Revue du notariat

LA REVUE DU NOTARIAT

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*

Pierre TRUDEL

Volume 106, Number 3, December 2004

URI: https://id.erudit.org/iderudit/1045704ar
DOI: https://doi.org/10.7202/1045704ar

See table of contents

Publisher(s)

Éditions Yvon Blais

ISSN

0035-2632 (print)
2369-6184 (digital)

Explore this journal

Cite this article

TRUDEL, P. (2004). 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*. *Revue du notariat*, *106*(3), 287–339. https://doi.org/10.7202/1045704ar

THÈME 1

L'encadrement des technologies par le droit : nécessité et sources de changements

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*

Pierre TRUDEL*

* Professeur titulaire de la chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, Faculté de droit, Université de Montréal. Les URLs cités étaient fonctionnels au 10 décembre 2004.

INTRODUCTION

Les technologies de l'information en général et la numérisation en particulier induisent des changements dans le droit. À l'instar des autres mutations dans les techniques, les phénomènes associés aux technologies de l'information appellent à relire, ou à comprendre le droit de façon différente. Cela ne devrait pas surprendre. Il serait en effet étonnant que tout ait vocation à changer dans la société sauf le droit ! Aussi, plutôt que de complaire dans le discours selon lequel le droit serait exempté des changements résultant des évolutions des technologies, le juriste doit se donner les moyens de comprendre les dynamiques associées aux technologies de l'information. C'est à cette condition que le droit sera en mesure d'assurer un encadrement efficace et respectueux des valeurs de respect des personnes, de prévisibilité et de cohérence.

Parce qu'elle permet de considérer l'information dans son unicité, la numérisation accentue les pressions vers un droit centré sur l'information plutôt que sur les techniques utilisées pour son traitement. D'où l'émergence croissante d'un corpus de règles portant sur l'information, ses caractéristiques, les qualités qu'elle doit posséder et ses rapports avec les personnes. Pierre Catala relève les difficultés qu'éprouve le droit à appréhender l'information[1]. Faut-il y voir une conséquence de l'inadéquation des catégories à partir desquelles les juristes cherchent à rendre compte de la norme ? Les tendances au développement d'une société de l'information interpellent le droit et nécessitent un retour critique sur certaines idées-refuges et concepts hérités des époques antérieures[2].

Le droit de l'information numérique a vocation à délimiter les droits et devoirs des usagers de l'information, ainsi que les usages

1. Pierre CATALA, « Ébauche d'une théorie juridique de l'information », dans *Le droit à l'épreuve du numérique jus ex machina*, Paris, P.U.F., 1998, p. 224 à 262.
2. Marie-Anne FRISON-ROCHE, « Les bouleversements du droit par Internet », dans Jean-Marie CHEVALIER, Ivar EKELAND, Marie-Anne FRISON-ROCHE et Michel KALIKA, *Internet et nos fondamentaux*, Paris, P.U.F., 2000, p. 37-76 ; M. Ethan KATSH, *Law in a Digital World*, New York Oxford, Oxford University Press, 1995, 294 p.

possibles de l'information. Dans une telle perspective, il contribue à définir les conditions fondamentales de la production et de l'utilisation voire de la circulation de l'information. Les règles de droit interviennent pour désigner les informations nécessaires aux transactions. Les législations désignent certaines informations comme étant nécessaires à l'accomplissement valide des transactions. Par exemple, dans certains pays, des dispositions fiscales désignent les informations devant apparaître sur les factures. Plusieurs lois exigent que des documents constatant des actes juridiques soient signés. À l'inverse, certaines lois limitent les informations auxquelles on peut avoir recours dans les transactions.

Les règles de droit viennent aussi préciser les qualités des informations échangées lors de transactions. La plupart des législations exigent que les échanges d'informations qui sont inhérents aux transactions s'effectuent selon des standards de qualité, de précision et d'exactitude. C'est ce que visent les règles prescrivant des exigences pour identifier une personne dans les transactions électroniques. Des lois font obligation de fournir certaines informations précontractuelles. Les règles de droit viennent assurer la protection des informations. Une fois la transaction accomplie, il faut éviter que les informations qui l'ont rendu possible soient utilisées à des fins étrangères aux finalités pour lesquelles elles ont été recueillies.

L'intervention du droit trouve plusieurs de ses justifications dans la détermination des niveaux de risques acceptables dans les différentes interactions que requiert la vie sociale. Le droit agit également afin d'assurer, voire renforcer la confiance nécessaire au déroulement des transactions. Il peut intervenir pour délimiter les risques des transactions. Le droit peut aussi intervenir afin de répartir les risques ou encore afin de renforcer ou d'assurer la confiance.

Le droit est un important définisseur des seuils de risques acceptés ou acceptables en matière de transactions. À plusieurs égards, les règles relatives à l'admissibilité en preuve et à la valeur juridique des preuves témoignant des transactions procèdent d'un souci de baliser les risques inhérents aux transactions. Ainsi, des réglementations obligent à vérifier certaines informations afin de s'assurer de l'identité ou des qualités des personnes. Pour certaines transactions, les lois exigent qu'un tiers constate l'identité des cocontractants. Dans de telles situations, le droit a défini des seuils de risques que les parties n'ont pas le loisir de franchir. Le

traitement de certaines informations pouvant servir à l'identification des personnes présente aussi des risques que les systèmes juridiques modernes ont cherché à baliser.

S'agissant du commerce électronique, plusieurs États ont jugé nécessaire de transposer, pour le milieu cyberspatial, les balises visant à délimiter les risques fondées à ce jour sur le paradigme du support-papier[3]. Pour gérer les risques inhérents aux transactions, on peut accroître la quantité ou la qualité des informations à comparer afin de disposer du degré de certitude recherché. Il y a donc un lien entre le niveau de risque qu'on est prêt à supporter et la quantité, voire la qualité d'informations, que l'on requiert afin de compléter un processus transactionnel.

