c. *Hôpital de Rivière-du-Loup*, C.A.I., 22 septembre 2003, Hélène Grenier (dossier 03 15 29); *X.* c. *Hôpital de Rivière-du-Loup*, C.A.I., 22 septembre 2003, Hélène Grenier (dossier 03 14 31).

225 *X.* c. *Centre hospitalier Fleury*, C.A.I., 19 juin 2003, Michel Laporte.

renseignements apparaissant au dossier de l'usager à la suite d'une seconde consultation, tenue le lendemain, diffèrent de l'impression diagnostique d'abord établie par le médecin qui a vu en premier l'usager, ne veut pas dire qu'ils sont équivoques ou incomplets s'il s'avère qu'ils correspondent aux propos tenus par l'usager à ce moment et à l'appréciation du comportement de l'usager, tel qu'il a été perçu et exprimé par le premier professionnel qui a vu l'usager[226]. La C.A.I. ne peut forcer une personne à modifier son opinion[227]. La seule façon de vérifier l'exactitude d'une opinion est de confronter l'écrit à son auteur. Si l'auteur admet qu'il s'agit de son opinion, le travail de la CAI s'arrête là[228]. La CAI n'est pas le bon forum pour débattre de l'exactitude des opinions médicales[229].

- Si la question de la détermination du site anatomique ayant fait l'objet d'un examen radiologique est une question objective, on ne peut faire prévaloir l'opinion d'un usager qui prétend qu'on a réalisé une arthrographie de son genou droit alors que la preuve scientifique montre que l'arthrographie réalisée est celle d'un genou gauche, que l'établissement montre qu'il prend grand soin de bien identifier les films radiologiques de ce type, que tous les renseignements au dossier de l'usager consignés par le personnel clinique avant l'arthrographie concernent des problèmes au genou gauche et que l'usager ne peut expliquer pourquoi il n'a pas protesté si on a procédé à une arthrographie de son genou gauche, alors qu'il prétend avoir eu des douleurs à son genou droit[230]. Il en est de même lorsque le médecin s'appuie sur l'interprétation donnée par un neuro-radiologiste dont la lecture des résultats d'une résonance magnétique montre que le problème existe tant à gauche qu'à droite[231].

- Constituent également des éléments subjectifs non susceptibles de rectification sans l'accord de leur auteur : l'appréciation si une personne est agressive ou simplement impatiente, dans la mesure où il s'agit d'une appréciation des faits par la professionnelle en cause[232]; le fait qu'elle feigne ou non relève de la même appréciation professionnelle[233]; le fait que l'usager refuse de s'autocritiquer, qu'il nie l'ensemble des faits et ne collabore pas ou qu'il conteste les moindres informations communiquées au médecin par d'autres sources[234]; le résumé d'une conversation entre le professionnel de la santé et l'usager, car

---

226 *X.* c. *Centre hospitalier régional de Lanaudière*, CAI, 2 juillet 2002, Hélène Grenier.

227 *J.* c. *Clinique Roy-Rousseau*, [1986] C.A.I. 129; *M.* c. *Centre local de services communautaires Normandie*, [1986] C.A.I. 87; *Thibert* c. *Les centres d'accueil du Haut Saint-Laurent*, [1987] C.A.I. 340; *X.* c. *S.A.A.Q.*, [1991] C.A.I. 79; *C.* c. *Hôpital Sainte-Justine*, [1993] C.A.I. 258; *C.* c. *Centre hospitalier de Granby*, [2001] C.A.I. 280.

228 *M.* c. *Centre hospitalier régional de l'Outaouais*, [1984-1986] 1 C.A.I. 120.

229 *X.* c. *Hôpital Sainte-Justine*, C.A.I. 10 janvier 2002, Hélène Grenier; *X.* c. *Centre hospitalier régional de Trois-Rivières*, C.A.I., 4 février 2002, Hélène Grenier.

230 *Roy* c. *Centre hospitalier universitaire de Sherbrooke*, C.A.I., 6 février 2002, Michel Laporte.

231 *X.* x. *Polyclinique Maisonneuve-Rosemont*, C.A.I., 22 juillet 2003, Hélène Grenier.

232 *Dupuis* c. *Hôtel-Dieu de Saint-Jérôme*, [1999] C.A.I. 346.

233 *X.* c. *Centre hospitalier régional de Trois-Rivières*, C.A.I., 4 février 2002, Hélène Grenier.

234 *X.* c *Hôpital Louis-H. Lafontaine*, C.A.I., 27 mars 2003, Hélène Grenier.

il s'agit d'une impression subjective[235]; l'appréciation de la dangerosité d'un usager[236]; le choix du médecin de traduire par des expressions spécifiques les résultats de ses examens et de l'évaluation du dossier médical de l'usager[237]; le diagnostic médical[238], le consentement aux soins[239]; toute question d'interprétation qui traduit la position de son auteur[240]; en matière d'expertise médicale, le résumé d'une entrevue avec le professionnel concerné[241]; des faits objectifs constatés par le professionnel de la santé, car cela a pour effet « d'y apporter aussi une dimension subjective »[242].

- Constituent des éléments objectifs susceptibles de rectification, les paroles effectivement prononcées par une personne dans une situation donnée[243]. Les paroles attribuées directement à une personne et exprimées par des guillemets peuvent être rectifiées, s'il s'avère qu'elles ne furent effectivement pas prononcées[244]. Lorsque des guillemets sont utilisés, mais que la personne nie avoir prononcé ces paroles, la rectification peut consister à ordonner d'enlever les guillemets qui laissent entendre qu'il s'agit d'une citation verbatim[245]. Une personne qui recherche une rectification dans de tels cas ne saurait se contenter d'une dénégation générale que ces paroles n'ont jamais été prononcées. Elle a le fardeau de preuve de montrer que ces paroles ne furent jamais prononcées ou que d'autres paroles ont été, dans les faits, prononcées[246]. Si le médecin fait une remarque incidente qui correspond dans les faits à un diagnostic médical, mais que ce n'est pas le but du médecin, il peut y avoir rectification[247]. Si le titre d'un document ne correspond pas à son contenu, il est effectivement équivoque[248]. Le fait d'inscrire que l'usager a fait l'objet d'une accusation criminelle (une « charge ») alors qu'il ne s'agit que d'une plainte déposée par une supposée victime constitue un renseignement objectif pouvant être rectifié[249]. De même l'expression « se dit autistique » peut être rectifiée alors

---

235 *C.* c. *Hôpital Sainte-Justine*, [1993] C.A.I. 258.

236 *X.* c *Hôpital Louis-H. Lafontaine*, C.A.I., 27 mars 2003, Hélène Grenier.

237 *X.* c. *Centre hospitalier universitaire de Québec*, [2001] C.A.I. 160.

238 *Zincoski* c. *Centre hospitalier de Ste-Mary*, [1993] C.A.I. 90; *E.* c. *Institut Philippe Pinel*, [1993] C.A.I. 105.

239 *Zincoski* c. *Centre hospitalier de Ste-Mary*, [1993] C.A.I. 90.

240 *X.* c. *Centre d'accueil et de réadaptation À la croisée*, [1992] C.A.I. 170.

241 *Dufour* c. *Ministère de la Justice*, [1987] C.A.I. 20.

242 *J.* c. *Clinique Roy-Rousseau*, [1986] C.A.I. 129.

243 *Dupuis* c. *Hôtel-Dieu de Saint-Jérôme*, [1999] C.A.I. 346.

244 *X.* c. *S.A.A.Q.*, [1991] C.A.I. 79.

245 *F.* c. *Hôpital général de Lakeshore*, [1986] C.A.I. 490.

246 *Dupuis* c. *Hôtel-Dieu de Saint-Jérôme*, [1999] C.A.I. 346.

247 *E.* c. *Institut Philippe Pinel*, [1993] C.A.I. 105.

248 *X.* c. *Centre d'accueil et de réadaptation À la croisée*, [1992] C.A.I. 170.

249 *X.* c. *Hôpital Louis-H. Lafontaine*, C.A.I., 27 mars 2003, Hélène Grenier.

que la personne avait indiqué qu'elle avait des problèmes de concentration et qu'elle se concentrait, lorsqu'elle étudiait, comme une personne autistique[250].

- La simple reprise dans le dossier d'un usager d'une annotation contenue dans le dossier d'un autre établissement, et alors que le premier établissement a accepté de rectifier l'information qui apparaissait dans son dossier, constitue un élément objectif pouvant être rectifié[251]; il en est de même si le dossier fait référence à une date d'occurrence d'un événement alors que la preuve montre que l'événement est survenu à un autre moment[252].

- Si la rectification d'éléments subjectifs n'est pas réalisable à l'encontre de la volonté du professionnel qui a réalisé les annotations dans le dossier, le remède approprié est l'enregistrement de la dissidence de l'usager à l'égard de cette opinion, comme le permet l'article 91 de la Loi sur l'accès[253].

- La conservation de tout renseignement qui, selon le calendrier de conservation de l'organisme public, aurait dû être détruit n'est pas permise, et le droit de rectification consiste alors à ordonner la destruction des renseignements en cause en s'appuyant sur l'article 73 de la Loi sur l'accès , article qui est d'ordre public[254]; il en est de même dans les dossier de la DPJ si, suite à un signalement non retenu, des informations sont conservées alors qu'elles devraient être détruite en vertu de l'article 37.1 de la Loi sur la protection de la jeunesse.

- La conservation de tout renseignement dont l'exactitude n'est pas établie constitue une conservation non autorisée par la loi[255].

- Ne peuvent faire l'objet de rectification les renseignements qui ne sont pas nominatifs, mais qui sont publics. Ainsi, le fait qu'une personne ait participé ou non à une rencontre du conseil d'administration d'un organisme public, renseignement qui est public, ne peut faire l'objet d'une rectification[256]. Il en est de même d'un renseignement apparaissant dans un rapport du coroner, rapport qui est aussi public[257].

- La rectification n'est pas le recours approprié pour contester le contenu d'un rapport dont une partie fut remplie par l'employeur seulement après que le réclamant ait complété sa

---

250 *X.* c. *Centre hospitalier universitaire de Sherbrooke*, C.A.I., 4 juin 2003, Michel Laporte.

251 *Côté* c. *Centre hospitalier affilié universitaire de Québec (Pavillon Saint-Sacrement)*, [1999] C.A.I. 352.

252 *Forget* c. *S.A.A.Q.*, [1992] C.A.I. 115.

253 Parmi beaucoup d'autres, consultez les arrêts suivants : *Lachance-Roy* c. *Centre local de services communautaires de l'Aquilon*, [1993] C.A.I. 22; *C.* c. *Centre hospitalier de Granby*, [2001] C.A.I. 280.

254 *Thibert* c. *Les centres d'accueil du Haut Saint-Laurent*, [1987] C.A.I. 340; *Bédard* c. *Hôpital Saint-Luc*, [1992] C.A.I. 5 .

255 *Thibert* c. *Les centres d'accueil du Haut Saint-Laurent*, [1987] C.A.I. 340

256 *Bordeleau* c. *Centre d'accueil Docteur Joseph Garceau*, [1986] C.A.I. 278.

257 *Payette* c *Bureau du coroner*, [1988] C.A.I. 311.

partie et sans qu'il ne soit porté à sa connaissance les renseignements ajoutés par l'employeur[258].

- Si un document est daté de la date A, mais remis à l'employeur à la date B, la rectification ne peut consister à ordonner que seule la date A apparaisse[259].

- Dans le cas où le document concerné fait mention d'une recommandation qui aurait été acceptée par le patient, alors que celui-ci le nie catégoriquement, on peut accepter une rectification si la preuve montre qu'aucune discussion ne fut tenue sur ce point. La personne doit être informée spécifiquement d'une recommandation pour qu'on ne puisse rectifier cette affirmation dans un document[260]. Toutefois, si un litige existe sur une recommandation, la CAI ne pourrait ordonner une rectification qui équivaudrait à rendre la conclusion illogique pour un lecteur attentif; quand de telles ambiguïtés surviennent, il faut demander à l'auteur le sens qu'il entendait donner à son texte[261].

- Le droit de rectification prévu par la Loi sur l'accès ne donne pas le droit à la CAI d'émettre des ordonnances qui touchent aux conséquences de la rectification ordonnée. Ainsi, la CAI ne pourrait ordonner le paiement pour une absence qui serait devenue motivée suite à la rectification accordée, par exemple[262].

- Le droit de rectification n'est pas le recours approprié pour contester le fait que des renseignements médicaux de nature psychologiques soient présents dans le dossier d'un usager et que cela serait susceptible de lui porter préjudice dans le futur[263]. Dans le contexte de l'application des dispositions parentes prévues par la Loi sur la protection des renseignements personnels dans le secteur privé, la CAI a jugé que des préoccupations liées à la préservation des attentes légitimes en matière de vie privée ou pour faire en sorte qu'un employeur ne puisse avoir accès aux informations médicales sensibles contenues au dossier d'un médecin, alors que ce dernier doit répondre aux questions posées par un assureur dans le cadre d'une réclamation, ne saurait être satisfaites par le biais des dispositions assurant une possible rectification des renseignements[264].

- Constitue une méthode appropriée de noter une rectification le fait de barrer en rouge un renseignement apparaissant au dossier en y juxtaposant la mention « erreur »[265].

---

258 *Bordeleau* c. *Centre d'accueil Docteur Joseph Garceau*, [1986] C.A.I. 278.

259 *Bordeleau* c. *Centre d'accueil Docteur Joseph Garceau*, [1986] C.A.I. 278.

260 *M.* c. *Centre hospitalier régional de l'Outaouais*, [1984-1986] 1 C.A.I. 120.

261 *X.* c. *Centre hospitalier affilié universitaire de Québec (Pavillon Enfant-Jésus)*, C.A.I., le 19 août 2003, Diane Boissinot, par. 42-43.

262 *M.* c. *Centre hospitalier régional de l'Outaouais*, [1984-1986] 1 C.A.I. 212.

263 *X.* c. *Hôpital Sainte-Justine*, C.A.I., 10 janvier 2002, Hélène Grenier.

264 *L.* c. *D^re^ Nicole Thibault*, C.A.I., 18 juillet 2002, Michel Laporte.

265 *X.* c. *Hôpital Louis-H. Lafontaine*, C.A.I., 27 mars 2003, Hélène Grenier.

- Seule la CAI a compétence pour examiner une demande de rectification refusée par un organisme public. La Cour supérieure doit décliner juridiction si une telle demande lui est formulée[266].

266 *Jalbert, Louisson* c. *Paré, Dr. Pierre et Centre hospitalier universitaire de Québec, Pavillon Hôtel-Dieu de Québec*, C.S. Québec 200-05-016487-022, le 26 septembre 2002, juge Jacques Babin; *X.* c. *Centre hospitalier affilié universitaire de Québec (Pavillon Enfant-Jésus)*, 91 août 2003, Diane Boissinot, par. 49.

6. Le lien entre un document et une personne, une association, une société ou l'État

Pour servir de preuve ou pour être opposables à une personne, les documents doivent pouvoir être associés à la personne de laquelle ils émanent.

Dans l'univers du papier, la signature est le moyen généralement utilisé afin d'établir ce lien entre une personne et un document émanant du signataire. Pour ajuster le cadre juridique aux caractéristiques des documents établis en faisant usage des technologies l'information, la *Loi concernant le cadre juridique des technologies de l'information* organise le régime juridique des divers moyens par lesquels il est possible d'établir un lien entre un document et une personne, une association, une société ou l'État.

La *Loi concernant le cadre juridique des technologies de l'information* ne précise pas les moyens ou procédés pour établir ce lien. Le lien peut être assuré par tout procédé ou par une combinaison de moyens du moment qu'ils permettent d'atteindre les résultats énoncés à l'article 38, c'est-à-dire identifier le document, au besoin sa provenance et sa destination, et confirmer l'identité d'une personne et son lien avec le document identifié.

La signature est l'un des moyens pour établir le lien entre une personne et un document. Elle peut être apposée au document par tout procédé qui satisfait aux exigences de l'article 2827 du *Code civil du Québec*, et ce, quel que soit le support du document. Cette notion de signature est neutre technologiquement (article 39).

Les articles 40 à 46 viennent préciser les qualités que doivent posséder les mécanismes utilisés pour établir ces liens, et imposent des conditions pour l'utilisation de certains moyens et procédés d'identification et de localisation.

- La confirmation de l'identité des personnes ou de l'identification des sociétés, des associations ou de l'État doit d'abord s'appuyer sur la vérification. La *Loi* énonce les façons d'effectuer cette vérification et rappelle l'obligation de respecter la loi lors de cette opération. Quant à la confirmation de l'identité ou de l'identification, elle peut se faire au moyen d'un document, entre autres un certificat, dont l'intégrité est assurée (article 40).

- Des obligations incombent à une personne qui utilise un document technologique pour preuve de son identité ou de celle d'une autre personne. Elle doit en préserver l'intégrité, et si le document circule sur un réseau de communication, elle doit le protéger contre l'interception et en assurer la confidentialité (article 41).

- La *Loi concernant le cadre juridique des technologies de l'information* crée l'équivalent fonctionnel des pièces d'identité sur papier. Une pièce d'identité peut se retrouver autant sur un document technologique que sur un document papier ou plastique (article 42).

- Des protections de l'intégrité et de la vie privée de la personne entourent les modes d'identification et de localisation. Il est interdit d'exiger que l'identité d'une personne puisse être établie au moyen d'un dispositif qui porte atteinte à son intégrité physique. Il est interdit

d'exiger qu'une personne soit liée à un dispositif qui permet de la retracer, sauf si la loi le permet expressément en vue de protéger la santé des personnes ou la sécurité publique (article 43).