1- Le fonctionnement du droit dans le cyberespace

La définition de normes encadrant les activités d'interaction prenant place dans les environnements virtuels est fortement marquée par les mutations induites par ces environnements à l'égard de ce que l'on se représente comme possible, légitime, ou nécessaire. Par exemple, Internet affecte 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[4]. La vélocité des mutations peut accroître la difficulté d'énoncer des droits et des obligations en termes précis ou formels. D'autres normes interviennent dans la délimitation des droits et des devoirs de ceux qui interagissent dans les environnements électroniques.

Dans le monde physique et dans le cyberespace, la normativité s'élabore de plus en plus dans les réseaux[5]. Les réseaux sont le résultat d'interactions répétées entre personnes poursuivant un but commun. L'« internetisation » s'accompagne de l'émergence de

3. John D. GREGORY, « Canadian Electronic Commerce Legislation », (2002) 17 *Banking & Finance L.R.* 277-339.
4. 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>.
5. Renaud BERTHOU, *L'évolution de la création du droit engendrée par Internet : vers un rôle de guide structurel pour l'ordre juridique européen*, thèse pour le doctorat de l'Université de Rennes 1 mention Droit, juillet 2004 ; Pierre TRUDEL, « La nouvelle territorialité du droit et la recherche juridique », dans *Les nouveaux territoires du droit et leur impact sur la recherche juridique*, colloque Poitiers-Montréal 12-13 décembre 2002, Paris, L.G.D.J., 2004, p. 276-289.

réseaux unissant les décideurs, les chercheurs, les régulateurs de même que les autres acteurs jouant un rôle dans la normativité d'Internet. La tendance à l'accroissement du déroulement dans des réseaux d'actes juridiques de même que des activités génératrices de faits juridiques suppose une appréhension conséquente du droit.

Un ensemble de systèmes de normes s'applique dans le cyberespace : il y est de plus en plus difficile de postuler que seules les normes édictées par le droit de l'État encadrent les interactions qui y prennent place. S'il est clair que le droit des États régit pratiquement un grand nombre d'interactions prenant place dans le cyberespace, on observe de plus en plus l'avènement d'usages et de normes techniques ayant vocation à procurer les encadrements des activités qui ne peuvent être entièrement régies par les systèmes de droits étatiques nationaux[6].

A. Les pôles de normativité

On peut retenir une représentation du cyberespace faisant de celui-ci un ensemble interconnecté constitué de pôles interagissants de normativité. 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.

Le cyberespace 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 espace virtuels. Elles coexistent dans le cyberespace soit en complémentarité avec d'autres règles soit en concurrence, se proposant à la place de celles qui sont issues d'autres pôles normatifs[7].

---

6. Graham GREENLEAF, « An Endnote on Regulating Cyberspace : Architecture vs Law », (1998) 21 *UNSWLJ* 593 ; Michael A GEIST, « The Reality of Bytes : Regulating Economic Activity in the Age of the Internet », (1998) 73 *Washington L.R.* 521-574.
7. Voir, pour un aperçu des approches rendant compte de ce phénomène : Michel COIPEL, « Quelques réflexions sur le droit et ses rapports avec d'autres régulations de la vie sociale », dans J. BERLEUR et al., *Gouvernance de la société de l'information*, Bruxelles, Bruylant, Presses Universitaires de Namur, 2002, p. 43-76.

1. Les systèmes de droit étatiques

Les États continuent de régir les activités se déroulant dans le cyberespace sur une base nationale, mais étant donné que le cyberespace fait abstraction des frontières, les droits nationaux connaissent des limites pratiques d'application. Les limites fixées par le droit étatique s'appliquent sur le territoire national concerné. Le droit d'un État peut trouver application ailleurs dans la mesure où il n'est pas incompatible avec le droit de cet autre territoire.

Dans la plupart des juridictions, les lois mises en place visent à faciliter le commerce électronique. Largement motivées par la volonté de lever les obstacles aux interactions électroniques, perçues ou à tout le moins présentées comme constituant en soi un facteurs de progrès, ces lois s'inscrivent dans une démarche d'habilitation des acteurs. Elles visent à assurer la validité des actes posés dans les environnements électroniques et procurer un cadre juridique prévisible et accueillant aux façons de faire découlant des environnements en réseaux.

À cet égard, il n'est pas surprenant que les États aient cherché, au moyen de concertations internationales à identifier les principes directeurs des législations qui viendraient procurer les ajustements et mises à niveaux des lois nationales.

La norme internationale en vue de faciliter le déroulement du commerce électronique est la *Loi type sur le commerce électronique* adoptée par la Commission des Nations Unies pour le droit commercial international (CNUDCI)[8]. Ce texte a été élaboré sous les auspices de la CNUDCI afin de répondre à une transformation profonde des moyens de communication entre des parties utilisant des techniques informatisées ou d'autres techniques modernes pour conclure des affaires[9]. Elle a pour objet de servir de modèle aux pays pour l'évaluation et la modernisation de certains aspects de leur législation et de leurs pratiques en matière de communications comportant l'emploi d'ordinateurs ou d'autres techniques modernes et pour l'adoption d'une législation pertinente lorsqu'elle fait défaut.

---

8. COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL (CNUDCI), *Loi type sur le commerce électronique et Guide pour son incorporation 2001*, New York, Nations Unies, 2002. <http://www.uncitral.org/french/texts/electcom/ecommerceindex-f.htm>.
9. Éric CAPRIOLLI et Renaud SORIEUL, « Le commerce international électronique : vers l'émergence des règles juridiques transnationales », (1997) *J.D.I.* 323.

Au niveau canadien, la *Loi uniforme sur le commerce électronique*[10] de la Conférence pour l'harmonisation des lois a retenu l'approche de la *Loi type de la CNUDCI sur le commerce électronique*. Dans le sillage de ces initiatives, les législateurs canadiens ont adopté des lois qui intègrent à leur droit, les principes mis de l'avant afin d'assurer la validité des transactions électroniques[11].

2. La normativité découlant de la technique

L'architecture technique constitue une composante du cadre juridique des activités prenant place dans le cyberespace. On entend par l'architecture technique l'ensemble des éléments ou artefacts techniques, tels les matériels, les logiciels, les standards et les configurations qui déterminent l'accès et les droits d'utilisation des ressources du cyberespace. Les objets ont un effet régulateur se présentant suivant diverses formes[12]. Il y a de plus en plus d'interactions entre les normativités découlant de la technique et les autres normes[13].

Les éléments d'architecture peuvent être des logiciels comme les censeurs comme le « V-chip » ou la puce anti-violence, au brouillage des émissions à caractère sexuel destinées aux adultes, à des logiciels comme *Cyber Patrol* et *Net Nanny*. Les éléments d'architecture prennent également la forme de configurations systématiques (default value) ou volontaires des ressources du réseau. Il peut aussi s'agir d'environnements techniques complexes comme les infrastructures à clés publiques (ICP). Les ICP sont conçues de manière à procurer soit des informations relatives à l'identité d'une personne ou encore confirmer un lien entre une personne et un document. Les auteurs Autret, Bellefin et Oble-Laffaire[14]

10. CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, *Loi uniforme sur le commerce électronique*, <http://www.law.ualberta.ca/alri/ulc/current/fueca-a.htm>. (Ci-après désignée par l'expression « Loi uniforme canadienne ».
11. Voir : John D. GREGORY, « Solving Legal Issues in Electronic Commerce », (1999) 32 *Can Business L.J.* 84-131.
12. Pierre TRUDEL, « L'architecture technique comme élément régulateur du cyberespace », (2000) *Media Lex* 187.
13. Margaret Jane RADIN, « Online Standardization and the Integration of Text and Machine », (2002) 70 *Fordham L.R.* 1125-1145.
14. Thierry AUTRET, Laurent BELLEFIN et Marie-Laure OBLE-LAFFAIRE, *Sécuriser ses échanges électroniques avec une PKI, solutions techniques et aspects juridiques*, Paris, Eyrolles, 2002, p. 11.

expliquent que « c'est un ensemble de moyens de gestion des ressources de sécurité qui vont permettre d'établir entre deux partenaires en communication les bases d'une relation de confiance, en particulier en obtenant quelque assurance sur leurs identités réciproques ».

Les outils techniques fonctionnent suivant des principes et des règles établis dans le cadre de processus de normalisation. De tels processus sont menés par des organismes de standardisation constitués de spécialistes des technologies concernées.

Les règles découlant des standards techniques ne sont pas nécessairement le produit de l'activité d'institutions constituées comme telles : elles peuvent résulter de décisions d'acteurs dominants dans certains marchés ou des comportements suivis et espérés des acteurs du cyberespace. Par exemple, l'ensemble des éléments ou artefacts techniques, tels les matériels, les logiciels, les standards et les configurations qui déterminent l'accès et les droits d'utilisation des ressources et des documents technologiques sont formulés dans des forums multiples. Ces lieux dans lesquels s'élaborent les règles réunissent des experts qui conviennent des spécifications que doivent posséder les éléments techniques d'un environnement électronique.

Comme une part significative des décisions relatives à l'architecture du cyberespace relève d'autorités non étatiques, il devient nécessaire d'organiser l'arrimage entre ces forums qui définissent les règles, les instances de l'État et les activités spécifiques se déroulant sur Internet. Ce processus est nécessaire afin d'assurer une cohérence entre la loi étatique et les limites et possibilités reconnues par les experts et les autres acteurs impliqués. C'est dire à quel point des relais sont nécessaires afin d'assurer les arrimages entre les normativités diverses.

Au Québec, un processus de relais entre les normes techniques et les normes juridiques est mis en place par l'article 63 de la *Loi concernant le cadre juridique des technologies de l'information*[15] qui prévoit que :

15. L.Q. 2001, c. 32, en ligne avec annotations à <http://www.autoroute.gouv.qc.ca/loi_en_ligne>.

> **63.** Pour favoriser l'harmonisation, tant au plan national qu'international, des procédés, des systèmes, des normes et des standards techniques mis en place pour la réalisation des objets de la présente loi, un comité multidisciplinaire est constitué. À cette fin, le gouvernement, après consultation du Bureau de normalisation du Québec, fait appel à des personnes provenant du milieu des affaires, de l'industrie des technologies de l'information et de la recherche scientifique et technique, à des personnes provenant des secteurs public, parapublic et municipal ainsi qu'à des personnes provenant des ordres professionnels, toutes ces personnes devant posséder une expertise relative au domaine des technologies de l'information.
>
> Le comité est présidé par un représentant du Bureau de normalisation du Québec. Le comité peut faire appel à d'autres personnes possédant une expertise relative au domaine des technologies de l'information. Le secrétariat du comité est assumé par le Bureau.
>
> Les personnes faisant partie du comité ne sont pas rémunérées, sauf dans les cas, aux conditions et dans la mesure que peut déterminer le gouvernement. Elles ont cependant droit au remboursement des dépenses faites dans l'exercice de leurs fonctions, aux conditions et dans la mesure que le gouvernement détermine.