- Des contrôles sont aussi mis en place en ce qui concerne l'utilisation des mesures biométriques comme moyen d'identification d'une personne (articles 44 et 45).

- La *Loi concernant le cadre juridique des technologies de l'information* prévoit des règles relatives à l'identification et à la localisation des objets, de manière à établir leur provenance ou leur destination, et ce, à l'aide d'un identifiant, qui devrait être accessible au moyen d'un service de répertoire (article 46).

La *Loi concernant le cadre juridique des technologies de l'information* reconnaît ainsi la possibilité d'utiliser divers modes d'authentification de l'identité d'une personne qui communique au moyen d'un document technologique et, dans ce contexte, elle contient des mesures de protection de la vie privée.

7. L'identification des personnes

L'identité concerne l'ensemble des données de fait et de droit qui permettent d'individualiser quelqu'un. Les identificateurs tels les pièces d'identités, les passeports, les permis de conduire etc., permettent d'établir les éléments qui, légalement, concourent à l'identification d'une personne physique dans la société au regard de l'état civil : nom, prénom, date de naissance, filiation etc. Au niveau judiciaire, établir l'identité consiste à assurer, par différents moyens techniques, l'identification des personnes.

7.1 L'identité légale

À la naissance, chaque personne se voit attribuer un nom et un prénom qu'elle conserve toute sa vie et sous lesquels elle a l'obligation d'exercer ses droits civils (art. 5 et 50 C.c.Q). Ces nom et prénom sont consignés dans un acte d'état civil conservé par le directeur de l'état civil. Lui seul a la charge de dresser les actes de l'état civil, d'en tenir un registre et d'en assurer la publicité (art. 103 C.c.Q).

Attribut de la personnalité et reflet de la personne, le nom n'a cependant pas le caractère immuable auquel on pourrait s'attendre. Ainsi, en certaines circonstances exceptionnelles, ce nom peut parfois être changé avec le consentement d'un tribunal ou du directeur de l'état civil (art. 57 et ss. C.c.Q.). Par ailleurs, l'obligation qui est faite à chaque personne d'exercer ses droits civils sous le nom qui lui est attribué à la naissance, n'empêche pas une personne d'utiliser un autre nom en d'autres circonstances (art. 56 C.c.Q.). Cette situation, on le sait, se rencontre fréquemment dans le cas d'artistes dont les noms de théâtre sont souvent beaucoup mieux connus que les noms de baptême. L'utilisation d'un nom autre que celui attribué à la naissance n'est toutefois pas sans réserve. En effet, la personne qui utilise un nom autre que le sien est responsable de la confusion ou du préjudice qui peut en résulter.

7.2 L'identification

L'identification est l'action d'identifier, c'est-à-dire de reconnaître une personne, à certains traits non équivoques. L'identification est un processus d'information par lequel on compare de l'information afin d'avoir le degré de certitude requis à l'égard des qualités de la personne avec laquelle on entre en contact. C'est pourquoi on utilise dans certains milieux la notion d'authentification. Ainsi, dans la terminologie de l'informatique la notion d'authentification renvoie aux mécanismes tendant à procurer le niveau recherché de certitude à l'égard de l'identité d'une personne.

L'identification ne réfère pas toujours à l'identité légale et la multiplicité des rapports humains emporte une diversité des besoins en matière d'identification. Le processus d'identification des personnes peut prendre diverses formes.

Dans les environnements de transactions électroniques comme dans le monde physique, l'identification est un processus inhérent à la vie sociale, il est tributaire du contexte et du genre de transaction et il comporte des risques qu'il est nécessaire de gérer correctement.

7.2.1 Un processus inhérent à la vie sociale

L'identification est un processus inhérent à la vie sociale. Pour assurer le déroulement de la plupart des activités, tous doivent procéder à l'identification des personnes physiques, des personnes morales et des choses. Il est en effet essentiel, pour la plupart des interactions humaines, de savoir, à des degrés variables, à qui l'on a affaire.

Pour effectuer les comparaisons inhérentes à l'identification et pour obtenir le degré recherché de certitude, on aura besoin de plus ou moins d'informations. Il sera parfois nécessaire d'avoir recours à des mécanismes de validation ou de corroboration des informations pouvant permettre d'accroître le degré de certitude à l'égard de l'identité d'une personne.

7.2.2. Un processus tributaire du contexte et du genre de transaction

Les relations que nous entretenons avec les autres sont variées : elles vont du simple salut au voisin que l'on reconnaît en raison de l'heure à laquelle il passe, jusqu'aux procédures complexes destinées à compléter une transaction importante.

L'identification est un processus qui n'est pas uniforme car le besoin d'identifier et de s'identifier est plus ou moins considérable selon les contextes[267]. On ne prend pas le même degré de précaution pour identifier nos vis-à-vis pour tous et chacun des contacts que l'on décide de faire. Certaines relations ont des enjeux plus importants que d'autres. Des transactions comportent des risques élevés tandis que d'autres portent peu à conséquence.

Ainsi, lors de rencontres dans un même lieu, l'identification d'un voisin ou d'un collègue de travail ne nécessite pas le recours à l'identité légale des personnes : on ne réclame pas sa carte d'identité à une personne pour les moindres contacts que l'on a avec elle! Bon nombre des transactions que nous faisons dans la vie courante ne supposent pas un niveau très élevé de certitude quant à l'identification. Par exemple, l'achat d'un journal au coin de la rue ne suppose pas pour le marchand et le client d'avoir mutuellement connaissance de leur identité respective. Il en va de même de la plupart des transactions dont le paiement s'effectue sur place et en argent comptant.

Certaines circonstances, par exemple l'exercice des droits d'accès à des informations personnelles ou encore la conclusion de contrats d'importance ou dont le paiement est différé, imposent toutefois un niveau de fiabilité plus élevé quant à l'identité des personnes impliquées. Ce phénomène met en lumière le fait que l'identification s'inscrit dans une logique de gestion des risques.

L'identification n'est pas un phénomène univoque : les situations dans lesquelles il est nécessaire d'identifier sont multiples. Le plus souvent, l'identification est volontaire mais elle est parfois une

---

267 Matthew D. FORD, « Identity Authentication and 'E-Commerce' », 1998 (3) *The Journal of Information, Law and Technology (JILT)*. http://www.law.warwick.ac.uk/jilt/98-3/ford.html.

condition de l'obtention d'un bien ou d'un service. Sur Internet, l'identification peut se faire à l'insu de l'intéressé. Enfin, en certaines circonstances, elle est faite de force.

L'identification volontaire est celle que l'on fait spontanément afin d'établir qui l'on est auprès d'une autre personne. Par exemple, on parle de l'identification-condition lorsque l'obtention d'un bien ou d'un service est assujettie à un processus déterminé d'identification.

En ayant recours à divers moyens, il est possible d'identifier à son insu une personne qui visite un site ou prend part à une transaction sur Internet. Une politique d'identification doit impérativement baliser de telles pratiques car elles peuvent contrevenir aux lois sur la protection de la vie privée. Enfin, l'identification forcée est celle que doivent faire les forces de police dans l'accomplissement de leurs fonctions de lutte contre le crime.

Toutes ces démarches relatives à l'identification comportent des risques.

7.2.3 Un processus comportant des risques qu'il faut gérer

Ne pas identifier adéquatement comporte des conséquences. Si l'on identifie en exigeant trop d'informations, l'on s'expose à contrevenir aux règles en matière de protection de la vie privée. Si l'on recueille des informations insuffisantes, l'on peut devoir répondre des pertes, dommages et inconvénients qui pourraient résulter des erreurs engendrées par une identification inadéquate.

À l'égard de toute activité comportant des risques, quatre attitudes sont possibles : accepter les risques, éviter les risques, les réduire ou les transférer. Mais pour accepter les risques, il faut les connaître et en apprécier l'ampleur et la portée. Pour les éviter, il faut les connaître de même que les précautions, méthodes et processus par lesquels l'évitement est possible. Pour réduire les risques, il faut mettre en place les précautions afin de diminuer les dangers associés aux activités concernées. Enfin, pour transférer les risques, il faut les identifier et les porter à la connaissance de celui sur lequel on se propose de les faire porter.

Afin de décider de manière adéquate des mécanismes et processus d'identification dans un environnement de transactions électroniques, il est nécessaire de suivre une méthode. Il faut se poser un ensemble de questions et y apporter des réponses dans l'ordre approprié.

Ainsi, il faut premièrement situer le besoin d'identification, i.e. répondre à la question : pourquoi doit-on identifier?

Deuxièmement, il faut spécifier le niveau de certitude requis quant à l'identité du co-contractant.

Troisièmement, il faut considérer les limites à la capacité d'identifier. Il est en effet fréquemment nécessaire de respecter un équilibre entre d'une part, les impératifs de certitude, voire de sécurité des transactions et, d'autre part, les exigences en matière de protection de la vie privée des personnes. Autrement dit, on ne peut exiger un niveau de certitude pour l'identification au point de porter atteinte au droit à la vie privée d'une personne.

Une fois ces étapes accomplies, il est possible de sélectionner les mécanismes et processus d'identification qui répondront à la fois aux besoins de certitude tout en respectant les exigences relatives au respect de la vie privée des personnes.

Enfin, on passe en revue les méthodes et les processus à suivre afin d'attribuer une identité à une personne dans un environnement électronique.

Les étapes du processus de détermination des besoins et des moyens d'identification	
Première étape :	La spécification des besoins d'identification
Seconde étape :	La détermination du degré de certitude requis pour l'identification
Troisième étape :	La considération des limites à la collecte et au traitement de l'information personnelle
Quatrième étape :	La détermination des mécanismes et processus d'identification, i.e. procéder au choix de la méthode d'identification

7.3 Baliser la collecte et le traitement de l'information personnelle

Dans l'absolu, on peut se prendre à rêver d'un système dans lequel on collecte et collige tous les renseignements permettant d'identifier et de vérifier l'identité d'une personne même pour faire face aux situations exceptionnelles. Mais un équilibre doit être respecté entre une collecte tous azimuts d'information et une approche de protection de la vie privée qui rendrait les transactions trop risquées. Aussi, après avoir établi les besoins d'identification et déterminé le degré requis de certitude, il faut considérer les limites imposées au nom de la protection de la vie privée des personnes.

En tant que processus supposant différents échanges d'information, l'identification présente à la fois des avantages et des écueils. Dans la plupart des situations, il faut mettre en place un environnement garantissant un équilibre entre les besoins de certitude dans l'identification et la protection des droits de la personne, notamment à la vie privée.

C'est pourquoi les processus d'identification électronique doivent êtres conçus de manière à respecter les principes des lois relatives à la protection des informations personnelles.

L'on s'accorde généralement à reconnaître que le droit à la vie privée suppose un droit de regard sur les informations qui y sont relatives et un droit balisé à l'anonymat. Dans l'univers des transactions électroniques, cela se traduit par un devoir de retenue dans les demandes d'informations personnelles et l'obligation de mettre en place ce qui est nécessaire afin que les personnes puissent en tout temps exercer leur droit de regard sur les informations qui les concernent.

En matière de protection de renseignements personnels, le principe de retenue (limitation en matière de collecte) vient guider les gestionnaires confrontés au défi d'assurer un équilibre entre les besoins de certitude, de sécurité et les obligations d'assurer le respect de la vie privée des personnes. En partant du principe suivant lequel on ne doit recueillir que les informations dont on est en mesure de démontrer la nécessité, compte tenu de la transaction considérée, on s'assure que les informations personnelles ne seront collectées que pour une fin clairement identifiable et limitée.

Un droit de contrôle sur l'information personnelle est reconnu dans la plupart des lois sur la protection des renseignements personnels. Une telle reconnaissance présente un double intérêt : elle permet à l'individu de contrôler l'exactitude des données stockées sur son compte et, naturellement en cas de besoin, de les faire rectifier; elle permet également de faire participer l'ensemble des personnes fichées au contrôle du respect des règles en matière d'informations nominatives.

7.3.1 La démarche

Comme l'identification implique souvent la collecte et le traitement de renseignements personnels, il importe de s'assurer que l'on respecte les principes les plus universellement admis en matière de protection d'informations relatives à la vie privée. L'identification des personnes dans l'environnement électronique soulève un grand nombre de préoccupations concernant la protection de la vie privée et la sécurité des transactions (voir annexe1, Tableau 6- *Les préoccupations rattachées à l'identification des personnes*).

Plusieurs utilisateurs d'Internet craignent que des informations à caractère personnel soient automatiquement générées, collectées, stockées rapprochées et exploitées à des fins diverses.

Les technologies de l'information permettent de recueillir un nombre croissant de renseignements sur un individu. Le développement du commerce électronique s'accompagnera d'une augmentation du volume et de la diversité des données de caractère personnel communiquées sur les réseaux aux cours d'activités et de transactions électroniques. Les nouvelles méthodes utilisées pour traiter de très grandes quantités de données permettent de créer des profils de consommateurs associant données démographiques, informations financières, pratiques de consommation et détails sur les transactions.

La prise en considération des principes relatifs à la collecte et au traitement des informations personnelles permet de mieux cerner les balises et précautions qui doivent êtres mises en place lors de l'établissement de processus d'identification.

Les avantages résultant de l'identification sont variables en fonction des besoins afférents aux différentes interactions et transactions dans lesquelles on s'engage.

Il est donc nécessaire de trouver un équilibre entre les impératifs de la protection des renseignements personnels, des droits individuels, des intérêts commerciaux, du droit à l'information et de l'obligation de l'État d'assurer une gestion correcte de ses programmes, de se protéger et de protéger les citoyens des menaces à la sécurité publique.

Afin de faciliter la détermination concrète des limites au droit de collecter et de traiter des informations personnelles lors de processus d'identification, on peut avoir recours à une grille d'analyse dans laquelle sont consignées les informations permettant d'associer la quantité et la qualité des informations demandées à chacun des principes fondamentaux en matière de collecte et de gestion de l'information personnelle.

Au TERME DE CETTE ÉTAPE, on sera en mesure d'associer les principes devant être respectés lors de la collecte, du traitement et de la conservation d'informations relatives à l'identité d'une personne en regard des risques et enjeux spécifiques à l'environnement que l'on met en place.

Cette démarche permet de compléter le processus de détermination des informations qui sont considérées comme étant nécessaires à la transaction considérée.

Elle aidera à déterminer les moyens acceptables pour obtenir le degré approprié de certitude à l'égard de l'identité d'une personne tout en assurant la protection de sa vie privée.

7.3.2 Les principes de gestion à respecter

La législation québécoise sur la protection des renseignements personnels limite le droit d'un organisme public ou d'une entreprise de recueillir des informations personnelles[268]. De telles informations ne peuvent être recueillies qu'auprès de la personne concernée ou d'un tiers, en certaines circonstances spécifiques (Loi sur l'accès, art. 65 et Loi sur le secteur privé, art. 6). Les limites au droit de collecter et de traiter des informations personnelles peuvent être synthétisées dans les principes de gestion ci-après explicités.

a) La nécessité de la collecte d'informations identifiantes

Il faut être en mesure de démontrer la nécessité des renseignements demandés.

Dans le secteur public, il est licite de recueillir un renseignement personnel seulement si cela est nécessaire à l'exercice des attributions de l'organisme public ou à la mise en œuvre d'un programme dont on a la gestion (Loi sur l'accès, art 64).

En vertu de la loi sur le secteur privé, l'on ne peut exiger des informations personnelles autres que celles qui sont strictement nécessaires à la prestation du service proposé ou à l'exécution du contrat. Par exemple, la Commission d'accès à l'information a expliqué, dans sa décision *Bellerose* c. *Université de Montréal*[269] que par informations nécessaires, il fallait entendre celles qui sont requises, indispensables, obligatoires pour le fonctionnement efficace du service concerné.

C'est à l'organisme ou à l'entreprise qui requiert le renseignement d'établir que ce dernier est nécessaire. Il est donc essentiel, dès la conception d'un système de transaction en ligne, de spécifier avec précision pourquoi chacune des informations personnelles demandées est nécessaire.

---

268 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, ci-après citée Loi sur l'accès; *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, ci-après citée Loi sur le secteur privé.

269 (1986) C.A.I. 236.

La nécessité s'apprécie évidemment en fonction de l'activité et du service concerné. Elle découle non seulement des exigences intrinsèques à la transaction prise isolément mais de l'ensemble du contexte dans lequel s'inscrit l'activité. Ainsi, dans sa décision *Bellerose* c. *Université de Montréal*, la Commission d'accès conclut que le numéro de téléphone résidentiel était, dans le contexte technique, budgétaire et contractuel de l'organisme public, un renseignement requis pour assurer la fourniture du service.

En vertu de ce principe, seules les informations nécessaires doivent être exigées, recueillies et traitées. La nécessité s'apprécie évidemment en fonction du contexte et des fins pour lesquelles l'information est recueillie.

Les finalités en vue desquelles les données à caractère personnel sont utilisées doivent être déterminées au plus tard au moment de leur collecte. Ces finalités devront être spécifiées par celui qui exige des informations personnelles[270]. Elles devront aussi être portées à la connaissance de la personne concernée.

Ce principe s'inscrit dans une logique voulant que la personne concernée puisse exercer un droit de contrôle sur les renseignements. Lorsqu'il est informé de la finalité pour laquelle on lui demande de fournir des informations personnelles, l'utilisateur est en mesure de formuler un consentement éclairé pour leur collecte.

Les renseignements personnels ne peuvent être utilisés que pour les fins pour lesquels ils ont été recueillis. Si de nouvelles finalités apparaissent, il faut s'assurer d'obtenir le consentement approprié de l'intéressé avant de faire usage des renseignements personnels.