Plusieurs règles prescrivant les caractéristiques que doivent posséder les documents et les autres composantes des transactions électroniques sont développées dans le cadre des processus de normalisation technique. Il est donc nécessaire de s'assurer que les différentes normes techniques et standards développés dans le monde soient examinés afin d'assurer l'intégration ordonnée de ces normes dans celles qui seront reconnues conformes aux exigences de la loi. Aux termes de l'article 64, le Comité a pour mission d' :

> [...] examiner les moyens susceptibles :
>
> 1º d'assurer la compatibilité ou l'interopérabilité des supports et des technologies ainsi que des normes et standards techniques permettant de réaliser un document technologique, de le signer ou de l'utiliser pour effectuer une communication ;
>
> 2º d'éviter la multiplication des procédures, particulièrement en ce qui a trait à la vérification de l'identité des personnes ;
>
> 3º de favoriser la standardisation des certificats et des répertoires ainsi que la reconnaissance mutuelle des certificats ;

> 4º de garantir l'intégrité d'un document technologique par des mesures de sécurité physiques, logiques ou opérationnelles ainsi que des mesures de gestion documentaire adéquates pour en assurer l'intégrité au cours de tout son cycle de vie ;
>
> 5º d'uniformiser les pratiques d'audit, lequel comporte l'examen et l'évaluation des méthodes d'accès, d'entretien ou de sauvegarde du support, des mesures de sécurité physiques, logiques ou opérationnelles, des registres de sécurité et des correctifs apportés en cas de défaillance d'un élément pouvant affecter l'intégrité d'un document ;
>
> 6º de formuler des recommandations quant à l'application de la loi.

Le Comité élabore des guides de pratiques portant sur les sujets prévus à l'article 64. Ces guides colligent les consensus atteints sur ces sujets. Ces textes ne sont pas des règlements mais se présenteront vraisemblablement comme des outils à l'usage des personnes souhaitant utiliser les technologies de l'information pour effectuer des opérations juridiques. De tels documents se présentent habituellement comme des recommandations que les acteurs demeurent libres d'adopter ou d'implanter moyennant les modifications jugées nécessaires à leur propre situation.

Plusieurs organisations contribuent à la définition des standards que doivent satisfaire les documents et autres artefacts techniques. Certaines sont des instances étatiques ou des organisations internationales constituées par les États. La plupart sont des entités de droit privé.

Un premier ensemble est constitué d'organismes ayant une longue implication dans la standardisation des artefacts techniques et électriques. Ils sont principalement constitués de spécialistes des technologies concernées et on leur doit les standards qui rendent compatibles un grand nombre d'appareils informatiques nécessaires à la communication. Il s'agit d'organismes de normalisation tels la Commission électrotechnique internationale (CEI), l'Organisation internationale de standardisation (ISO), l'Union internationale des télécommunications (UIT), le Conseil canadien des normes (CCN) et le Bureau de normalisation du Québec (BNQ).

Un second ensemble mentionné à l'article 68 est constitué de groupes d'experts. Il s'agit de l'Internet Engineering Task Force (IETF) – une fédération de groupes organisés de façon informelle qui travaillent à l'évolution des technologies qui sous-tendent l'Internet et le World Wide Web Consortium (W3C) une organisation non gouvernementale mise en place afin d'assurer le développement optimal du WWW[16].

La place que prend la normativité technique de même que la relative insuffisance des règles étatiques requiert d'identifier les relais par lesquels la normativité doit nécessairement passer pour acquérir son effectivité.

B. Les relais de la normativité

Les relais sont les différents moyens par lesquels les acteurs d'Internet reçoivent et appliquent effectivement les normes perçues par eux comme relevantes ou obligatoires. 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. Il s'agit de prendre acte, de reconnaître les lois qui sont impératives et de les relayer, d'en combler les interstices afin d'en assurer une application concrète et effective.

La normativité est relayée aux acteurs par le truchement de la responsabilité et de la responsabilisation des acteurs. Pour la plupart des acteurs du cyberespace, la responsabilité se présente comme un ensemble de risques à gérer. Les personnes et entreprises 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.

---

16. Pour une présentation de ces divers organismes voir : Jacques BERLEUR et Yves POULLET, « Quelles régulations pour l'Internet ? », dans J. BERLEUR et al., *Gouvernance de la société de l'information*, Bruxelles, Bruylant, Presses Universitaires de Namur, 2002, p. 133-151 ; pour les organismes canadiens et québécois, voir : Daniel POULIN et Pierre TRUDEL (dir.), *Loi annotée concernant le cadre juridique des technologies de l'information*, *glossaire* <http://www.autoroute.gouv.qc.ca/loi_en_ligne/glossaire/glossaire.html>.

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 pourraient s'appliquer.

C'est de cette façon qu'au niveau des acteurs sont vécues les règles de droit. Pour gérer les risques associés aux possibles conflits, il leur revient d'expliciter leur compréhension des normativités. Ils le feront dans des règles de conduite qui s'adresseront aux limites qui doivent être respectées lors de l'émission de messages. Ils pourront aussi prévoir des règles et précautions à l'égard des messages qui peuvent être reçus.

C'est primordialement pour gérer les risques et tenter de baliser leur responsabilité que les acteurs mettent en place des mécanismes d'autorégulation[17]. Les processus d'autorégulation et de co-régulation sont les principaux relais des normativités encadrant les activités se déroulant dans le cyberespace. Par ces processus, on opère l'actualisation, l'adaptation et la particularisation des règles de droit considérées comme relevantes à un site ou à un environnement. De tels processus peuvent s'envisager comme un cycle continu dans lequel les besoins et les exigences découlant des autres normativités, dont les lois étatiques sont systématiquement pris en compte de manière évolutive.

Les règles de conduite s'expriment dans des cycles se développant généralement suivant cinq étapes. Premièrement, il importe de spécifier les fonctions et les vocations du site au plan des besoins d'y prévoir des normes. Deuxièmement, il faut déterminer et tenir à jour le socle d'obligations à respecter en vertu des législations étatiques. Troisièmement, il faut organiser la préparation des outils de régulation, codes, guides, FAQ. Quatrièmement, l'on procède à la rédaction du texte ou des textes normatifs. Cinquièmement, il faut assurer le suivi de l'application et la révision continue de la régulation ainsi mise en place[18].

---

17. Pour un exemple de méthodologie de gestion des risques et d'autoréglementation voir : Christophe ROQUILLY et Jean-Paul CAILLOUX, *Assurer la sécurité juridique des sites web, audit, méthodologie e-business*, Paris, Lamy-Les Échos, coll. « Agir en connaissance de cause », 2001, 153 p.
18. Pierre TRUDEL, « L'élaboration des règles de conduite pour les environnements Internet : éléments de méthode », dans Daniel POULIN, Éric LABBÉ, François JACQUOT et Jean-François BOURQUE, *Guide juridique du commerçant électronique*, Montréal, Éditions Thémis, 2003, p. 285-306.

2- Les principaux traits de la législation sur les documents technologiques

Le droit de la société de l'information porte sur les réalités de la société de l'information. L'univers de la société de l'information pose d'importants défis au législateur. Il comporte un important contingent de références à des concepts qui sont issus de l'univers des technologies de l'information. Le défi est de formuler des règles qui sauront procurer la prévisibilité et la flexibilité nécessaires pour encadrer le déroulement des transactions et autres interactions.

A. 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 s'explique par plusieurs facteurs.

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 lesquels 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.

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. 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 aussi l'internormativité entre les politiques publiques supranationales, nationales et infranationales.[19]

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. Au premier chef, la neutralité technologique ; la Loi ne spécifie pas la technologie qui doit être installée pour la réalisation et le maintien de l'intégrité des documents et l'établissement d'un lien avec un document. Le législateur demeure impartial par rapport aux standards et aux normes technologiques sur lesquels les intervenants ont porté leur choix pour les fins de la création et l'utilisation des documents.

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 et 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.

B. L'énonciation d'objectifs

L'énonciation d'objectifs dans les textes de lois tient habituellement une fonction symbolique, une fonction informative et une fonction interprétative. En formulant les objectifs, le législateur recherche souvent un effet d'affichage d'une politique déterminée ou de la finalité du texte. On décèle alors la fonction symbolique de la disposition proclamant les objectifs. On vise un effet d'annonce afin de guider le lecteur du texte. Deuxièmement, la formulation d'objectifs représente une sorte de « pédagogie de l'explication ». En les énonçant, la loi tend à éduquer le citoyen en certains domaines. Cela peut aussi servir à inspirer les auteurs des textes réglementai-

19. Charles-Albert MORAND, *Le droit néo-moderne des politiques publiques*, Paris, L.G.D.J., 1999, p. 190.

res ou quasi réglementaires, tels que ceux prévus aux articles 63 et suivants relativement aux mesures à prendre afin d'harmoniser les systèmes, les normes ainsi que les standards techniques. Enfin, troisièmement, la formulation d'objectifs a une valeur interprétative. Il est usuel que l'interprète donne au texte de la loi un sens conforme à ce qui est présenté comme l'objectif ou la finalité de la loi[20].

Les objectifs visés par les lois encadrant les activités se déroulant dans le cyberespace sont généralement d'assurer la sécurité et la prévisibilité du droit. Animés d'un souci de promouvoir le commerce électronique tenu pour être porteur de progrès et de richesse, on veut s'assurer d'un cadre juridique adapté et prévisible.

Un premier objet de la *Loi concernant le cadre juridique des technologies de l'information* est d'ailleurs d'assurer la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports. Ainsi, la loi précise les précautions à prendre afin de conserver la validité juridique des documents tout au long de leur cycle de vie.

La loi a pour second objet d'assurer la cohérence des règles de droit et leur application aux communications effectuées au moyen de documents qui sont sur des supports faisant appel aux technologies de l'information. On vise tous les supports qu'ils soient électronique, magnétique, optique, sans fil ou autres ou faisant appel à une combinaison de technologies.

Un troisième objet de la loi est d'assurer l'équivalence fonctionnelle des documents et leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent. La loi indique comment les situations juridiques connues dans le monde des documents sur papier se transposent dans un univers où l'on fait usage de documents s'appuyant sur les technologies. On se fonde sur les fonctions accomplies par les différents gestes et processus de production et de circulation des documents[21].

---

20. Jean-Louis BERGEL, « Essai de synthèse », dans *La formulation d'objectifs dans les textes législatifs*, (1989) 14 *R.R.J.* 975, 980.
21. *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c. 32, en ligne avec annotations à <http://www.autoroute.gouv.qc.ca/loi_en_ligne>, art. 1.

C. *Des notions neutres pour désigner les artefacts techniques : la notion de document*

Le souci de neutralité technologique est incarné dans la notion charnière de la *Loi concernant le cadre juridique des technologies de l'information*, celle de document. Ce qui est caractéristique des tendances induites par la numérisation est le haut niveau d'interchangeabilité des artefacts sur lesquels peut être consignée l'information. Le texte d'un exposé présenté dans une conférence peut être consigné, sous forme de fichier numérique, sur le disque dur d'un ordinateur ; ce même fichier peut être transmis par courriel, il peut être copié dans une clé USB ou sur un disque CD-ROM. Cette versatilité appelle un régime juridique axé sur les conditions à respecter pour assurer la valeur juridique de l'information.

La loi uniforme canadienne comporte une définition du mot « électronique » se lisant comme suit :

> « électronique » : Créé, enregistré, transmis ou mis en mémoire sous forme numérique ou sous une autre forme intangible par des moyens électroniques, magnétiques ou optiques ou par d'autres moyens capables de créer, d'enregistrer, de transmettre ou de mettre en mémoire de façon similaire à ceux-ci ; « électroniquement » a le même sens.

Au Québec, avec la *Loi concernant le cadre juridique des technologies de l'information*, la réalité numérique est appréhendée par l'énoncé d'une définition se voulant générale et non tributaire d'un procédé technique en particulier. Ainsi, le document technologique y est défini comme un document réalisé en utilisant l'une ou l'autre des technologies capables de produire un objet dans lequel l'information est délimitée, structurée et intelligible sous la forme de mots, de sons ou d'images. Un document constitué de signes, qu'il soit sur un support numérique ou sur un support optique, est un document technologique.