La divulgation ou la transmission des données aux tiers est possible si cela est nécessaire : à l'exécution du contrat entre les parties, au respect d'une obligation légale imposée par une autorité, à la sauvegarde de l'intérêt vital de la personne, à l'exécution d'une mission d'intérêt public, à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement.

Autrement, les données à caractère personnel ne peuvent pas être divulguées, ni transmises à des tiers qu'avec le consentement de la personne concernée[271] ou lorsqu'une règle de droit le permet[272].

C'est pourquoi il faut en tout temps être en mesure d'indiquer quelles sont les utilisations qui sont faites des informations personnelles demandées et détenues.

b) La détention limitée dans le temps

Le principe de la retenue vaut également pour la durée pendant laquelle les renseignements personnels sont détenus. Les informations personnelles ne doivent être détenues que dans la

---

270 Loi sur l'accès, art. 65; Loi sur le secteur privé, art. 8.

271 Voir article 13 de la Loi sur le secteur privé. et 37 du C.c.Q.

272 Voir article 18 de la Loi sur le secteur privé.

mesure où elles sont nécessaires à l'accomplissement de la fin pour laquelle elles ont été recueillies. Ainsi, l'article 73 de la Loi sur l'accès prévoit que les organismes publics ont l'obligation de détruire le renseignement nominatif ou de le traiter conformément à la loi sur les archives lorsque l'objet pour lequel il a été recueilli est accompli. Au-delà de la période où le renseignement est utilisé, ces informations doivent être retirées et archivées de manière à en assurer le caractère confidentiel.

c) La qualité des données

Il faut s'assurer du maintien de la qualité des données personnelles. Celles-ci doivent être maintenues exactes et à jour de manière à servir aux fins pour lesquelles elles sont recueillies et détenues (Loi sur l'accès, art. 72, Loi sur le secteur privé, art. 11). L'article 6)1c) de la *Directive européenne* spécifie que de telles données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ».

La législation québécoise repose sur le même souci. Cela appelle la mise en place d'une gestion rigoureuse des données personnelles au sein de toutes les organisations qui en détiennent. Cette obligation se double d'un devoir d'assurer la sécurité.

d) Les garanties de sécurité

La législation québécoise exige que soient prises des mesures de sécurité propres à assurer le caractère confidentiel des renseignements[273]. Le caractère raisonnable de ces mesures doit être évalué dans le contexte d'Internet[274]. Les mesures doivent être élaborées en fonction du degré de sensibilité des renseignements.

Ces garanties de sécurité peuvent comprendre :

- des mesures d'ordre matériel. Ex. : verrouillage des portes et cartes d'identification;
- des mesures structurelles. Ex. : les niveaux hiérarchiques en ce qui concerne l'accès aux données;

---

273 Loi sur le secteur privé, art. 10 et 17.

274 L'article 17(1) de la *Directive européenne* précise que : «1. Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Voir également les article 7 et 8 de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*.

- des mesures informationnelles. Ex. : le chiffrement et la surveillance des activités inhabituelles susceptibles de présenter un danger et des mesures destinées à y faire face. (le protocole Secure Socket Layer "SSL").

Le concepteur doit se doter de règles de conduite précisant ses devoirs et obligations à l'égard des renseignements personnels. Quant aux employés, voici quelques mesures devant être prises :

- un code d'accès et un mot de passe pour accéder aux systèmes;
- l'accès limité en fonction des nécessités administratives;
- la signature d'un protocole de confidentialité;
- la journalisation des consultations des renseignements personnels.

En plus il est nécessaire que tous les préposés soient adéquatement informés des mesures mises en place[275].

e) La transparence

L'utilisateur doit être en mesure de déterminer facilement l'existence et la nature des données à caractère personnel et les finalités de leur utilisation[276]. Il faut expliquer de façon claire et simple quel type d'information personnelle est recueillie, dans quel but et expliquer la manière dont cette information est traitée[277]. L'utilisateur ne doit pas être laissé dans un état d'incertitude quant à la politique du site concernant la protection des renseignements personnels. Ainsi le concepteur d'un environnement doit éviter que soient recueillies des informations personnelles sans que les utilisateurs soient informés au préalable de la façon dont ces renseignements seront traités et utilisés.

Dans le secteur public, l'établissement d'un fichier de renseignements nominatifs doit faire l'objet d'une déclaration à la Commission d'accès. Cette déclaration doit comporter les indications suivantes :

1° la désignation du fichier, les types de renseignements qu'il contient, l'usage projeté de ces renseignements et le mode de gestion du fichier;

2° la provenance des renseignements versés au fichier;

3° les catégories de personnes concernées par les renseignements versés au fichier;

---

275 Voir CAI, *L'accès à l'information et la confidentialité des renseignements personnels sur l'autoroute de l'information*, septembre 1995, http://www.cai.gouv.qc.ca/auto.htm et OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, 1980.

276 Loi sur le secteur privé, art. 8 et 27; Loi sur l'accès, art. 65 et 83.

277 The Australian Privacy Commissioner's Website, "Guidelines for Federal and ACT Government World Wide Websites", http://www.privacy.gov.au/issues/p7_2.html, page 1 de 4.

4° les catégories de personnes qui auront accès au fichier dans l'exercice de leurs fonctions;

5° les mesures de sécurité prises au sein de l'organisme pour assurer le caractère confidentiel des renseignements nominatifs et leur utilisation suivant les fins pour lesquelles ils ont été recueillis;

6° le titre, l'adresse et le numéro de téléphone de la personne responsable de la protection des renseignements personnels;

7° les modalités d'accès offertes à la personne concernée;

8° toute autre indication prescrite par règlement du gouvernement.

La déclaration doit être faite conformément aux règles établies par la Commission d'accès à l'information.

f) La responsabilité

Celui qui procède ou fait procéder au traitement des données à caractère personnel assume la responsabilité qui en découle. Il lui incombe de prendre toutes les mesures requises afin que les principes relatifs à la protection des renseignements personnels aient plein effet.

g) La participation individuelle

Ce principe fait écho au droit de la personne concernée de s'informer de l'existence d'un dossier la concernant et de modifier ou effacer les informations erronées.

Ainsi, la personne a un droit d'accès à son dossier[278], ce qui emporte l'obligation de permettre l'accès à ce dossier d'une manière simple et facile. Le plus souvent, on cherchera à assurer les accès à ces dossiers par un mécanisme en ligne.

En outre, la personne concernée doit avoir la possibilité de corriger ou effacer les informations erronées ou incomplètes la concernant[279]. Elle dispose d'un droit de recours lorsque ces droits lui sont refusés[280].

---

278 Voir les articles 38 à 40 du C.c.Q; Loi sur le secteur privé, art. 27 et ss.; Loi sur l'accès, art. 83 et ss.

279 Ce principe a inspiré l'article 12 de la *Directive européenne*. Loi sur l'accès, art. 89 et ss.; Loi sur le secteur privé, art. 28; art. 40 C.c.Q.

280 Loi sur le secteur privé, art. 42 à 53; Loi sur l'accès, art. 135 et ss.

7.3.3 Les devoirs et obligations relatifs au traitement et à l'utilisation de l'information identifiante

Au Québec, la loi[281]. consacre le caractère confidentiel des renseignements personnels. Ainsi il est prévu un ensemble de mesures visant à encadrer la cueillette de renseignements personnels, leur utilisation, leur conservation et leur communication. Quant à son application, tous les renseignements qui concernent une personne physique et permettent de l'identifier sont visés.

a) La démonstration de la nécessité de la cueillette

En règle générale, il faut justifier d'un « intérêt sérieux et légitime » pour recueillir des renseignements personnels.[282] L'organisme public doit être en mesure de démontrer la nécessité d'un renseignement personnel, compte tenu de ses attributions ou d'un programme dont il assure la gestion[283]. Dans la mesure où la personne concernée y consent; la Loi ne fait que formuler les critères suivant lesquels la personne concernée doit être informée des modalités suivant lesquelles une autre personne peut recueillir ou utiliser des renseignements la concernant[284]. En effet, la loi établit une série de critères et d'exceptions concernant la collecte, la détention, l'utilisation et la non-communication des renseignements personnels. Ainsi, la personne constituant un dossier sur autrui doit, lorsqu'elle constitue le dossier, inscrire son objet et ne recueillir, par des moyens licites, que les renseignements nécessaires à l'objet du dossier[285]. Dans le secteur public, les seuls renseignements pouvant être recueillis sont ceux qui ont un lien de connexité avec les attributions de l'organisme ou du programme pertinent.

b) Le traitement

Une fois les données personnelles collectées d'autres obligations sont imposées par les lois :

- la personne qui détient des renseignements sur une autre personne doit prendre et appliquer des mesures de sécurité pour garantir leur confidentialité[286]
- des mesures doivent être prises pour que les renseignements collectés soient à jour et exacts[287]
- la personne concernée doit avoir la possibilité d'accéder à son dossier[288]

---

281 Loi sur le secteur privé, art. 10; Loi sur l'accès, art. 53; voir aussi le *Code civil du Québec*, articles 35 à 41.

282 C.c.Q., art. 37 et la Loi sur le secteur privé, art. 4.

283 Loi sur l'accès, art. 64.

284 L'art. 9 de la Loi sur le secteur privé indique toutefois les circonstances où un individu ne peut pas refuser de fournir un renseignement personnel. Ce sont les cas où la collecte est nécessaire à la conclusion ou à l'exécution d'un contrat, la collecte est autorisée par la loi ou s'il y a des motifs raisonnables de croire que la demande de biens, de services ou d'emploi de l'individu désirant conserver son anonymat n'est pas licite.

285 Loi sur le secteur privé, art. 4 et 5.

286 Loi sur le secteur privé, art. 10; Loi sur l'accès, art. 76.

287 Loi sur le secteur privé, art. 11; Loi sur l'accès, art 72.

- la personne concernée doit avoir la possibilité de rectifier les renseignements inexacts ou incomplets la concernant[289]

- certaines restrictions à l'accès peuvent être imposées[290].

- les différends quant au traitement des renseignements personnels doivent être soumis à la Commission d'accès à l'information suivant la procédure établie par la Loi[291].

c) L'utilisation et la communication des renseignements personnels

Quant à l'utilisation et la communication des renseignements personnels, il importe de s'assurer que :

- l'utilisation des renseignements est interdite lorsque leur objet initial a été accompli[292];

- la communication des renseignements personnels à des tiers est interdite sauf avec le consentement de la personne concernée ou si la loi le prévoit[293];

- un renseignement personnel n'est accessible à un mandataire ou agent de celle-ci sans le consentement de la personne concernée que si ce renseignement est nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat[294];

- une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel contenu dans un dossier qu'elle détient sur autrui dans certaines circonstances prévues par la loi [295]. L'organisme public a aussi cette possibilité mais lorsque cela est nécessaire à l'application d'une loi[296].

Type d'opération	Obligations découlant de la Loi sur le secteur privé	Obligations découlant de la Loi sur l'accès
La cueillette des renseignements personnels	➢ la personne doit avoir un « intérêt sérieux et légitime » pour recueillir des renseignements personnels ➢ il est nécessaire que la personne concernée consente à cette collecte d'informations. ➢ la personne constituant un dossier sur autrui doit, lorsqu'elle constitue le dossier, inscrire son objet ➢ la personne constituant un dossier sur autrui doit recueillir les renseignements person-	➢ L'organisme ne peut recueillir des renseignements nominatifs que si cela est nécessaire à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. ➢ L'organisme qui recueille un renseignement nominatif auprès de la personne concernée doit s'identifier ➢ Il doit informer la personne : ▪ du nom, de l'adresse de l'organisme

288 Loi sur le secteur privé, art. 27; Loi sur l'accès, art 83.

289 Loi sur le secteur privé, art. 29; Loi sur l'accès, art 89.

290 Loi sur le secteur privé, art. 37 à 41; Loi sur l'accès, art. 86 à 88.1.

291 Loi sur le secteur privé, art. 42 à 69; Loi sur l'accès, art 135.

292 Loi sur le secteur privé, art. 12; Loi sur l'accès, art. 73.

293 Loi sur le secteur privé, art. 13; Loi sur l'accès, art 59.

294 Loi sur le secteur privé, art. 20.

295 Loi sur le secteur privé, art. 18.

296 Loi d'accès, art. 59 et 67.

Type d'opération	Obligations découlant de la Loi sur le secteur privé	Obligations découlant de la Loi sur l'accès
	nels par des moyens licites ➢ seulement les renseignements nécessaires à l'objet du dossier peuvent être collectés ➢ une personne peut recueillir les renseignements personnels auprès d'un tiers si elle a un intérêt sérieux et légitime et si les renseignements sont recueillis dans l'intérêt de la personne concernée et ils ne peuvent être recueillis auprès de celle-ci en temps opportun ➢ une personne peut recueillir les renseignements personnels auprès d'un tiers si elle a un intérêt sérieux et légitime et si la cueillette auprès d'un tiers est nécessaire pour s'assurer de l'exactitude des renseignements ➢ la personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer : de l'objet du dossier; de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise; de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification.	public; ▪ de l'usage auquel ce renseignement est destiné; ▪ des catégories de personnes qui auront accès au renseignement; ▪ du caractère obligatoire ou facultatif de la demande; ▪ des conséquences pour la personne concernée ou du tiers, du refus de répondre à la demande; ▪ des droits d'accès et de rectification prévus à la loi. ➢ L'organisme peut recueillir des renseignements personnels auprès d'un organisme privé après en avoir informé la CAI. ➢ Un organisme peut communiquer un renseignement nominatif à toute personne si cela est nécessaire à l'application de la loi. ➢ L'organisme public doit inscrire à un registre toute communication de renseignements nominatifs.
Le traitement des renseignements personnels	➢ la personne qui détient des renseignements sur une autre personne doit prendre et appliquer des mesures de sécurité pour garantir leur confidentialité ➢ des mesures doivent être prises pour que les renseignements collectés soient à jour et exacts pour la prise de décision ➢ la personne concernée doit avoir la possibilité d'accéder à son dossier ➢ la personne concernée doit avoir la possibilité de rectifier les renseignements inexacts ou incomplets la concernant ➢ par ailleurs des restrictions quant à l'accès peuvent être imposées ➢ les différends quant au traitement des renseignements personnels doivent être soumis à la Commission d'accès à l'information suivant la procédure établie par la Loi.	Un organisme public doit veiller à ce que les renseignements nominatifs qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis. L'établissement d'un fichier fait l'objet d'une déclaration à la CAI.. Cette déclaration doit préciser : 1° la désignation du fichier, les types de renseignements qu'il contient, l'usage projeté de ces renseignements et le mode de gestion du fichier; 2° la provenance des renseignements versés au fichier; 3° les catégories de personnes concernées par les renseignements versés au fichier; 4° les catégories de personnes qui auront accès au fichier dans l'exercice de leurs fonctions; 5° les mesures de sécurité prises au sein de l'organisme pour assurer le caractère confidentiel des renseignements nominatifs et leur utilisation suivant les fins pour lesquelles ils ont été recueillis; 6° le titre, l'adresse et le numéro de téléphone de la personne responsable de la protection des renseignements personnels; 7° les modalités d'accès offertes à la personne concernée; 8° tout autre indication prescrite par règlement du gouvernement.

Type d'opération	Obligations découlant de la Loi sur le secteur privé	Obligations découlant de la Loi sur l'accès
L'utilisation et la communication des renseignements personnels	➢ l'utilisation des renseignements lorsque leur objet initial a été accompli est interdite, ➢ la communication des renseignements personnels à des tiers est interdite sauf avec le consentement de la personne concernée ➢ dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible à un mandataire ou agent de celle-ci sans le consentement de la personne concernée que si ce renseignement est nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat ➢ une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel contenu dans un dossier qu'elle détient sur autrui : à son procureur ou au procureur général, lors de la poursuite pour une infraction; à une personne ou à un organisme ayant pouvoir de contraindre à leur communication et qui les requiert dans l'exercice de ses fonctions; à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;.	Lorsque son objet est accompli, le renseignement doit être archivé conformément à la loi ou détruit.

Les principes de gestion de l'information personnelle doivent être connus des usagers. L'entreprise ou l'organisme peut mettre en place une politique de la vie privée (Privacy Policy) dans laquelle le public est informé des pratiques du site quant à l'identification des usagers, au traitement des renseignements personnels ainsi que des mesures de protection prises à l'égard de ces informations. Également, le public doit être informé des mécanismes d'identification automatique, tels les cookies ou les variables d'environnement.

8. La biométrie

La *Loi concernant le cadre juridique des technologies de l'information* prévoit des règles relatives à l'identification et à la localisation des objets, de manière à établir leur provenance ou leur destination, et ce, à l'aide d'un identifiant qui devrait être accessible au moyen d'un service de répertoire (article 46).

Le principe énoncé à l'article 43 est qu'on interdit d'exiger l'utilisation d'un procédé ou d'un dispositif pour établir l'identité d'une personne et qui porte atteinte à son intégrité physique (ex : puce implantée dans le corps, prélèvement d'une substance corporelle).

Cependant, le deuxième alinéa permet l'utilisation d'un dispositif permettant de retracer une personne (par exemple, un bracelet de localisation) dans le cas où le législateur le prévoit expressément en vue de protéger la santé des personnes ou la sécurité publique. Par exemple, ces procédés pourraient être utilisés afin de localiser des personnes atteintes de maladies laissant craindre qu'elles oublient le lieu de leur domicile. Ces dispositifs pourraient aussi servir en lieu et place de l'incarcération.

L'article 44 de la *Loi concernant le cadre juridique des technologies de l'information* vient baliser le recours à des mesures biométriques comme moyen d'identification.

Les traits de la personne peuvent être utilisés dans le cadre du processus d'identification fondés sur la physiologie naturelle d'une personne. On parle alors d'identification biométrique. La biométrie s'appuie sur la prise en compte d'éléments morphologiques uniques et propres des individus, tels que les caractères physiologiques ou les traits comportementaux automatiquement reconnaissables et vérifiables. Il existe deux catégories de technologies permettant de saisir des caractéristiques ou des mesures biométriques :

- **Les techniques d'analyse du comportement :**
  - la dynamique de la signature (la vitesse de déplacement du stylo, les accélérations, la pression exercée, l'inclinaison…);
  - la façon d'utiliser un clavier d'ordinateur (la pression exercée, la vitesse de frappe…).
- **Les techniques d'analyse de la morphologie humaine :**
  - les empreintes digitales;
  - la forme de la main;
  - les traits du visage;
  - le dessin du réseau veineux de l'œil (l'iris et la rétine);
  - la voix.

Par exemple, des dispositifs peuvent effectuer l'appariement entre une carte comportant une empreinte digitale et l'empreinte qui est présentée par le possesseur de la carte.

Le législateur limite le recours à l'identification par la biométrie en imposant les balises suivantes :

- ☞ Le consentement exprès de la personne est exigé.
    - o Le consentement de la personne est nécessaire pour vérifier ou confirmer son identité au moyen de mesures biométriques. On ne précise pas la forme que doit prendre ce consentement, mais son importance appelle de consigner ce consentement dans un document explicite.

- ☞ La prise de mesures ou de caractéristiques doit être minimale.
    - o On limite ici la quantité d'informations biométriques recueillies. L'identité ne peut être établie qu'en faisant appel au minimum de caractéristiques ou de mesures requises pour relier un individu à l'action qu'il pose.

- ☞ Le procédé utilisé doit permettre à la personne de savoir que des mesures portant sur ses caractéristiques biométriques sont prises. Par conséquent, on ne peut capter de telles caractéristiques à l'insu de la personne.

- ☞ Tout autre renseignement concernant la personne et obtenu suite à la saisie des mesures ne peut être utilisé à aucune autre fin que l'identification de cette personne.

Cette interdiction a pour but de protéger la personne contre l'utilisation de renseignements secondaires qui pourraient émaner de la saisie de mesures biométriques.

Par exemple, la cueillette d'une image de la rétine d'un individu dans le cadre d'un système de sécurité pourrait en certains cas déceler une maladie de l'œil. Cette information secondaire, en vertu du deuxième alinéa de l'article 44, ne pourrait être utilisée par l'employeur pour justifier une décision à son égard. De plus, cette information ne pourrait être dévoilée qu'au principal intéressé, et à sa demande s'il a connaissance qu'elle a été recueillie.

- ☞ Les caractéristiques doivent être détruites lorsque l'objet fondant la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

On confirme ici la règle du respect de la finalité pour laquelle les informations ont été recueillies ou conservées. Cet alinéa vise à empêcher que des dossiers biométriques soient conservés sans motif valable.

La *Loi* confère des pouvoirs spécifiques à la Commission d'accès à l'information (ci-après la CAI) en matière de biométrie.

La création d'une banque de données biométriques doit être préalablement divulguée à la CAI. Il en va de même pour toute banque de données biométriques existante même si elle n'est pas en service. Par conséquent, toute banque de données biométriques est sujette à une obligation de divulgation à la CAI.

La CAI peut rendre toute ordonnance concernant de telles banques, afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation, y compris

l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne. Elle peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction.

La CAI exerce un pouvoir étendu à l'égard des banques de données biométriques. Elle peut rendre toute ordonnance sur les règles qui gouverneront la confection, l'utilisation, la consultation, la communication et la conservation, y compris l'archivage ou la destruction de telles banques.

Elle peut aussi en suspendre ou interdire la mise en service ou en ordonner la destruction, si ses ordonnances ne sont pas respectées ou si la banque porte atteinte au respect de la vie privée.

9. La signature

La signature est une marque personnelle au signataire. Cette marque est apposée à un acte dans le but de manifester un consentement. C'est en cela que la signature a des effets de droit. Par le consentement qu'elle permet d'exprimer, elle emporte des effets. Des droits peuvent naître ou s'éteindre dès lors que la personne a exprimé son consentement par le moyen de la signature. Comme la signature peut engendrer des conséquences au plan des droits d'une personne, elle doit pouvoir être établie en preuve devant les tribunaux. L'article 2827 du CCQ définit ainsi la notion de signature :

> ***2827.*** *La signature consiste dans l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement*.

La définition de signature reconnaît que celle-ci a les fonctions d'identification et de manifestation de la volonté. Cette définition élargit les formes extérieures de la signature au-delà de la simple transcription d'un nom. De simples initiales, griffes, paraphes ou autres constituent des « marques personnelles » au sens de l'article 2827 du Code. Rien ne laisse supposer que la signature doive être manuscrite.

Traditionnellement, la transcription du nom a constitué une condition essentielle à la validité de la signature. Ainsi, « la tradition a voulu que c'est par l'apposition de son nom que le signataire atteste aussi bien de son identité que de sa présence à l'acte. C'est donc en reproduisant graphiquement le vocable sous lequel le signataire est désigné oralement qu'il signe valablement un contrat ou un testament »[297].

Avec la définition de l'article 2827, c'est une notion large de la signature qui prévaut et non celle que la tradition a léguée. On relèvera en effet que rien dans l'article 2827 n'indique que la signature doive comporter le nom du signataire. Les Commentaires du Ministre de la justice expliquent que :

> *Cette définition est suffisamment large pour comprendre par exemple un numéro de code spécifique permettant d'identifier une personne en matière d'inscriptions informatisées; en effet, la signature ne correspond pas uniquement à l'écriture qu'une personne fait de son nom*.[298]

La définition de signature énoncée au Code civil fait appel aux notions de « marque personnelle » et « d'usage courant » de cette marque comme manifestation du consentement. L'apposition de la

---

297 Marc VAN QUIKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », (1985) *Revue critique de jurisprudence Belge* 65, 104.

298 *Commentaires du ministre de la justice, le Code civil du Québec*, T. II, Québec, Les publications du Québec, 1993, p. 1771.

marque personnelle d'une personne sur un document implique un lien durable entre la signature et le document.

9.1 Une marque personnelle

Le premier ensemble de composantes de la signature consiste en une marque personnelle. Il faut donc préciser et déterminer ce qu'est une marque et ensuite déterminer ce qui fait qu'une telle marque est personnelle à un individu.

a) Une marque

La définition de la signature implique que celle-ci laisse des traces : c'est une marque. *Le Robert* définit la « marque » comme étant un « signe matériel, empreinte mise, faite sur une chose pour la distinguer, la reconnaître ou pour servir de repère. » Le mot désigne aussi une « trace naturelle dont l'origine est reconnaissable. » Un troisième sens est « tout ce qui sert à faire reconnaître, retrouver une chose. » enfin un quatrième sens reconnu du mot est : « Caractère, signe particulier qui permet de reconnaître, d'identifier quelque chose. »

En somme, la marque est un signe qui permet de distinguer une entité parmi la multitude. Mais en plus, la notion de marque comporte l'idée de trace : c'est un signe, donc une information qui persiste et qui permet de reconnaître, de distinguer.

b) Personnelle

La marque personnelle est celle qui est unique à l'individu. Elle est intimement associée à ce dernier et à personne d'autre.

Le certificat est unique à l'usager; il n'en existe aucun autre similaire. La signature est un « signe choisi » rappelle Isabelle Dauriac qui ajoute que « quand bien même des contraintes fonctionnelles encadreraient l'exercice de ce choix, son existence même manifeste indiscutablement l'absence de condition de forme tenant au nom et au graphisme. »[299]

Même lorsqu'il ne comporte pas le nom du titulaire de certificat, celui-ci est associé à une personne de manière unique. L'article 48 de la Loi concernant le cadre juridique des technologies de l'information reconnaît la possibilité d'utiliser un pseudonyme. Mais dans de telles situations, les services de certification doivent dévoiler le nom véritable de la personne qui utilise un tel pseudonyme à « toute personne légalement autorisée à obtenir ce renseignement. »

9.2 D'usage courant

La marque personnelle doit être « d'usage courant ». Dans le Robert, « courant » signifie « qui a cours d'une manière habituelle ». On peut se demander si le signataire peut changer de signe sans

---

299 Isabelle DAURIAC, *La signature*, Thèse de doctorat en droit, Université Panthéon-Assas (Paris II) 10 janvier 1997, p. 23.

que sa signature soit considérée irrégulière car elle ne serait pas d'usage courant. En droit français, Isabelle Dauriac constate que « si les tribunaux utilisent la référence au caractère habituel du signe pour apprécier la régularité de certaines signatures, ce caractère n'est pour eux qu'un simple indice de la régularité du signe. [300]» Par conséquent, la notion d'usage courant à l'égard de la signature renvoie à la régularité de l'usage, plutôt qu'à une obligation d'utilisation constante de la même signature, du même signe.

La notion « d'usage courant » doit être interprétée en fonction des règles classiques d'interprétation des lois. Ainsi, comme l'écrit Pierre-André Côté, « il faut donner aux mots le sens qu'ils ont dans la langue courante ». Par ailleurs, « les termes de la loi doivent être lus dans leur contexte global, selon leur sens grammatical et ordinaire en harmonie avec l'économie générale de la loi, avec son objet et avec l'intention du législateur »[301]. Ainsi, l'utilisation courante dans un contexte donné est celle qui est usuelle, au regard de chaque personne qui y a recours.

L'utilisation est courante eu égard au contexte au sein duquel s'effectue l'expression d'un consentement. Par exemple, on peut dans sa vie signer une seule fois un acte d'achat d'un immeuble et signer des milliers de chèques. Il est possible que dans le premier cas, la signature manuscrite soit plus appliquée que celle que l'on appose quotidiennement : cela n'en fait pas pour autant disparaître sa qualité « d'usage courant ». Compte tenu des habitudes et préférences de l'usager, les faits doivent indiquer un élément d' « habituel » aux fins de manifester un consentement. A contrario, l'utilisation ayant un caractère inhabituel ou autrement inusité qui donnerait à conclure que l'usager n'a pas pu déclencher le processus aux fins d'exprimer un consentement ne serait pas une utilisation courante.

L'expression « une marque personnelle qu'elle utilise de façon courante » suppose que cette marque soit susceptible de permettre l'identification d'une personne. Ainsi, on doit considérer comme répondant aux critères de l'article 2827, une marque qui permet d'identifier une personne avec une raisonnable certitude. À l'inverse, une marque n'offrant pas de garanties raisonnables doit être écartée. Enfin, rien dans le libellé de l'article 2827 ne s'oppose à ce qu'une même personne puisse utiliser plusieurs marques correspondant aux critères qui y sont énoncés.

9.3 Apposée à un acte

La signature est définie comme une marque apposée à un acte. La question de savoir si un signe ou une marque sont apposés à un acte est régie par les articles 38 et suivants de la *Loi concernant le cadre juridique des technologies de l'information*.

Avant l'amendement introduit par l'article 77 de la Loi concernant le cadre juridique des technologies de l'information, la disposition du Code civil parlait de marque apposée « sur un acte » laissant penser que seule la signature sur un support-papier était visée. En précisant que la

---

300 Isabelle DAURIAC, *La signature*, Thèse de doctorat en droit, Université Panthéon-Assas (Paris II) 10 janvier 1997, pp. 54 et 55.

301 Pierre-André CÔTÉ, *Interprétation des lois*, 2e éd., Cowansville, Les Éditions Yvon Blais, 1990, p. 365.

signature est faite « à un acte », le principe est neutre au plan des technologies. Il est nécessaire et suffisant que la signature soit associée à un acte.

La *Loi concernant le cadre juridique des technologies de l'information* vise à assurer l'établissement du lien qui permet de relier un document qui est sur un support faisant appel aux technologies de l'information à ceux qui communiquent par ce moyen. À cette fin, elle énonce les critères et les qualités requises des mécanismes utilisés afin d'établir un tel lien. L'article 38 de la Loi concernant le cadre juridique des technologies de l'information prévoit que :

> ***38.*** *Le lien entre une personne et un document technologique, ou le lien entre un tel document et une association, une société ou l'État, peut être établi par tout procédé ou par une combinaison de moyens dans la mesure où ceux-ci permettent :*
>
> *1° de confirmer l'identité de la personne qui effectue la communication ou l'identification de l'association, de la société ou de l'État et, le cas échéant, de sa localisation, ainsi que la confirmation de leur lien avec le document;*
>
> *2° d'identifier le document et, au besoin, sa provenance et sa destination à un moment déterminé*.

Autrement dit, pour déterminer si le mécanisme mis en place permet d'apposer des signatures à des documents, il faut se demander s'il rend possible l'association d'une marque personnelle à un document technologique.

9.4 Manifestant un consentement

La signature est une marque pouvant servir à une multitude de fins. Par exemple, un artiste peintre peut apposer sa signature sur une toile. Mais l'article 2827 du Code civil retient la notion de signature en tant que marque utilisée afin de manifester un consentement. On vise ici le volet intentionnel de la signature, celui qui s'attache à l'état d'esprit de la personne qui pose la marque au document. Pour engendrer des effets juridiques, c'est-à-dire pour obliger le signataire, il faut qu'il y une intention du signataire de se lier par le geste déclenchant la signature.

10. La certification

La « certification », dans son sens général, signifie « assurance donnée par écrit »; quant au mot « certifier », il signifie « assurer qu'une chose est vraie » (*Le Petit Robert*). Une section de la *Loi concernant le cadre juridique des technologies de l'information* traite des exigences à satisfaire dans le cadre d'activités visant à certifier une information, c'est-à-dire à établir ou à confirmer un fait.

Schématiquement, un tiers, digne de confiance, atteste d'un fait au bénéfice de ceux qui ont besoin de disposer d'un niveau approprié de certitude quant à l'existence de ce fait. Dans les transactions effectuées avec des documents technologiques, les certificats sont utilisés afin d'établir un ou plusieurs faits, comme la confirmation de l'identité d'une personne, l'identification d'une société ou encore confirmer l'exactitude d'un document, tel un identifiant.

En somme, la certification est un processus destiné à réduire l'incertitude. Il vise à procurer la quantité optimale d'information à l'égard d'une personne, d'un document, d'un objet, afin de pouvoir procéder à une transaction avec un niveau de risque acceptable.

La *Loi concernant le cadre juridique des technologies de l'information* édicte les principes et normes relatifs à l'utilisation des certificats et des répertoires et à l'encadrement des activités des personnes qui proposent des services de certification. La *Loi* prévoit les conditions régissant l'offre de services de certification ou de répertoire. Elle prévoit aussi un mécanisme d'accréditation volontaire des prestataires de service de certification et précise la responsabilité incombant à ceux qui émettent, utilisent ou se fient à un certificat.

10.1 Le certificat

Le certificat est la pierre angulaire du processus d'identification. Plusieurs articles de la loi prévoient son utilisation.

L'article 38 de la loi prévoit, entre autres, que le lien entre une personne et un document technologique peut être établi par tout procédé ou combinaison de moyens, en autant qu'ils permettent de confirmer l'identité de la personne, de l'association, de la société ou de l'État qui effectue la communication, et le cas échéant sa localisation, ainsi que son lien avec le document.

L'article 39 précise que la signature d'une personne peut servir à établir le lien entre elle et le document et être apposée au moyen de tout procédé qui satisfait les exigences de l'article 2827 du Code civil .

L'article 40 de la loi indique qu'une personne qui est appelée à confirmer l'identité d'une autre peut le faire entre autres au moyen d'un certificat.

On voit donc l'importance des certificats, lesquels servent, par exemple, à confirmer l'identité de la personne titulaire d'une clé publique, laquelle on utilise pour « vérifier » la signature que cette personne a effectuée numériquement au moyen de sa clé privée.

L'article 47 circonscrit la notion de certificat en déterminant ses fonctions. Il énonce de façon plus détaillée celles d'une catégorie particulière de certificat, soit le certificat d'attribut.

Un certificat peut servir à établir un ou des faits, dont la confirmation :

1- de l'identité d'une personne, d'une société d'une association ou de l'État;
2- de l'exactitude d'un identifiant (?) d'un document ou d'un autre objet;
(Le paragraphe 3° de l'article 46 précise ce qu'est un identifiant)
3- de l'existence de certains attributs (d'une personne, d'un document ou d'un autre objet). Par exemple, un certificat d'attribut peut confirmer le fait qu'une personne est un employé de la firme X.
4- du lien entre une personne, un document, un objet et un dispositif d'identification ou de localisation tangible ou logique.

Il faut noter la présence du mot « dont », qui signifie que les faits énumérés ne sont pas limitatifs.

Le certificat d'attribut est une catégorie particulière de certificat dont on précise les fonctions. Le certificat d'attribut peut servir

1- à l'égard d'une personne : à établir sa fonction, sa qualité, ses droits, pouvoirs ou privilèges au sein d'une personne morale, association, société, État ou dans le cadre d'un emploi.

Le troisième paragraphe de cet article comporte une mesure de protection de la vie privée**.** L'obtention de renseignements relatifs aux attributs d'une personne n'est pas automatique. L'accès à ce certificat doit être autorisé par la personne concernée ou par une personne en autorité par rapport à elle. Par exemple, dans une entreprise un employé peut faire l'objet d'un certificat d'attribut pour lui permettre d'effectuer certaines transactions en ligne. La personne en autorité dans cette entreprise qui a autorisé l'employé à agir ainsi peut vouloir garder le contrôle de l'accès au certificat d'attribut. Tout dépend du niveau de confiance qui existe entre les personnes dans une situation donnée.