Le document est défini comme étant de l'information délimitée et structurée portée par un support. L'unité de base constitutive du document est l'information. Ce qui caractérise le document est le fait que l'information y est délimitée et structurée de façon tangible ou logique, compte tenu du support. L'information délimitée et structurée – le document – constitue ainsi la notion fondamentale du droit relatif au statut des documents et, en particulier, de l'écrit en droit québécois. L'article 3 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 2º de l'article 1 sont qualifiés dans la présente loi de documents technologiques.

La notion d'écrit, historiquement associée au papier est remplacée par celle, plus générale, de document. Et la notion de document est définie de manière à affranchir celui-ci du support. Ce qui est de l'essence du document, c'est l'information. Il faut que celle-ci soit délimitée et structurée de façon tangible et logique, et elle doit être intelligible sous forme de mots, de sons ou d'images. L'écrit n'est plus le point central du droit de la preuve. L'information structurée dans un document tend de plus en plus à se constituer comme la notion de référence.

Le second alinéa de l'article 3 de la Loi assimile à un 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. Cette assimilation entre banque de données et document tient compte du fait que plusieurs documents technologiques sont obtenus en actionnant des fonctions de banques de données. Par exemple, les informations d'un formulaire saisi sur une page web sont souvent conservées dans des banques de données capables de restituer, lorsque demandé, le document qui a été initialement complété, tel un formulaire rempli en ligne puis transmis. Seules certaines informations variables peuvent être transmises, tandis que le formulaire est consigné dans la banque de données.

L'assimilation est un procédé utilisé par le législateur afin de conférer à un objet le statut juridique d'un autre objet. L'assimilation de la banque de données à la notion de document ne transforme pas celle-ci en document, mais entraîne à son égard l'application des règles qui régissent les documents. Par conséquent, on traite les banques de données dans la Loi comme on traite les documents.

Un dossier réfère à un ensemble de documents relativement à une personne ou à une question spécifique. Par exemple, un dossier médical, un dossier de conduite automobile, un dossier scolaire. L'article 3 de la Loi précise qu'un dossier peut être composé d'un ou de plusieurs documents. La précision a son importance, car plusieurs personnes ou entreprises gèrent leurs documents à l'aide de dossiers (par ex. : domaine des assurances, domaine médical). La notion de dossier renvoie à un ensemble de documents de même qu'au contenant de ces documents.

Même les documents technologiques dont l'information est fragmentée ou qui sont réunis en un seul pour des fins de transmission ou de conservation conservent cette qualité s'ils rencontrent certaines conditions énoncées à l'article 4 :

> **4.** Un document technologique, dont l'information est fragmentée et répartie sur un ou plusieurs supports situés en un ou plusieurs emplacements, doit être considéré comme formant un tout, lorsque des éléments logiques structurants permettent d'en relier les fragments, directement ou par référence, et que ces éléments assurent à la fois l'intégrité de chacun des fragments d'information et l'intégrité de la reconstitution du document antérieur à la fragmentation et à la répartition.
>
> Inversement, plusieurs documents technologiques, même réunis en un seul à des fins de transmission ou de conservation, ne perdent pas leur caractère distinct, lorsque des éléments logiques structurants permettent d'assurer à la fois l'intégrité du document qui les réunit et celle de la reconstitution de chacun des documents qui ont été ainsi réunis.

Ainsi, l'unité de lieu et de support n'est plus un élément déterminant de l'existence d'un document. C'est la structuration selon des éléments logiques qui devient déterminante. Le principe ouvre la voie à la reconnaissance juridique des objets virtuels, ceux qui sont à la fois ici et ailleurs.

D. La qualité de l'information

Les rapports entre les règles de droit et la qualité de l'information sont au cœur des questions que doit résoudre le droit. Une grande part du corpus de règles encadrant la production et la circulation de l'information est concernée par le souci d'assurer que l'information produite ou transmise soit de qualité.

Pour certaines situations, le législateur détermine *a priori*, le seuil de qualité nécessaire pour engendrer une conséquence juridique. Mais le plus souvent, la qualité est exprimée dans un standard d'appréciation des conduites ou des caractéristiques des objets. La plupart des législations exigent que les échanges d'informations inhérents aux transactions s'effectuent selon des standards de lisibilité, de précision et d'exactitude[22]. Alors, le droit institue des processus afin d'évaluer si une entité possède ou non le niveau requis de qualité[23]. C'est cette approche qui est généralement retenue dans les lois relatives à l'information numérique. Au Québec, des exigences de qualité sont énoncées entre autres à l'égard des documents, au titre des conditions de validité. L'opposabilité des documents préprogrammés de même que les caractéristiques des originaux et des copies sont tributaires des qualités que possèdent ces objets.

1. L'intégrité

Au nombre des exigences de qualité que prescrit le droit à l'égard de l'information, il y a l'intégrité. La *Loi concernant le cadre juridique des technologies de l'information*[24] identifie les qualités que doivent posséder les documents technologiques pour être considérés comme intègres. L'article 6 de cette loi prévoit que :

> **6.** L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulues.

---

22. Vincent GAUTRAIS, « La couleur du consentement électronique », (2003) 16 *C.P.I.* 61-127.
23. Pierre TRUDEL, « Law in Pursuit of Information Quality », dans Urs GASSER (éd.) *Information Quality Regulation : Foundations, Perspectives, and Applications*, Baden-Baden, Nomos Verlagsgesellschaft, 2004, p. 91 à 106.
24. L.Q. 2001, c. 32, en ligne avec annotations à <http://www.autoroute.gouv.qc.ca/loi_en_ligne>.

> L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction.
>
> Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie.