Ce type de certificat sera donc utilisé à chaque fois qu'une personne agira autrement qu'en sa qualité strictement personnelle. Il peut aussi servir donc à établir le lien entre un mandant et un mandataire.

2- à l'égard d'une association, d'une société ou d'un emplacement où l'État effectue ou reçoit une communication : à établir leur localisation. Le terme « localisation » réfère à une « adresse officielle », plus ou moins formelle suivant les exigences commandées par le contexte. Par exemple, le certificat servirait à confirmer le siège d'une société.

3- à l'égard d'un document ou d'un autre objet : à confirmer l'information qui permet de l'identifier ou de le localiser ou de déterminer son usage ou le droit d'y avoir accès ou tout autre droit ou privilège afférent.

Il sera donc utile pour confirmer d'autres faits que l'exactitude de l'identifiant, par exemple s'il s'agit d'une oeuvre, le nom de l'auteur, les limites à l'utilisation et les droits d'auteur applicables le cas échéant.

10.2 Le contenu obligatoire du certificat

L'article 48 précise le contenu obligatoire des certificats.

> ***48.*** *Un certificat peut être joint directement à un autre document utilisé pour effectuer une communication ou être accessible au moyen d'un répertoire lui-même accessible au public.*
>
> *Le certificat doit au moins comprendre les renseignements suivants :*
>
> *1° le nom distinctif du prestataire de services qui délivre le certificat ainsi que sa signature;*
>
> *2° la référence à l'énoncé de politique du prestataire de services de certification, y compris ses pratiques, sur lequel s'appuient les garanties qu'offre le certificat qu'il délivre;*
>
> *3° la version de certificat et le numéro de série du certificat;*
>
> *4° le début et la fin de sa période de validité;*
>
> *5° s'il s'agit d'un certificat confirmant l'identité d'une personne, l'identification d'une association, d'une société ou de l'État, leur nom distinctif ou, selon le cas, s'il s'agit d'un certificat confirmant l'exactitude de l'identifiant d'un objet, cet identifiant;*
>
> *6° s'il s'agit d'un certificat d'attribut, la désignation de l'attribut dont le certificat confirme l'existence et l'identification de la personne, de l'association, de la société, de l'État ou de l'objet auquel il est lié.*
>
> *Le nom distinctif d'une personne physique peut être un pseudonyme, mais le certificat doit alors indiquer qu'il s'agit d'un pseudonyme. Les services de certification sont tenus de communiquer le nom de la personne à qui correspond le pseudonyme à toute personne légalement autorisée à obtenir ce renseignement.*

Le contenu d'un certificat revêt une importance primordiale, car le degré de fiabilité qu'on lui attribuera est tributaire de la profondeur, de la précision et de la mise à jour des informations qu'on y retrouvera. Cet article édicte le contenu minimum obligatoire d'un certificat.

Suivant le paragraphe 1° de cet article, le prestataire de services doit signer le certificat qu'il délivre : ceci implique qu'une autorité supérieure aura certifié l'identité de ce prestataire.

Suivant le paragraphe 2°, le certificat doit contenir une référence à l'énoncé de politique du prestataire de services : celui-ci doit être accessible, facile à consulter. Cet énoncé doit comprendre les éléments qui sont de nature à rassurer l'utilisateur, comme ses pratiques sur lesquelles il appuie ses garanties.

Le contenu minimal de l'énoncé de politique est détaillé à l'article 52 de la loi : par exemple, la valeur numérique de la clé publique émise, l'identifiant de l'algorithme, les normes et standards techniques utilisés.

La version du certificat doit être indiquée : elle donne l'indication de sa mise à jour.

La mention de la période de validité est requise par le paragraphe 4°. Cette information est très importante, et l'utilisateur d'un certificat doit y apporter une attention particulière. En effet,

l'article 60 de la loi impose certaines obligations de vérification, dont celle relative à la validité du certificat, à la personne qui veut agir en se fondant sur un certificat.

Le nom distinctif d'une personne physique indiqué au certificat peut être un pseudonyme, avec l'indication que c'en est un. Cependant les services de certification doivent dévoiler le nom véritable de la personne qui utilise un tel pseudonyme à « toute personne légalement autorisée à obtenir ce renseignement ». Par exemple, les agents de la paix dans l'exercice de leurs fonctions de prévention des infractions pourraient obtenir un tel renseignement. C'est donc dire que l'emploi d'un certificat est compatible avec l'usage d'un pseudonyme pour préserver, dans le respect de la loi, l'anonymat des personnes comme c'est le cas actuellement pour les transactions effectuées dans les kiosques ou les magasins.

L'article 49 vise à assurer, dans le contexte des technologies de l'information, que l'on sache à qui on a affaire, par exemple lorsqu'on communique avec une personne morale et que l'action de cette dernière doit être posée par l'intermédiaire d'une personne autorisée.

> ***49.*** *Le certificat confirmant l'identification d'une personne morale, d'une association, d'une société ou de l'État, lorsque l'un d'eux doit agir par l'intermédiaire d'une personne autorisée, doit indiquer qui agit ou, à défaut, la personne physique qui agit doit joindre un ou des certificats qui confirment ce fait.*

Par exemple, lorsqu'une paire de clés (clé publique-clé privée) est attribuée à une personne morale, le certificat doit indiquer quelle personne physique détient la clé privée liée à la clé publique de cette personne morale, et agit au nom de celle-ci. À défaut, la personne physique qui agit doit joindre un autre certificat confirmant son autorité pour représenter cette personne morale.

10.3 Le répertoire

L'article 50 circonscrit la notion de répertoire. Il définit le type de répertoire visé par cette loi en se référant aux fonctions qu'il peut remplir.

> ***50.*** *Le répertoire qui a pour fonction d'identifier ou de localiser une personne ou un objet, de confirmer l'identification d'une association ou d'une société ou de localiser l'une d'elles, de confirmer l'identification de l'État ou de localiser un emplacement où celui-ci effectue ou reçoit communication, ou encore d'établir un lien entre l'un d'eux et un objet doit être constitué conformément aux normes ou standards techniques approuvés par un organisme reconnu visé à l'article 67.*
>
> *Le répertoire doit être accessible au public, soit directement ou au moyen d'un dispositif de consultation sur place ou à distance, soit à l'aide d'une procédure d'accès aux différents domaines d'un réseau susceptibles de confirmer la validité d'un identifiant, d'un certificat ou d'un autre renseignement qu'il comporte.*
>
> *Toutefois, le répertoire ne peut rendre public le motif pour lequel un certificat a pu être suspendu ou annulé.*

Ainsi le répertoire peut servir à :

1- identifier ou localiser une personne ou un objet;
2- confirmer l'identification d'une association ou d'une société ou localiser l'une d'elles;
3- confirmer l'identification de l'État ou localiser un emplacement où celui-ci effectue ou reçoit une communication; ou
4- établir un lien entre l'un d'eux et un objet.

Ces rôles se réfèrent plutôt aux « services de répertoire » dont parle l'article 51 de la loi . Il faut comprendre ici que c'est par le biais des procédés ou moyens qu'il renferme que le répertoire peut réaliser ces fonctions, qu'il est en fait un lieu virtuel d'où ces instruments sont accessibles. Par exemple, une clé publique d'un titulaire de biclés peut être accessible au public par le répertoire où elle est stockée et publiée. Ce n'est pas le répertoire lui-même qui permet d'identifier cette personne, mais bien le certificat qui fait le lien entre elle et sa clé publique.

En fait un répertoire est un instrument, une sorte de bottin, dans lequel on recherche l'identification ou la localisation d'une personne.

Il est primordial que le répertoire soit accessible au public, eu égard à ses fonctions. Il peut l'être de différentes façons :

1- directement;
2- par un dispositif de consultation sur place ou à distance; ou
3- à l'aide d'une procédure d'accès aux différents domaines d'un réseau susceptibles de confirmer la validité :
   i) d'un identifiant;
   ii) d'un certificat; ou
   iii) d'un autre renseignement qu'il comporte.

Un certificat pouvant être annulé ou suspendu pour des raisons parfois confidentielles ou personnelles, il est prévu que le répertoire ne peut rendre public le motif de son annulation ou de sa suspension. Dans certains cas, cela pourrait indûment porter atteinte à la réputation de la personne concernée.

10.4 Les services de certification et de répertoire

L'expression « prestataire de services » a un sens assez général dans la loi. Elle réfère à toute personne appelée à fournir des services structurés dans un réseau de communication utilisant des technologies de l'information. On retrouve aussi cette expression entre autres aux articles 22, 26, 27, 36, 37 dans un autre contexte. On appelle aussi « autorité de certification » l'entité qui propose ce genre de services. La loi indique qu'une personne ou l'État peut le faire, et qu'un prestataire de services peut offrir l'un ou l'autre des services de certification ou de répertoire, ou les deux à la fois. Ces services peuvent être fournis par des entités différentes. L'article 51 dispose à cet égard que :

> ***51.*** *Les services de certification et de répertoire peuvent être offerts par une personne ou par l'État*.

> *Les services de certification comprennent la vérification de l'identité de personnes et la délivrance de certificats confirmant leur identité, l'identification d'une association, d'une société ou de l'État ou l'exactitude de l'identifiant d'un objet. Les services de répertoire comprennent l'inscription des certificats et des identifiants dans un répertoire accessible au public et la confirmation de la validité des certificats répertoriés ainsi que leur lien avec ce qu'ils confirment.*
>
> *Un prestataire de services peut offrir ces services en tout ou en partie.*

Les services de certification comprennent :

1- la vérification de l'identité de personnes et la délivrance de certificats confirmant leur identité. L'article 40 de la loi traite de la vérification et de la confirmation d'identité.
2- l'identification d'une association, d'une société ou de l'État; et
3- la vérification de l'exactitude de l'identifiant d'un objet.

Les services de répertoire comprennent :

1- l'inscription des certificats et des identifiants dans un répertoire accessible au public; et
2- la confirmation de la validité des certificats issus du répertoire concerné et leur lien avec ce qui est confirmé.

L'article 50 de la loi décrit les fonctions des répertoires.

Voici quelques exemples de personnes ou entités qui pourraient agir comme prestataires de services (autorité de certification) en regard de l'identité des personnes :

Des tiers de confiance :

1- une institution financière;
2- une entreprise spécialisée dans ce service;
3- un notaire.

Des personnes détenant l'autorité requise :

1- une université par rapport à ses étudiants;
2- l'État par rapport à ses citoyens;
3- l'employeur en regard de ses employés.

Le gouvernement pourrait aussi certifier certaines informations ou documents émanant des ministères et organismes publics et parapublics, ou concernant ses employés.

10.5 L'énoncé de politique

L'article 52 identifie les questions sur lesquelles les prestataires de services doivent fournir de l'information aux utilisateurs.

> ***52.*** *L'énoncé de politique d'un prestataire de services de certification ou de répertoire indique au moins :*

1° ce qui peut être inscrit dans un certificat ou un répertoire et, dans ce qui y est inscrit, l'information dont l'exactitude est confirmée ainsi que les garanties offertes à cet égard par le prestataire;

2° la périodicité de la révision de l'information ainsi que la procédure de mise à jour;

3° qui peut obtenir la délivrance d'un certificat ou faire inscrire de l'information au certificat ou au répertoire;

4° les limites à l'utilisation d'un certificat et d'une inscription contenue au répertoire, dont celle relative à la valeur d'une transaction dans le cadre de laquelle ils peuvent être utilisés;

5° l'information permettant de déterminer, au moment d'une communication, si un certificat ou un renseignement inscrit au certificat ou au répertoire par un prestataire est valide, suspendu, annulé ou archivé;

6° la façon d'obtenir de l'information additionnelle, lorsqu'elle est disponible mais non encore inscrite au certificat ou au répertoire;

7° la politique relative à la confidentialité de l'information reçue ou communiquée par le prestataire;

8° le traitement des plaintes;

9° la manière dont le prestataire dispose des certificats en cas de cessation de ses activités ou de faillite.

L'énoncé de politique du prestataire de services de certification ou de répertoire doit être accessible au public.

L'énoncé de politique est un ensemble d'informations qui vise notamment à permettre à l'utilisateur d'un certificat de se faire une idée sur les niveaux de qualité et de sécurité rattachés à celui-ci, ainsi que d'indiquer les principales obligations auxquelles le prestataire de services est astreint. Ce dernier peut en effet limiter la valeur des transactions pour lesquelles le certificat peut être utilisé.

L'accessibilité par le public à l'énoncé de politique est impérative : le moyen d'y accéder fait d'ailleurs partie des mentions devant obligatoirement être incluses dans le certificat, en vertu du paragraphe 2° de l'article 48 de la loi .

Le contenu de l'énoncé de politique

Les informations que doit contenir l'énoncé de politique suivant cet article correspondent à des exigences minimales. Le prestataire de services peut donc rajouter les items qu'il juge pertinents ou utiles eu égard au type de certificat qu'il émet et à la clientèle visée. Ces informations minimales sont :

1- les éléments que l'on retrouvera dans le certificat ou le répertoire concerné. L'énoncé indique entre autres :

   i) quelle information est confirmée de façon exacte; et

ii) les garanties que le prestataire offre à cet égard : ceci revêt une extrême importance. En effet, le prestataire de services doit indiquer quelles procédures, normes et standards spécifiques il utilise pour les fins de garantir l'intégrité, la sécurité et la confidentialité des données qu'il recueille, gère et conserve.

2- les items permettant de savoir dans quelle mesure le certificat que l'on consulte est à jour;

3- les critères utilisés par le prestataire de services pour déterminer qui a le droit de faire émettre un certificat et de le faire modifier : lorsqu'il s'agit d'un individu, ceci ne cause pas trop de problèmes. Par contre, s'il s'agit d'une société qui veut faire émettre un certificat pour permettre à un de ses dirigeants de signer numériquement des documents en son nom, il faut que le prestataire de services ait préalablement établi ses exigences relatives à la preuve qu'il demandera en regard de l'autorité de la personne qui fera une telle demande au nom de la société. Ceci impliquera nécessairement un autre niveau de certification, et le prestataire devra faire part de sa politique à cet égard;

4- les restrictions quant à l'utilisation d'un certificat : ce sont des éléments que l'utilisateur devra scruter minutieusement, particulièrement eu égard aux dispositions de l'article 61 de la loi qui prévoit un régime de responsabilité particulier à l'égard des personnes impliquées, soit comme utilisateur, soit comme prestataire de services. Ce dernier pourra faire sa preuve plus facilement si ces limites sont clairement établies. La limite relative à la valeur de la transaction concernée sera vraisemblablement en corrélation avec le niveau du certificat émis, dont le prix sera aussi établi en fonction du risque encouru.

5- la manière dont le prestataire indique, au moment de la communication concernée, le statut du certificat (valide, suspendu, annulé ou archivé);

6- comment l'utilisateur peut obtenir de l'information qui devrait être inscrite au certificat ou au répertoire mais qui n'y figure pas encore;

7- la politique du prestataire quant à la confidentialité des informations dont il dispose : il est clair que cette question est l'une de celles qui préoccupent le plus les utilisateurs actuels et futurs de ces services et que cette politique devra comprendre entre autres une référence à l'utilisation de normes et standards reconnus pour les fins de protection de la vie privée des personnes;

8- le traitement des plaintes : il peut s'agir par exemple d'une procédure d'arbitrage; et

9- le sort des certificats en cas de faillite ou de cessation des activités du prestataire de services : cet item est crucial, car ces événements pourraient bien entraîner une brèche importante dans une infrastructure de certification si un élément de la pyramide devenait tout d'un coup absent ou inutilisable, causant un tort immense aux personnes ou entreprises impliquées. Il faut donc que le prestataire de services prévoie une solution qui assurera la pérennité de l'accessibilité aux certificats dont il dispose et aux services de répertoire qu'il offre, le cas échéant.

10.6 L'accréditation

L'article 53 prévoit la création d'un régime d'accréditation volontaire des prestataires de services de certification.

> ***53.*** *Le prestataire de services de certification peut adhérer à un régime d'accréditation volontaire. L'accréditation est accordée, eu égard aux exigences à satisfaire en vertu du paragraphe 3° de l'article 68, par une personne ou un organisme désigné par le gouvernement.*
>
> *Les mêmes critères sont appliqués quelle que soit l'origine territoriale du prestataire. L'accréditation fait présumer que les certificats délivrés par le prestataire répondent aux exigences de la présente loi.*

L'accréditation d'un prestataire de services est effectuée sur une base volontaire. Cependant l'accréditation comporte un avantage important : les certificats délivrés par un prestataire accrédité sont présumés être conformes aux exigences de la loi, en vertu du 2° paragraphe de cet article. L'utilisateur d'un certificat émis par une autorité accréditée n'aura donc pas à vérifier si les exigences minimales de la loi sont rencontrées. Les prestataires soumis à la juridiction du Québec doivent se conformer aux exigences de ses lois, mais l'utilisateur n'est pas toujours en mesure de vérifier si cette conformité existe.

De plus, dans le cas de prestataires de services qui ne seraient pas assujettis pour quelque raison que ce soit à la juridiction du Québec, le fait d'obtenir une telle accréditation en vertu de l'article 54 de la loi sera de nature à rassurer les utilisateurs de leurs certificats. Les mêmes critères sont appliqués, quelle que soit l'origine territoriale du prestataire. On applique ici le principe de la non discrimination quant à l'origine territoriale des prestataires de services de certification mis de l'avant par la CNUDCI .

L'accréditation ne comporte pas de garantie quant à la valeur ou la validité des certificats ou de leur contenu.