Dans cette disposition, l'intégrité est une qualité que possède un document. Elle résulte de deux éléments : premièrement, on considère que l'intégrité d'un document est assurée lorsqu'il y a possibilité de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité. Deuxièmement, il faut que le support portant l'information procure à celle-ci la stabilité et la pérennité voulues[25]. Il ne faut pas que l'information soit volatile ou susceptible de disparaître ou d'être modifiée sans que l'on puisse s'en apercevoir. C'est à une appréciation *in concreto* que l'on renvoie ici. Les qualités que doivent posséder un document ne sont pas déterminées une fois pour toutes : elles dépendent plutôt de leur capacité à procurer des moyens de vérifier le maintien intégral du document de même qu'elle appelle à une évaluation de la capacité technique du support à procurer stabilité et pérennité. Une telle capacité s'apprécie nécessairement dans chaque contexte particulier.

Le seuil de qualité que doivent posséder les informations est ici exprimé au moyen d'un standard. Le standard est une norme souple fondée sur un critère intentionnellement indéterminé. Cette technique convient aux situations pour lesquelles il est malaisé de formuler une règle *a priori* sur les comportements que doivent avoir les sujets de droit. La transmission de l'information, caractérisée par son évolution rapide et la place importante qu'elle laisse à l'activité créatrice s'accommode mal de règles détaillées. Le standard ne tend pas à une délimitation objective de ce qui est permis et de ce qui est défendu. Il constitue plutôt une formule d'appréciation de la conduite des personnes sur la base d'un type-modèle. Il constitue une directive générale qui indique le but poursuivi. Il constitue un guide qui identifie le seuil ou le résultat qu'il faut atteindre[26].

---

25. *Loi concernant le cadre juridique des technologies de l'information*, art. 6, al. 1.
26. André-Jean ARNAUD, *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., Paris, L.G.D.J., 1993, p. 581.

Dans les matières fortement marquées par la vélocité des mutations techniques, il est difficile 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 technologies de l'information, l'on constate souvent que le législateur ne maîtrise pas les données scientifiques et techniques, ou que ces données sont susceptibles de changer. Plutôt que de formuler la loi en se référant à un contexte technique susceptible de changer très rapidement, l'on va plutôt établir, dans la loi, les caractéristiques que doivent posséder les réalités que l'on régit.

Par exemple, il peut être difficile, compte tenu de la grande variété de contextes, d'identifier les qualités que doivent posséder les documents technologiques pour être considérés comme intègres. Alors, le législateur se limite à réaffirmer son attachement à certaines valeurs et proclamer des principes dont il doit être tenu compte. En somme, on élabore des règles comportant des directives – non des prescriptions. Le standard commande à l'interprète, au juge de se référer à un autre système normatif : comme ceux qui prescrivent les meilleures pratiques, techniques ou précautions afin d'atteindre un résultat à l'égard de documents[27].

2. Les qualités requises pour les documents préprogrammés

Dans les univers d'interaction, l'exigence de qualité de l'information se confond avec celle de l'équité dans les interactions. Les interfaces préprogrammées destinées à encadrer les interactions doivent donc également répondre à des exigences qualitatives.

Dans la *Loi uniforme canadienne sur le Commerce électronique*[28] cette réalité est visée par la notion d'agent électronique. L'article 19 se lit comme suit :

---

27. Marcel O. STATI, *Le standard juridique*, Paris, Librairie de jurisprudence ancienne et moderne Édouard Duchemin, 1927 ; Pierre TRUDEL, « Le standard de programmation de haute qualité dans la législation sur la radio et la télévision », (1989) 34 *R.D. McGill* 203.
28. CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, *Loi uniforme sur le commerce électronique*, <http://www.law.ualberta.ca/alri/ulc/current/fueca-a.htm>.

> **19.** Dans la présente partie, « agent électronique » s'entend d'un programme informatique ou d'un moyen électronique qui permet d'entreprendre une action ou de répondre à des documents électroniques ou à des actions en tout ou en partie, sans examen par une personne physique au moment de la réponse ou de l'action.

L'article 35 de la *Loi concernant le cadre juridique des technologies de l'information* assure une protection à ceux qui utilisent un document préprogrammé, tel un formulaire électronique. Il oblige ceux qui offrent ces produits ou services au moyen de tels documents préprogrammés à fournir certaines fonctionnalités, soit :

– des instructions nécessaires pour que la personne qui utilise un document préprogrammé puisse dans les meilleurs délais l'aviser d'une erreur commise ou disposer des moyens pour prévenir ou corriger une erreur ;

– des instructions ou des moyens afin que la personne soit en mesure d'éviter l'obtention d'un produit ou d'un service dont elle ne veut pas ou qu'elle n'obtiendrait pas sans l'erreur commise ou pour qu'elle soit en mesure de le rendre ou, le cas échéant, de le détruire.

Si ces fonctionnalités ne sont pas disponibles, cela emporte l'inopposabilité de la communication – *i.e.* qu'elle n'a pas d'effet à l'encontre de qui on veut l'invoquer – ou l'annulation de la transaction. La notion d'erreur est ici très large car elle vise toute erreur : qu'elle découle d'une erreur de manipulation faite par l'usager ou qu'elle résulte du mauvais fonctionnement du document préprogrammé. Par exemple, cette notion englobe une erreur générée par le logiciel ou par l'utilisateur lui-même. Ainsi, si un client remplit un formulaire de commande en ligne, commet une erreur et que ce formulaire ne comporte pas ce qu'il faut afin de prévenir ou corriger une erreur, la personne qui offre par ce moyen un produit ou un service ne pourra pas se prévaloir du formulaire, c'est-à-dire l'invoquer contre le client[29].

29. Charlaine BOUCHARD et Marc LACOURSIÈRE, « Les enjeux du contrat de consommation en ligne », (2003) 33 *R.G.D.* 373-438, 389.

3. La notion d'exemplaire original et de copie

Dans l'univers numérique, il peut devenir difficile, parfois inutile de distinguer entre l'original et la copie. Mais certains documents doivent impérativement posséder un original tandis que les copies de ce dernier sont réputées posséder un statut différent. Le principe de l'équivalent fonctionnel joue pleinement lorsque l'on se demande ce qu'il advient, dans l'univers numérique des notions d'original et de copie. Ce qui caractérise l'original au regard de la copie, c'est que l'original présente des qualités laissant présumer d'une plus grande fiabilité. L'original a souvent un caractère unique alors que la copie peut être multiple.