Le paragraphe 3° de l'article 68 de la loi prévoit que le gouvernement peut déterminer par règlement :

1- la procédure d'accréditation;

2- les conditions d'octroi;

3- les délais d'obtention de l'accréditation ou d'une modification de ses conditions;

4- les conditions relatives au renouvellement, à la suspension ou à l'annulation de l'accréditation; et

5- les frais afférents.

Selon quels critères

L'article 55 de la loi indique sur quels critères minimums on se base pour accorder une accréditation, et qui s'ajoutent à l'information contenue dans l'énoncé de politique.

L'inscription dans un registre

Le paragraphe 2° de l'article 54 prévoit que les prestataires accrédités ou dont les services sont reconnus équivalents doivent être inscrits dans un registre accessible au public.

10.7 La reconnaissance mutuelle et l'équivalence des certificats

Étant donné le caractère transfrontalier des communications qui surviennent sur Internet, il est important que les certificats émis par des prestataires de services en fonction d'autres normes, mais qui peuvent être valables, soient reconnus. L'article 54 prévoit la possibilité de faire des ententes de reconnaissance mutuelle des certificats délivrés ailleurs qu'au Québec.

> ***54.*** *Les certificats délivrés par un prestataire de services de certification en fonction d'autres normes que celles applicables au Québec peuvent être considérés équivalents aux certificats délivrés par un prestataire de services de certification accrédité. L'équivalence doit être constatée par la personne ou l'organisme désigné par le gouvernement pour conclure des ententes de reconnaissance mutuelle de tels certificats avec l'autorité désignée qui a établi ces normes. Il en est de même pour les services de répertoire.*
>
> *Les prestataires accrédités ou dont les services sont reconnus équivalents à ceux d'un prestataire accrédité doivent être inscrits dans un registre accessible au public tenu par la personne ou l'organisme qui a constaté l'équivalence.*

Cette reconnaissance mutuelle permet d'assurer que les certificats délivrés ailleurs qu'au Québec sont de qualité équivalente à ceux délivrés par les prestataires accrédités, ce qui permet à la fois l'harmonisation des certificats à l'échelle internationale et procure une assurance que ces certificats sont dignes de confiance.

Cet article dispose que le prestataire dont les services sont reconnus équivalents est considéré comme ayant le même statut qu'un prestataire accrédité.

Par exemple, un prestataire d'une autre origine territoriale que le Québec qui rencontre toutes les normes applicables au Québec pourrait obtenir son accréditation sans passer par le système de l'équivalence. Par contre, s'il ne rencontre pas toutes ces normes (par exemple il n'utiliserait pas exactement la même technologie que celle qui pourrait être prescrite par règlement au Québec, mais qui serait équivalente), il pourrait demander que ses services soient reconnus équivalents et ainsi bénéficier des effets de l'accréditation, soit la présomption de conformité en vertu de l'article 53 de la loi.

Le comité pour l'harmonisation des systèmes et des normes a entre autres pour mission, suivant le paragraphe 3° de l'article 63 de la loi, « de favoriser la standardisation des certificats et des répertoires ainsi que la reconnaissance mutuelle des certificats ». Le gouvernement désigne la personne ou l'organisme qui est appelé à constater de telles équivalences et à conclure des ententes de reconnaissance mutuelle avec l'organisme qui a établi les normes dont l'équivalence est reconnue. Ceci vaut autant pour les services de certificat que de répertoire.

L'inscription dans un registre

Le 2° paragraphe de cet article prévoit que les prestataires accrédités ou dont les services ont été reconnus équivalents doivent être inscrits dans un registre accessible au public, tenu par la personne ou l'organisme qui a constaté l'équivalence.

> ***55.*** *Pour la délivrance ou le renouvellement d'une accréditation, il est tenu compte, outre l'information contenue dans l'énoncé de politique proposé, au moins :*
>
> *1° du fait que l'identité de la personne qui fait la demande est établie;*
>
> *2° de l'étendue de l'expertise, de l'infrastructure mise en place, des services offerts ainsi que de la régularité et l'étendue des audits effectués;*
>
> *3° de la disponibilité de garanties financières pour exercer l'activité;*
>
> *4° des garanties offertes quant à l'indépendance et à la probité du prestataire de services de certification ainsi que de la politique qu'il a établie pour garantir l'expertise et la probité des personnes qui les dispense;*
>
> *5° des garanties d'intégrité, d'accessibilité et de sécurité des répertoires ou des certificats fournis;*
>
> *6° de l'applicabilité des politiques énoncées et, en cas de renouvellement, de leur application ainsi que du respect des autres obligations qui incombent à un prestataire de services*.
>
> (**NOTE** : faute de conjugaison au par. 4° : « qui les dispense**nt** »)

Cet article expose les facteurs qui seront examinés lors d'une accréditation, comme les garanties financières et l'étendue de l'expertise offerte.

Les critères de délivrance et de renouvellement de l'accréditation

L'entité qui délivre ou renouvelle une accréditation doit tenir compte des informations et faits suivants :

1- les informations qui se retrouvent dans l'énoncé de politique du prestataire de services, dont les mentions minimales obligatoires sont prescrites par l'article 52 de la loi.

2- l'identité du prestataire de services doit pouvoir être établie hors de tout doute : donc, par exemple dans le cas d'une société étrangère, il faut avoir une confirmation blindée de son existence eu égard à la loi en vertu de laquelle elle a été créée.

3- l'étendue de l'expertise, de l'infrastructure mise en place, des services offerts : il s'agit ici d'évaluer le sérieux des connaissances et des outils utilisés pour offrir des services de certification sécuritaires et fiables.

4- la régularité et l'étendue des audits effectués : le paragraphe 5° de l'article 63 de la loi prévoit que le comité pour l'harmonisation des systèmes et des normes a pour mission d'examiner les moyens susceptibles d'uniformiser, entre autres, les pratiques d'audit.

5- la disponibilité des garanties financières pour exercer l'activité : il faudra que le prestataire de services démontre un bilan financier solide et prouve qu'il peut faire face aux obligations engendrées par son activité, soit par le biais d'assurances ou autrement.

6- les garanties que le prestataire de services offre en regard de :
   i) son indépendance et sa probité : il s'agit ici de vérifier, par exemple, les moyens prévus et pris par le prestataire de services pour éviter d'être placé dans une situation de conflit d'intérêt dans l'exercice de son activité. Le 1° paragraphe de l'article 56 est clair à cet effet.
   ii) sa politique établie pour les fins de garantir l'expertise et la probité des personnes qui dispensent les services.
   iii) l'intégrité, l'accessibilité et la sécurité des répertoires ou des certificats fournis : ces garanties sont fondamentales pour rassurer les utilisateurs de ces services.

7- l'applicabilité des politiques énoncées : il s'agit d'évaluer s'il s'agit de voeux pieux ou si elles sont effectivement réalisables.

8- en cas de renouvellement, l'application réelle des politiques énoncées et le respect des autres obligations qui lui incombent.

10.8 Les obligations du prestataire de services de certification

L'article 56 prévoit certaines des obligations auxquelles sont assujettis les prestataires de services de certification. On retrouve aussi dans d'autres articles de la loi des dispositions qui énoncent des obligations qui sont aussi applicables à ces prestataires. Il faut souligner que l'article 61 de la loi indique que le prestataire de services de certification et de répertoire est tenu à une obligation de moyens à l'égard des obligations qui lui incombent en vertu de cette loi. Il peut cependant être quand même tenu responsable sans égard à sa faute en certaines circonstances énoncées au 2° paragraphe de cet article 61.

1- Les obligations de l'article 56

Cet article édicte certaines obligations particulières du prestataire de services de certification. Celui-ci doit :

   i) présenter des garanties d'impartialité : le libellé de cet article laisse entendre que ce prestataire peut être lié à la personne qu'il identifie, mais dans cette éventualité il doit offrir des garanties qui font en sorte qu'il démontre une grande objectivité dans l'application de ses critères habituels, qu'il ne peut y avoir de doute quant au sérieux de la délivrance du certificat concerné. Ce pourrait être le cas par exemple d'une société qui émet un certificat d'identité pour l'un de ses actionnaires.
   ii) assurer l'intégrité (référence à l'article 6?) du certificat délivré au cours de son cycle de vie. On mentionne ici certaines étapes du cycle de vie d'un certificat, soit : sa modification, sa suspension, son annulation, son archivage et sa mise à jour.

   iii) être en mesure de confirmer :
      a- le lien entre le dispositif d'identification, tangible ou logique et la personne, l'association, la société, l'État ou l'objet identifié. Un exemple de dispositif

logique serait la clé publique d'une personne dans le système de cryptographie asymétrique

b- le lien entre le dispositif de localisation, tangible ou logique, et la personne, l'association, la société, l'État ou l'objet localisé. Un exemple de dispositif tangible, c'est-à-dire matériel, serait un appareil quelconque lié à une personne dans le but de savoir où elle se trouve, en tout temps et en tout lieu, si une loi le prévoit expressément, dans les cas prévus au 2° paragraphe de l'article 43 de la loi (pour protéger la santé des personnes ou si la sécurité publique le requiert).

2- Certaines obligations applicables entre autres aux prestataires de services de certification et de répertoire et stipulées ailleurs dans la loi

i) concernant la conservation des documents : ces obligations se retrouvent aux articles 19 à 22 de la loi. À souligner : le paragraphe 2° de l'article 20 qui concerne la protection des renseignements confidentiels et personnels que comportent des documents qui peuvent être détruits.

ii) concernant la consultation des documents : ces obligations se retrouvent aux articles 23 à 27 de la loi. À souligner : l'article 24 qui traite de la protection des renseignements personnels contenus dans un document technologique rendu public et l'article 25 qui balise l'accès à un document technologique qui porte un renseignement confidentiel.

iii) concernant la transmission des documents : l'article 30 prévoit que la documentation nécessaire pour fins de preuve établissant la capacité d'un mode de transmission de préserver l'intégrité du document doit être disponible, donc conservée par le prestataire. Cet article énonce que pour que le document technologique reçu soit considéré comme ayant la même valeur que le document technologique transmis, il faut que le mode de transmission choisi permette de préserver l'intégrité des deux documents. Ill faut pouvoir en faire la preuve, le cas échéant. Par ailleurs, l'article 33 énonce une présomption d'intégrité d'un document d'une entreprise au sens du Code civil ou de l'État en faveur d'un tiers qui en génère un exemplaire ou une copie à partir d'un système ou document, y compris un logiciel, mis à sa disposition par l'un d'eux.

iv) concernant l'identification : lorsque le prestataire de services de certification confirme l'identité des personnes, l'article 40 de la loi stipule que cela doit se faire dans le respect de la loi. L'article 41 prévoit qu'un document technologique qui présente, par exemple, une caractéristique personnelle, doit être protégé contre l'interception qui rendrait possible l'usurpation d'identité, et que sa confidentialité doit être protégée. L'article 44 pose certaines exigences quant à l'utilisation de caractéristiques ou mesures biométriques.

v) concernant les identifiants : l'article 46 énonce que lorsqu'un document utilisé pour effectuer une communication en réseau doit être conservé pour fins de preuve (et c'est certainement le cas des certificats), son identifiant (le paragraphe 3° de cet article précise ce qu'est un identifiant) doit être conservé avec lui pendant tout le cycle de vie du document par la personne responsable du document. Le 4° paragraphe de cet article 46 précise que pour établir la provenance ou la destination d'un document à un moment déterminé, les certificats, entre autres objets, qui ont servi à effectuer la communication, doivent pouvoir être identifiés ou localisés au moyen des identifiants

qui leur sont attribués. On peut penser ici aux certificats de clés publiques qui sont joints à des documents lors d'une transaction.

3- La fausse représentation

L'article 56 prévoit que le fait de délivrer un document présenté comme un certificat servant à confirmer (entre autres) l'identité d'une personne :

i) alors qu'aucune vérification n'a été faite; ou que

ii) l'insuffisance de la vérification équivaut à une absence de vérification constitue une fausse représentation.

L'article 57 prévoit certaines obligations de la personne qui est titulaire d'un dispositif, tangible ou logique, qui permet de l'identifier, de la localiser ou d'indiquer un de ses attributs. Un dispositif peut être tangible ou logique, i.e. que cela peut être un objet physique ou des données stockées dans une carte à puce ou encore des données biométriques qu'un appareil reconnaît sur présentation de la forme de la main.

Lorsqu'un titulaire détient un dispositif :

1- tangible ou logique;

2- permettant de :
   i) l'identifier
   ii) le localiser ou
   iii) indiquer un de ses attributs et

3- comportant un élément secret (par exemple la clé privée d'une biclé), il doit en assurer la confidentialité.

Le titulaire a donc la responsabilité de prendre les mesures adéquates afin que sa clé privée, par exemple, qui lui est attribuée, ne soit pas accessible à d'autres. En effet, un individu ne pourrait se plaindre des conséquences d'une usurpation d'identité s'il laisse d'autres personnes, par exemple, utiliser sa clé de signature. Le 2° paragraphe de cet article crée même un présomption d'utilisation par le titulaire. Il devra donc en cas d'usurpation prouver que c'est quelqu'un d'autre qui a utilisé sa clé privée, le cas échéant, ce qui peut s'avérer assez difficile.

Ce 2° paragraphe prévoit, *a contrario*, que le dispositif peut être utilisé par une autre personne avec l'autorisation du titulaire : par exemple lorsqu'une société signe par l'intermédiaire de l'un de ses dirigeants, elle doit prendre les moyens pour s'assurer que c'est bien ce dirigeant qui signera en son nom, puisque toute utilisation est présumée faite par cette société.

Le prestataire de services de certification a aussi sa part de responsabilité, car lors de l'envoi au titulaire de l'élément secret du dispositif, il doit prendre les moyens qui s'imposent pour que ce soit seulement le titulaire visé qui en prenne connaissance et le reçoive.

10.9 Les obligations du titulaire du certificat

> ***58.*** *Le titulaire qui a des motifs raisonnables de croire que le dispositif a été volé ou perdu ou que sa confidentialité est compromise doit aviser, dans les meilleurs délais :*
>
> *1° la personne qu'il a autorisée à utiliser le dispositif;*
>
> *2° le tiers dont il peut raisonnablement croire qu'il agit en se fondant sur le fait que le dispositif a été utilisé par la personne qui en a le droit;*
>
> *3° le prestataire de services de certification pour que celui-ci puisse suspendre ou annuler le certificat lié au dispositif.*
>
> *Il en est de même pour la personne autorisée qui doit aviser le titulaire et les personnes visées aux paragraphes 2° et 3°.*
>
> *Il est interdit d'utiliser un dispositif, tangible ou logique, pour signer un document sachant que le certificat auquel le dispositif est lié est suspendu ou annulé.*

Cet article traite aussi, en addition à l'article 57, de certaines des obligations du titulaire d'un dispositif, dans le cas où celui-ci a été volé ou perdu ou lorsque des données confidentielles ont été compromises.

Il faut noter que l'expression « qui a des motifs raisonnables de croire » est assez exigeante : en effet, le titulaire du dispositif concerné doit aviser les personnes visées par cet article même s'il n'est pas certain que celui-ci a été volé ou perdu. Il doit le faire aussitôt qu'il a un soupçon sérieux à cet égard.

Un exemple de telle situation serait un notaire qui possède une clé de signature qui lui a été attribuée par la Chambre des notaires (agissant comme autorité de certification) et qui est conservée sur une disquette qu'il ne peut soudainement retrouver. La clé privée emmagasinée sur cette disquette pourrait être utilisée sans droit par un employé de ce notaire. C'est pourquoi il se devra d'aviser sans délai la Chambre des notaires et tout autre personne dont il « peut raisonnablement croire » qu'elle agit en pensant que c'est bien lui qui aurait utilisé sa signature électronique. La Chambre des notaires suspendra ou annulera (selon les circonstances) le certificat de clé publique lié à cette clé privée.

Un autre exemple serait une personne morale qui a autorisé un dirigeant à signer en son nom et à utiliser sa clé privée : s'il perd la clé privée qui lui a été attribuée, par exemple, ce dirigeant devra aussi aviser sans délai le titulaire de cette clé, la personne morale, afin que celle-ci à son tour avise les personnes visées à cet article.

Le dernier paragraphe de cet article contient une prohibition qui entre dans la logique de la loi : personne ne peut utiliser, par exemple, une clé privée de signature tout en sachant que le certificat de clé publique correspondant a été suspendu ou annulé.

> ***59.*** *Celui qui fournit des renseignements afin d'obtenir pour lui-même la délivrance d'un certificat est tenu d'informer le prestataire de services de certification, dans les meilleurs délais, de toute modification de ces renseignements.*

> *Lorsque les renseignements sont fournis dans le cadre d'un mandat ou d'un contrat de service ou d'entreprise, celui pour qui le certificat a été délivré est tenu, subséquemment, de la même obligation d'information envers le prestataire de services de certification.*

Cet article prévoit une obligation de mise à jour des renseignements fournis en vue de l'obtention d'un certificat. Cette obligation est imposée :

1- à celui qui obtient pour lui-même un certificat; et

2- à celui pour qui le certificat a été délivré dans le cadre d'un mandat ou d'un contrat de service ou d'entreprise.

Prenons comme exemple le cas d'un certificat d'attribut (prévu au 2° paragraphe de l'article 47), lequel peut entre autres servir à établir la fonction d'une personne au sein d'une personne morale : si la personne concernée cesse de détenir cette fonction, alors la personne en autorité chez cette personne morale devra en aviser dans les meilleurs délais le prestataire de services de certification qui a émis le certificat d'attribut, afin qu'il fasse la modification nécessaire pour que les tiers sachent avec quel représentant de cette personne morale ils peuvent transiger.

10.10 Les obligations de celui qui agit sur la foi du certificat

> ***60.*** *Dans le cadre d'une communication au moyen d'un document technologique, la validité et la portée du certificat doivent préalablement être vérifiées, par la personne qui veut agir en se fondant sur le certificat, afin d'obtenir confirmation de l'identité ou de l'identification de toute partie à la communication ou de l'exactitude d'un identifiant d'un objet.*
>
> *De même, avant de se fonder sur un renseignement inscrit au certificat, il lui faut vérifier si le prestataire de services de certification confirme l'exactitude du renseignement.*
>
> *La vérification peut être faite au répertoire ou à l'emplacement qui y est indiqué ou auprès du prestataire, au moyen d'un dispositif de consultation sur place ou à distance.*

Cet article édicte des obligations envers l'utilisateur du certificat. En effet, celui-ci doit effectuer des vérifications minimales avant de se fonder sur un certificat lors d'une communication au moyen d'un document technologique. Il risque de voir sa responsabilité engagée suivant les dispositions de l'article 61 de la loi s'il ne remplit pas ses obligations, lesquelles sont par ailleurs des obligations de moyens, selon le premier paragraphe de cet article 61.

Les vérifications à faire

1- La validité du certificat : il s'agit ici de vérifier si le certificat est en force. Par exemple, il faut vérifier la date d'échéance : le paragraphe 4° de l'article 48 prévoit que le certificat doit comprendre cette information.

2- **La portée du certificat** : il faut vérifier, par exemple dans le cas d'une transaction, la limite du montant des transactions permises en se basant sur le certificat. L'énoncé de politique du prestataire devrait contenir cette information, suivant le paragraphe 4° de l'article 52.

3- **L'exactitude du renseignement sur lequel on veut se fonder et qui est inscrit sur le certificat doit être confirmée par le prestataire de services de certification** : lors de la consultation du certificat, il faut que le prestataire confirme à ce moment même si ce qui est inscrit sur le certificat est toujours valide et en vigueur. Dans l'énoncé de politique du prestataire, la fréquence de la mise à jour devrait être indiquée, suivant le paragraphe 2° de l'article 52.

L'endroit où la vérification peut être effectuée

Le 3° paragraphe de cet article prévoit que la vérification peut être faite :

1- au répertoire;

2- à l'emplacement qui est indiqué au répertoire, ou

3- auprès du prestataire.

Comment la vérification peut être faite

Au moyen d'un dispositif de consultation sur place ou à distance.

10.11 La responsabilité des parties impliquées dans un certificat

L'article 61 précise et répartit les obligations et les responsabilités respectives de ceux qui sont impliqués dans la mise en circulation et l'utilisation d'un certificat. Il s'agit du prestataire de services de certification et de répertoire, du titulaire visé par le certificat et de la personne qui agit en se fondant sur le certificat

Ils sont chacun tenus à une obligation de moyens en ce qui a trait aux devoirs qui leur incombent aux termes des autres dispositions cette loi. L'article 61 est d'ordre public et ne peut être écarté par contrat. Il se lit ainsi :

> ***61.*** *Le prestataire de services de certification et de répertoire, le titulaire visé par le certificat et la personne qui agit en se fondant sur le certificat sont, à l'égard des obligations qui leur incombent en vertu de la présente loi, tenus à une obligation de moyens.*
>
> *À moins de démontrer qu'elle n'a pas commis de faute dans l'exécution de ses obligations, chacune de ces personnes est responsable de réparer le préjudice résultant de l'inexactitude ou de l'invalidité du certificat ou d'un renseignement contenu au répertoire. Lorsque plus d'une d'entre elles est responsable, l'obligation de réparer est conjointe; si leur part de responsabilité ne peut être établie, elle est répartie à parts égales. De plus, en l'absence de faute de la part de toutes ces personnes, elles assument la réparation du préjudice conjointement et à parts égales.*
>
> *Aucune de ces personnes ne peut exclure la responsabilité qui lui incombe en vertu du présent article.*

L'obligation de moyens

La disposition prévoit que chacune de ses personnes a une obligation de moyens. En conséquence, elles doivent prendre les moyens raisonnables pour satisfaire aux obligations que leur impose la présente loi.

La responsabilité

Lorsque l'une ou l'autre des personnes concernées démontre qu'elle n'a pas commis de faute dans l'exécution de ses obligations, elle n'est pas responsable.

Mais lorsqu'il y a faute d'une ou plusieurs des personnes impliquées dans un certificat :

Chacune des personnes mentionnées est responsable de réparer le préjudice résultant de l'inexactitude ou de l'invalidité du certificat ou d'un renseignement contenu au répertoire.

Lorsque plus d'une personne est responsable, la responsabilité est conjointe.

Lorsque l'obligation est conjointe, les débiteurs ne sont obligés que d'acquitter leur part respective de l'obligation (art. 1518 CCQ). La loi établit, à l'égard de la responsabilité découlant de l'utilisation des certificats, le principe de la responsabilité conjointe. Par conséquent, à l'égard de la responsabilité visée ici, l'on écarte le principe de l'article 1480 du Code civil selon lequel la responsabilité solidaire s'applique en matière de responsabilité civile.

Si aucune faute ne peut être reprochée à l'une ou l'autres des personnes impliquées, la responsabilité pour la réparation du préjudice est alors assumée à parts égales.

L'obligation de réparer

L'obligation de réparer incombe donc à ceux qui n'ont pas agi de manière prudente et diligente. Si personne n'a commis de faute, alors la responsabilité est partagée entre tous les intervenants et elle est alors fondée sur le risque inhérent à l'activité de certification.

La caractère d'ordre public

Le dernier alinéa de l'article écarte la possibilité pour une personne d'exclure sa responsabilité lui incombant selon cette disposition de la loi.

En résumé,

1° si aucune de ces personnes ne réussit à démontrer qu'elle a pris des moyens raisonnables pour se décharger de son obligation, elles sont toutes responsables de la réparation du préjudice causé par l'inexactitude du renseignement inscrit au certificat;

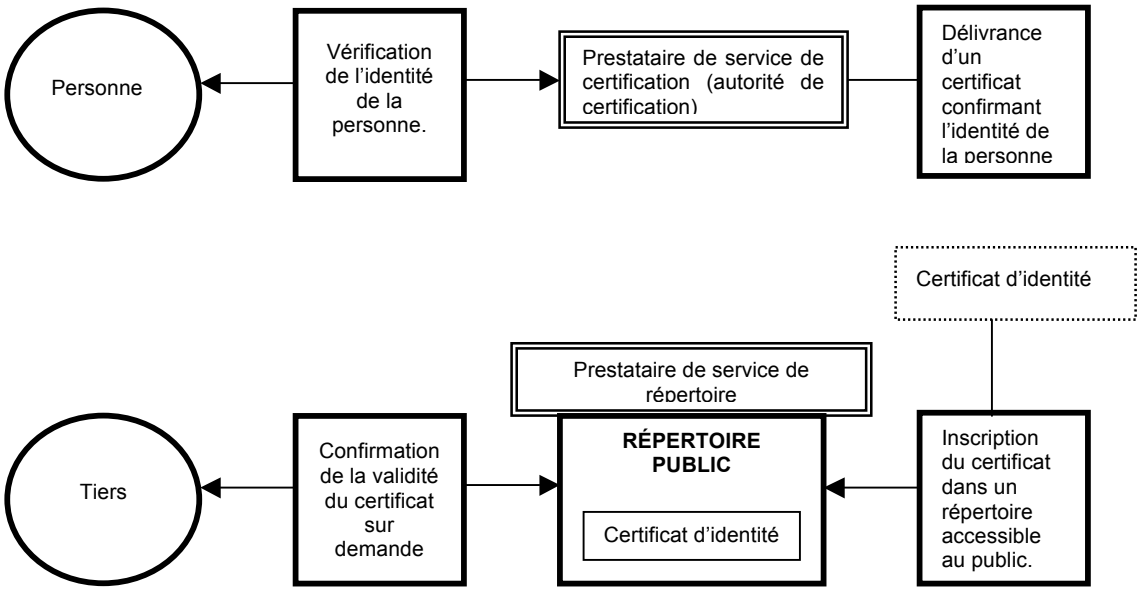
2° si deux ou plusieurs personnes sont responsables, la responsabilité est conjointe;

3° si deux ou plusieurs personnes sont responsables et que leur responsabilité ne peut être départagée, leur quote-part de responsabilité est partagée à parts égales;

4° si toutes ces personnes réussissent à démontrer qu'elles ont pris des moyens raisonnables pour remplir leurs obligations et que malgré tout un préjudice a été causé, par exemple à la personne qui a investi des fonds en se fondant sur le certificat, le risque est partagé conjointement et à parts égales.

Aucune de ces personnes ne peut écarter la responsabilité qui lui incombe à cet article. Ainsi, un contrat qui stipulerait des règles de responsabilités différentes de celles prévues ici serait sans effet.

Prestataire de service de certification et de service de répertoire



11. La gestion des risques juridiques dans les environnements en ligne

Tobias Mahler définit ainsi le risque juridique envisagé au niveau des sujets de droit: « A risk is a legal risk if its source involves a legal norm. Thus the risk needs to be the manifestation of a legal norm's potential detriment. Both factual and legal uncertainty may influence legal risk » (p. 21). Mahler[302] définit la gestion du risque juridique comme étant une méthodologie consistant en un ensemble d'activités de gestion de certains types de risques, à savoir les risques découlant de la loi et les risques qui peuvent être traités (gérés) par des moyens juridiques.

La gestion du risque juridique est ainsi comprise comme visant deux types de risques que les professionnels du droit peuvent aider à identifier et à baliser à savoir les risques découlant de la loi et ceux qui peuvent être balisés en faisant appel à des solutions juridiques[303].

Le risque juridique découle en effet des situations où la violation des droits d'autrui est susceptible de se produire. Même s'ils sont différents, il y a une étroite proximité entre le risque technologique et le risque juridique : lorsque le risque technologique est avéré, il naît presque toujours une obligation d'en tenir compte et de se comporter de façon conséquente. Le risque juridique peut aussi découler de la possible non-conformité à une loi ou à une autre sorte d'obligation également applicable comme un contrat. Le risque juridique, en toute hypothèse, résulte des situations dans lesquelles la responsabilité d'une personne peut être mise en cause. C'est dire l'importance d'évaluer les enjeux et risques juridiques lors de la conception, de la planification et de la mise en place de projets de prestations en ligne de services gouvernementaux.

11.1 L'application du droit : de la « résolution de problèmes » à la « gestion des risques juridiques »

La nature même de l'application du droit paraît connaître des changements. Alors que l'on postulait que l'application du droit consiste à appliquer la règle appropriée afin de résoudre un problème, on tend de plus en plus vers une démarche d'identification et de gestion des « risques » qui peuvent découler directement ou indirectement des règles de droit.

Richard Susskind explique que le principal aspect du travail des juristes, le « legal problem solving » va perdre de son importance. L'emphase va être mis davantage sur le *legal risk management* ¨. Une telle tendance accentue l'importance des méthodes afin de gérer les risques juridiques. Susskind explique que :

---

302 Tobias MAHLER, « Defining Legal Risk », in Proceedings of the Conference 'Commercial Contracting for Strategic Advantage- Potentials and Prospects', Turku, University of Applied Sciences, 2007, < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1014364 >.

303 C. COLLARD, "*Le risque juridique existe-t-il ? Contribution à la définition du risque juridique* ", JCP, Cah. dr. ent. 2008, n° 1 (numéro spécial sur le risque juridique), pp. 8-13.

"In conventional, reactive legal service, when a legal risk has been perceived and a lawyer instructed, there is an expectation that some optimum disposal of the matter will be achieved. In contrast, legal risk management techniques are often brought to bear in respect of legal risks that would otherwise not be managed at all or would be addressed too late. And in this context, in the latent legal market, it may be entirely tolerable (commercially and as a matter of practicality) that any solution reached may be well short of the optimum position. The point is that the legal risk is being managed. Without such techniques, such risks would not have been managed at all or may not have been manageable. Thus there can be improvement if not perfection"[304].

Le phénomène paraît particulièrement présent dans les environnements qui ne semblent pas posséder de limites facilement identifiables comme les réseaux interconnectés dans lesquels se déroulent des activités. Dans ces contextes, les moindres activités sont théoriquement visées par une multitude de règles de droit de même que par d'autres normativités. Alors, la démarche encyclopédique consistant à identifier toutes et chacune des règls (théoriquement, les lois de tous les pays) et à déterminer laquelle ou lesquelles trouve application peut être supplantée par une analyse des risques que s'appliquent certaines règles ou les risques que ces dernières emportent des conséquences adverses.

Le risque juridique vient rendre compte de la relative incertitude qui peut exister quant aux conditions d'application d'une norme et quant au sens de celle-ci. C'est pourquoi l'on retient que le risque juridique est engendré par l'incertitude. L'incertitude quant au cadre juridique et à son application apparaît souvent comme l'un des risques majeurs à considérer lors du déploiement de services dans des environnements inédits comme les réseaux informatiques.

Par exemple, à l'égard de l'analyse des enjeux et risques d'un portail d'un organisme public, l'analyse des risques doit normalement succéder —et non précéder— à une analyse des obligations imposées par la loi. C'est dans la Loi que l'on trouve les obligations fondamentales à partir desquelles se situe nécessairement une analyse de risques. Une telle démarche suppose d'identifier non seulement les exigences des lois qui s'appliquent spécifiquement aux situation visées mais également les obligations plus floues résultant des devoirs de prudence et de diligence qui sont considérés lorsqu'est mise en cause la responsabilité d'un ministère ou d'un organisme public.

L'analyse de risques consiste habituellement à identifier, à partir des gisements, des flux et de l'utilisation envisagée des informations, ce qui présente des risques pour la protection de la vie privée. Elle vise aussi à déterminer l'étendue des précautions à prendre aux fins de maîtriser les risques. Une telle démarche permet de tenir compte des situations présentant des risques devant être pris en charge et de fournir, le cas échéant, une indication des niveaux de risques à

---

304 Richard SUSSKIND, *The Future of Law: Facing the Challenges of Information Technology*, Oxford University Press, 1998, p. 27.

considérer[305]. Bien qu'il soit généralement impossible de quantifier de façon chiffrée, les risques d'atteintes à la vie privée, il est possible d'indiquer que telle ou telle situation comporte un risque faible, moyen ou élevé et d'identifier les mesures prises ou à envisager pour y faire face.

11.2 Les environnements en ligne modifient l'échelle des risques

Dans les environnements en ligne, les repères spatiaux et temporels sont modifiés. Les balises conçues dans un monde dans lequel les réseaux prenaient moins de place sont prises en défaut. Des enjeux inédits dans le monde physique se manifestent avec une grande acuité dans l'espace en réseaux[306]. Le *Rapport sur l'application transfrontière de la législation relative à la vie privée* de l'OCDE relève que la circulation accrue de l'information notamment sur Internet accroît les risques pour la vie privée. On ajoute que :

> *La multiplication des flux transfrontières de données, à des débits plus élevés, couvrant des zones géographiques plus étendues, et englobant des données alphanumériques, de la voix et des images entre une multiplicité croissante d'acteurs est susceptible d'augmenter le nombre et le coût des violations de la vie privée subies par les individus et les organisations.*[307]

Les risques pour la dignité humaine se présentent à des échelles différentes. Il y a reconstruction des cercles de la vie privée. Il y a décentrage et recentrage des cercles de la vie privée.

On observe un décentrage spatial : l'espace physique semble se dissoudre dans le cyberespace : le lieu dans lequel est située l'information a désormais peu d'impact sur son accessibilité. Dès lors qu'un document est disponible sur un serveur, les outils de recherche couramment utilisés sur Internet ou certains outils spécialisés sont en mesure de le retrouver. L'éloignement dans l'espace de même que le passage du temps semblent avoir beaucoup moins de prise sur la disponibilité effective de l'information.

Par exemple, Internet banalise la diffusion : l'information peut aisément se trouver à être diffusée en dehors des cercles de circulation légitime ; d'où l'accroissement des risques. Certes, le cyberespace est constitué de lieux publics et de lieux privés. Mais les repères permettant de délimiter le privé du public sont brouillés. Belgum rappelle que :

---

[305] Pierre TRUDEL et France ABRAN, *Guide pour un usage responsable d'Internet à l'intention des responsables des lieux d'accès publics à Internet et des utilisateurs,* réalisé pour le Ministère de l'éducation et la Direction de l'Autoroute de l'Information du Conseil du trésor, Montréal, avril 2003, en ligne à < http://www.droitsurinternet.ca/versions.html >.

[306] Frederick SCHAUER, « Internet Privacy and the Public-Private Distinction », [1998] 38 *Jurimetrics* 555 ;

[307] OCDE, *Rapport sur l'application transfrontière de la législation relative à la vie privée,* Paris, OCDE, 2006, p. 8, < http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119666_1_1_1,00.html >.

Personal data, such as address, phone number, income, poperty value, and marital status have always been avalable to those willing to dig. The Internet can make it possible for a much wider class of persons – essentially all internet users – to gain access to similar types of personal information at little or no cost.[308]

Internet modifie l'échelle spatiale à partir de laquelle s'apprécient les risques pour la vie privée. En dehors du monde en réseaux, l'accessibilité à une information demande des ressources qui peuvent être importantes. Sur Internet, on a l'impression que beaucoup d'informations sont à portée d'une requête de moteur de recherche. Solove observe que :

Until recently, public records were difficult to access. For a long time, public records were only available locally. Finding information about a person often involved a treasure hunt around the country to a series of local offices to dig up records. But with Internet revolution, public records can be easily obtained and searched from anywhere.[309]

La problématique de l'accès aux documents rendant compte du déroulement des processus judiciaires est emblématique des changements quantitatifs et qualitatifs générés par Internet. Natale M. Gome-Velez relève que :

> *Providing Internet access to court records increases exponentially the availibility of court records, including any sensitive information they contain. Examples of sensitive informaion that might be found in court records include : social security numbers, home addresses, names of minor children finncial account numbers, and medical information.*[310]

Il y a aussi décentrage temporel : la persistance de l'information emporte que celle-ci traverse les cercles dans lesquelles elle était tenue pour légitime. Par exemple, une information peut être légitimement disponible au public en raison de l'actualité de l'événement. L'archivage et la disponibilité virtuellement permanente sur Internet irait au-delà de ce qui est nécessaire afin de rendre compte de l'actualité.

Les capacités d'agglomération d'information permettent la constitution de gisements d'informations sur les personnes qui peuvent du coup devenir disponibles pour des forces de police de même que devenir des enjeux pour des malfaiteurs. En somme la disparition des efforts à consacrer pour trouver l'information emporte la disparition d'une protection par défaut pour la vie privée. Cela porte à revoir les raisonnements qui permettaient de déterminer si on se trouvait dans le domaine de la vie privée ou dans le domaine de l'espace public.

---

308 Karl D. BELGUM, « Who leads at Half-time ?: Three Conflicting Visions of Internet Privacy Policy [1999] 6 *Rich. J.L. & Tech.* 1.

309 Daniel J. SOLOVE, « Access and Aggregation : Public Records, Privacy and the Consituttion, » [2002] 86 *Minn. L. Rev.,* 1137-1218, p. 1139.

310 Natalie M. GOMEZ-VELEZ, « Internet Access to Court Reports- Balancing Pblic Access and Privacy, » [2005] 51 *Loyola L.Rev.*, 365-438, p. 371.

Tous ces changements dans les dimensions des enjeux relatifs à la vie privée indiquent des modifications dans les niveaux de risques causés par la circulation de l'information dans le réseau. Ces dimensionnements nouveaux des risques pour la vie privée induisent des mutations au niveau de la raison d'être des règles de droit. Là où l'on prenait pour acquis que le niveau de risques pour la vie privée demeurait faible ou aisément maîtrisé, les mutations dans l 'échelle qualitative et temporelle qu'induit la généralisation d'Internet, conduit à postuler que les risques sont accrus. D'où les revendications pour un renforcement de la protection de la vie privée des personnes lors de la mise en place des environnements de traitement de l'information.

11.3 La gestion des risques dans le e-gouvernement

L'encadrement normatif des environnements en ligne peut s'envisager dans le contexte des risques que la technologie paraît induire. À l'égard de la vie privée, la régulation d'Internet se présente comme un ensemble de décisions de gestion des risques qui sont perçus par les acteurs au sein du réseau.

Le risque en tant que construction sociale sera apprécié de façon différente selon les époques et selon le contexte culturel, politique ou social[311]. Les représentations des dangers et des bienfaits des technologies contribuent à la construction des perceptions collectives des risques et des bénéfices des objets techniques. Ces perceptions varient dans le temps : elles ne sont pas identiques à toutes les époques. Elles diffèrent également selon les contextes sociaux : le droit et les autres normativités procèdent en grande partie de ces perceptions variables reflétant les contextes sociétaux et historiques.

Les acteurs évaluent les risques qu'une mesure ou une règle s'applique à leur activité. La décision de se conformer à telle règle et pas à d'autres procède d'une démarche d'évaluation des risques juridiques. Le potentiel d'application du droit de tel ordre juridique est évalué par chacun des acteurs en fonction de divers facteurs. tels que les possibilités effectives de poursuites, la possession d'actifs sur le territoire étatique concerné, le désir d'inspirer confiance ou de se comporter en « bon citoyen ». Ces facteurs concourent aux analyses par lesquelles les acteurs orientent leurs stratégies de gestion de risques.

11.4 L'analyse des environnements d'information

Il s'agit de caractériser les environnements, les gisements et mouvements d'informations qu'ils supposent de même que leurs processus de gouvernance. Dans une seconde phase les voies et moyens d'expression de la gouvernance des réseaux sont analysés.

Il faut identifier les caractéristiques de ces environnements, quels gisements et mouvements d'information ils supposent ou autorisent, ce qu'ils facilitent, ce qu'ils autorisent et ce qu'ils empêchent de faire.

---

311 Christine NOIVILLE, *Du bon gouvernement des risques*, Paris PUF, les voies du droit, 235 p.

11.4.1 Identifier les gisements et les mouvements d'information

L'on identifie les gisements d'information de même que les mouvements prévus ou envisagés de l'information. Cette identification tient compte du cycle entier de l'information depuis sa confection, le cas échéant, sa collecte, sa gestion, sa circulation, son utilisation, son archivage et sa destruction. Le cycle de l'information peut varier selon les types d'environnements.

La première étape consiste à identifier les traits caractéristiques du fonctionnement, de la configuration et des fonctionnalités des environnements électroniques envisagés. Cette démarche s'effectue à partir de l'analyse systématique du fonctionnement des environnements.

Dans une seconde étape, l'on dresse un bilan des enjeux et risques soulevés par les divers environnements et les types d'informations concernés. Ce bilan est dressé à l'égard de chacune des étapes du cheminement de l'information au sein des environnements de même qu'au moment de l'entrée et de la sortie des données. Cela permet de dresser un bilan qui reflète une analyse des zones de risques et de conflits.

11.4.2 Situer les responsabilités

Les enjeux de gouvernance ne découlent pas que de l'environnement informationnel mis en place. La responsabilité des acteurs est un relais de normativité important et un mécanisme majeur des processus de gouvernance. Il faudra situer les responsabilités des divers intervenants et décideurs oeuvrant dans le secteur judiciaire et para-judiciaire. Si les questions de responsabilité doivent s'appréhender dès la conception d'un réseau, elles ne doivent pas faire oublier que les acteurs participant à ce réseau ont des rôles, des besoins et des priorités spécifiques engendrant différents niveaux et types de responsabilité. Par conséquent, il faudra établir quel type de responsabilité correspond à chacun des acteurs, et ce pour les différents gisements et mouvements d'information. Par la suite, il faut déterminer quels outils de droit formel et informel, législatifs et contractuels, encadrent ces responsabilités au regard de la gouvernance de l'environnement-réseau concerné, par exemple : lois et règlements, code de conduite, code d'éthique, de déontologie professionnelle, etc.

Pour réaliser cette typologie des responsabilités et des outils normatifs afférents, il faut déterminer 1er) qui est le producteur de l'instrument normatif, 2e) quelles sont les personnes et les matières concernées et, 3e) quelles sont les sanctions en cas de non-respect des obligations découlant de ces outils normatifs. Cette grille d'analyse permettra de déterminer si les outils actuels de gouvernance doivent ou non faire l'objet d'adaptations.

11.4.3 Identifier les risques et les enjeux généraux par application

À partir des pratiques et applications (ex : dossier électronique), il faut identifier les risques et les enjeux qui ont des conséquences au plan de la gouvernance. Par exemple : interopérabilité / arrimage des systèmes / disponibilité des systèmes, transparence, responsabilité, rémunération, confidentialité / partage de l'information, sécurité, protection de la vie privée lors des étapes du cycle de vie des renseignements personnels, juridiction.

11.5 Identifier les stratégies de régulation des environnements en ligne

La gouvernance dans les réseaux se crée par des individus à travers des entités sociales et juridiques et selon des processus relationnels complexes découlant de la nature de l'espace où ils se tiennent. La normativité y est en continuelle mutation; elle résulte d'un dialogue continu entre les différents acteurs agissant dans le réseau. Il importe donc de cerner les modes de fonctionnement des réseaux dans l'ensemble des dimensions ayant des impacts sur les normes effectivement appliquées. Dans les réseaux de e-gouvernement, le paradigme de la gouvernance permet de rendre compte d'un environnement normatif diversifié et moins formel que celui tracé par le droit étatique et formaliste. Dans une logique de gouvernance caractéristique des réseaux, la décision résulte habituellement d'une négociation permanente entre les acteurs, constitués en partenariat au sein de l'entreprise, de l'État, d'une organisation, ou même d'un problème à résoudre.

Plusieurs chercheurs constatent que la gouvernance en réseau apparaît comme une solution originale et novatrice pour assurer une administration efficace et respectueuse des valeurs fondamentales. Elle assure la concertation et la décision par consensus, une meilleure diffusion de l'exercice du pouvoir et une meilleure prise en compte des avis et opinions de la pluralité d'intervenants. Dans les réseaux, les processus de gouvernance concernent forcément l'évaluation continue des enjeux et des risques de même que les façons de prendre en charge et de gérer les risques et enjeux.

11.5.1 Les outils d'évaluation des risques et des enjeux

Au nombre des délibérations se déroulant en réseau, il y a celles concernant les interactions relatives aux enjeux et risques à gérer dans le fonctionnement du réseau. La virtualisation emporte des changements de rationalités et le défi de la gouvernance des réseaux est de procurer des méthodologies et approches optimales afin de débattre de ces enjeux et risques et formuler des modes de fonctionnement des services offrant des solutions adéquates.

Le développement des services en ligne a donc amené les entités publiques à mettre en place divers outils afin de mieux identifier les approches et les outils les plus indiquées afin d'assurer, dans les réseaux, l'identification et la maîtrise adéquate des risques et enjeux.

Ainsi, au Québec, le *Règlement sur la diffusion et sur la protection des renseignements personnels*[312] précise les obligations incombant aux dirigeants des organismes assujettis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[313]. Il prescrit la mise en place d'un un comité sur l'accès à l'information et la protection des renseignements personnels relevant du dirigeant de l'organisme. Ce comité se compose du responsable de l'accès aux documents et de la protection des renseignements personnels et, le cas échéant, du responsable de la sécurité de l'information et du responsable de

---

312 R.Q. c. A-2.1, r.0.2.

313 L.R.Q., c. A-2.1.

la gestion documentaire ; il est chargé de soutenir le sous-ministre ou le dirigeant de l'organisme public dans l'exercice de ses responsabilités et obligations et, à cette fin, il peut s'adjoindre toute autre personne dont l'expertise est requise pour exercer sa fonction ;

Le Règlement s'applique aux organismes publics visés à l'article 3 de la *Loi sur l'accès,* c'est-à-dire le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères, les organismes gouvernementaux, les organismes municipaux, les organismes scolaires et les établissements de santé ou de services sociaux. Le règlement ne vise pas le Lieutenant-gouverneur, l'Assemblée nationale, d'une personne ni les organismes publics visés aux articles 5 à 7 de cette Loi. Il ne s'applique pas non plus à un ordre professionnel.

L'article 7 du Règlement prévoit qu'un organisme public doit informer le comité des projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels. Le comité suggère, parmi ces projets, ceux qui doivent être encadrés par des mesures particulières de protection des renseignements personnels. Ces mesures comprennent :

> *1° la nomination d'une personne chargée de la mise en oeuvre des mesures de protection des renseignements personnels pour chaque projet ;*
>
> *2° l'évaluation, dès l'étude préliminaire du projet, des risques d'atteinte à la protection des renseignements personnels ;*
>
> *3° des mesures propres à assurer la protection des renseignements personnels pendant toute la période de réalisation du projet et son maintien lors de l'utilisation, de l'entretien, de la modification et de l'évolution du système d'information ou de prestation électronique des services visés ;*
>
> *4° la description des exigences de protection des renseignements personnels dans le cahier de charges ou le contrat relatif au projet, à moins que l'exécutant du contrat soit un autre organisme public ;*
>
> *5° la description des responsabilités des participants au projet en matière de protection des renseignements personnels ;*
>
> *6° la tenue d'activités de formation sur la protection des renseignements personnels à l'intention des participants au projet*.

Aux termes des articles 8 et 9, le Comité doit également être consulté lorsqu'un organisme entend mener un sondage impliquant des renseignements personnels ou mettre en place des mécanismes de vidéosurveillance.

Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* paraît emblématique des tendances de l'État en réseau en ce qu'il prescrit des mesures ayant pour but d'anticiper et de maîtriser les risques pouvant découler de la mise en place de systèmes d'information.

11.5.2 La prise en charge des risques et des enjeux en fonction des responsabilités incombant aux acteurs

Une fois les risques et enjeux identifiés, il faut identifier méthodiquement les processus, outils et autres moyens d'expression de la gouvernance. Ces moyens doivent refléter la diversité et la complexité des réseaux et procurer des outils conceptuels afin de mettre en place des processus effectifs de gouvernance. De tels processus doivent être conséquents avec les risques et enjeux qui sont spécifiques à chacun des environnements.

Dans le secteur public, l'analyse des enjeux relatifs à la mise en place de prestations électroniques de services peut présenter des différences avec celle qui peut être menée dans le secteur privé[314]. Une entreprise œuvrant dans le secteur privé pourra évaluer les risques associés à la mise en place de services Internet en termes de pertes financières. Cette évaluation est nécessaire : une entreprise peut être poursuivie devant les tribunaux et tenue responsable pour la façon incorrecte dont ses services sont offerts. Un organisme public doit se soucier aussi bien des conséquences financières que des conséquences non financières de son activité. L'évaluation des risques reliés aux services offerts en ligne ne peut procéder uniquement d'une analyse des dimensions financières de l'activité concernée ou du service.

Dans son analyse des risques, l'organisme public doit tenir compte des enjeux associés à son champ d'activité, de la sensibilité des informations ou des services qui sont en cause et des attentes des clientèles spécifiques.

Ces facteurs incitent généralement plusieurs entités de service public à adopter des standards qui tiennent compte des attentes du public, et pas seulement des risques spécifiques associés aux transactions.

Dans le contexte d'un organisme public, l'analyse des risques doit normalement succéder —et non précéder— à une analyse des obligations imposées par la loi. C'est dans la Loi que l'on trouve les obligations fondamentales à partir desquelles se situe nécessairement une analyse de risques. Une telle démarche suppose d'identifier non seulement les exigences des lois qui s'appliquent spécifiquement aux situation visées mais également les obligations plus floues résultant des devoirs de prudence et de diligence qui sont considérés lorsque est mise en cause la responsabilité d'un ministère ou d'un organisme public.

L'analyse de risques consiste habituellement à identifier, à partir des gisements, des flux et de l'utilisation envisagée des informations, ce qui présente des risques pour la protection de la vie privée. Elle vise aussi à déterminer l'étendue des précautions à prendre aux fins de maîtriser les risques. Une telle démarche permet de tenir compte des situations présentant des risques devant être pris en charge et de fournir, le cas échéant, une indication des niveaux de risques à considérer. Bien qu'il soit généralement impossible de quantifier de façon chiffrée, les risques

---

314 Voir : Jane Kaufman WINN, « The Hedgehog and the Fox : Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions », [1999] 51 : *Administrative Law Review*, 955, 959-960.

d'atteintes à la vie privée, il est possible d'indiquer que telle ou telle situation comporte un risque faible, moyen ou élevé et d'identifier les mesures prises ou à envisager pour y faire face.

Conclusion

Dans la plupart des pays développés, l'État connaît des mutations : ses moyens d'intervention connaissent des transformations. L'état moderne est remplacé par un État de type post-moderne fonctionnant suivant des paradigmes différents[315]. Au plan du droit, l'émergence des environnements de e-gouvernement est un révélateur de plusieurs tendances lourdes du droit contemporain. La pyramide emblématique de la hiérarchie admininistrative caractéristique de l'admininistration publique de l'État providence fait place de plus en plus à un environnement configuré en réseau au sein duquel le dialogue entre les administrations et entre les administrations et les citoyens tend à prendre plus de place.

Dans un tel univers en réseau, les approches autoritaires de la loi paraissent impraticables. Il faut rechercher les consensus, construire les alliances. Tant au plan interne qu'au plan externe de l'organisation étatique, il importe d'assurer les équilibres fragiles caractéristiques des sociétés complexes.

Les mécanismes par lesquels s'expriment les interventions étatiques se modifient afin de refléter un univers où la régulation est pensée et appliquée suivant une dynamique de réseau. Devant le haut degré de technicité des environnements dans lesquels évolue le e-gouvernement, les lois s'expriment en forme de principes généraux, prescrivent les résultats à atteindre, les seuils de qualité qui doivent être respectés . C'est dans l'univers réglementaire ou même dans celui des normes techniques que sont exprimés les détails précis des techniques à installer. C'est ainsi que le droit canadien a connu des évolutions afin d'habiliter les décideurs à mettre en place les environnements techniques destinés à la fourniture des services en ligne par l'État. Largement tributaires des principes du droit commun et des pratiques développées d'abord dans le domaine du commerce électronique, les principes des lois visent à poser les principes à respecter peu importe les moyens auxquels il est fait recours pour réaliser une transaction.

En plus des ajustements aux cadres du droit commun, des défis majeurs sont encore à relever. Le fait que plusieurs interactions impliquant le gouvernement se déroulent dans des environnements essentiellement constitués par la technique pose le défi de l'ajustement des paradigmes fondateurs du droit administratif en général et en premier lieu, du droit de la protection des données personnelles. Au plan des méthodes de travail, la mise en place et le monitoring juridique des activités et interactions qui se déroulent en ligne nécessite le développement de méthodes différentes que celles que procure l'analyse de la conformité aux règles de droit envisagée de façon réactive ou contentieuse. On tend à convenir de l'importance de développer des modes d'identification et de prise en charge des enjeux et risques juridiques dans les réseaux consacrés à la fourniture des services publics.

---

315 Charles-Albert MORAND, *Le droit néo-moderne des politiques publiques*, Paris, LGDJ, 2000.

C’est pourquoi il faut porter l’attention au développement de méthodes afin d’accroître la connaissance et la compréhension des multiples facteurs qui contribuent à la normativité et à la gouvernance en ligne.