La *Loi uniforme canadienne* fait échos au fait que le rôle premier du document original est de garantir l'intégrité de l'information qu'il contient. Il est en général plus difficile de modifier un original qu'une copie. La loi assimile le document électronique à un original si une garantie fiable est donnée quant à l'intégrité de l'information qu'il renferme. L'article 11 de la *Loi uniforme canadienne* prévoit en effet que :

> **11.** (1) L'exigence d'une règle de droit [d'une juridiction compétente] qu'une personne présente ou conserve un document sous sa forme originale est satisfaite avec la fourniture ou la conservation d'un document électronique, si les conditions suivantes sont réunies :
>
> a) il existe une garantie fiable quant à l'intégrité de l'information contenue dans le document électronique à compter du moment où celui-ci a été créé jusqu'au moment où il est présenté ou conservé, sous forme d'un document papier ou électronique ;
>
> b) lorsque le document sous sa forme originale doit être fourni à une personne, celle-ci a accès au document électronique et peut le conserver de façon à ce qu'il soit utilisable pour consultation ultérieure ;
>
> [...]
>
> (2) Pour l'application de l'alinéa (1)a) :
>
> a) l'intégrité de l'information s'apprécie en déterminant si celle-ci est restée complète et n'a pas été altérée, exception faite de l'introduction de toute modification intervenant dans le cours normal de la communication, de la mise en mémoire et de l'affichage ;

> b) le niveau de fiabilité requis s'apprécie eu égard à l'objet pour lequel le document électronique a été créé et à la lumière de toutes les circonstances pertinentes.

De son côté, la loi québécoise prévoit les conditions que doit remplir un document technologique pour remplir la fonction d'original :

> **12.** Un document technologique peut remplir les fonctions d'un original. À cette fin, son intégrité doit être assurée et, lorsque l'une de ces fonctions est d'établir que le document :
>
> 1º est la source première d'une reproduction, les composantes du document source doivent être conservées de sorte qu'elles puissent servir de référence ultérieurement ;
>
> 2º présente un caractère unique, les composantes du document ou de son support sont structurées au moyen d'un procédé de traitement qui permet d'affirmer le caractère unique du document, notamment par l'inclusion d'une composante exclusive ou distinctive ou par l'exclusion de toute forme de reproduction du document ;
>
> 3º est la forme première d'un document relié à une personne, les composantes du document ou de son support sont structurées au moyen d'un procédé de traitement qui permet à la fois d'affirmer le caractère unique du document, d'identifier la personne auquel le document est relié et de maintenir ce lien au cours de tout le cycle de vie du document.
>
> Pour l'application des paragraphes 2º et 3º du premier alinéa, les procédés de traitement doivent s'appuyer sur des normes ou standards techniques approuvés par un organisme reconnu visé à l'article 68.

L'article 12 détermine, comme le fait la loi uniforme canadienne, comment ce concept se transpose dans l'univers des technologies de l'information. Cet article prévoit que les fonctions d'un original sur support papier peuvent être satisfaites par un document technologique à certaines conditions. Cette disposition assure l'équivalence fonctionnelle de la notion d'original.

Cette disposition permet de préciser les conditions à remplir pour qu'un document qui, par sa nature, ne doit comporter qu'un original (ou qu'un seul original) puisse être établi par un document technologique. Par exemple, un chèque établi par un document technologique doit comporter les caractéristiques mentionnées à l'article 12.

L'article 19 de la loi québécoise établit la règle équivalente à celle de l'article 11 de la loi uniforme lorsqu'il précise les exigences que doit respecter la personne qui a l'obligation de conserver un document.

La loi québécoise prévoit aussi l'équivalent fonctionnel de la notion d'original en utilisant le critère d'intégrité. Mais la portée de la loi québécoise est plus précise, en identifiant plus d'une fonction à l'original, non pas seulement la fonction de garantir l'intégrité de l'information comme la loi uniforme canadienne. La loi québécoise traite aussi du caractère unique et de la relation avec une personne lorsqu'un document assure une fonction d'original (ex. : fonction d'être unique d'un chèque). L'équivalent technologique d'un tel document doit rencontrer les caractéristiques mentionnées dans la loi. Ceci permet de transposer dans l'univers électronique, par exemple les exigences inhérentes à des documents par nature uniques comme les diplômes, les effets négociables ou certaines œuvres de création.

3- Le cycle de vie des documents

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.

A. Le choix du support

Le cycle de vie du document commence par sa création. Comme un document peut être consigné sur différents supports, se pose la question de savoir qui décide du choix du support ? La loi québécoise affirme le principe de la liberté de choisir, d'utiliser ou d'accepter l'information sous forme électronique. L'article 2 énonce le principe général de la liberté des personnes quant au choix des supports qui servent à produire des documents :

> **2.** À moins que la loi n'exige l'emploi exclusif d'un support ou d'une technologie spécifique, chacun peut utiliser le support ou la technologie de son choix, dans la mesure où ce choix respecte les règles de droit, notamment celles prévues au Code civil.

> Ainsi, les supports qui portent l'information du document sont interchangeables et, l'exigence d'un écrit n'emporte pas l'obligation d'utiliser un support ou une technologie spécifique.

Les lois affirment le principe de l'utilisation non obligatoire des documents électroniques ou technologiques. Ainsi, l'article 6(1) de la *Loi uniforme canadienne* prévoit que :

> **6.**(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.

La liberté de choix des supports 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 également mentionné à l'article 5.

Plusieurs articles de la loi québécoise viennent préciser la portée du principe de la liberté du choix des supports et des technologies. Ainsi, l'article 29 applique ce principe pour la transmission et la réception de documents.

> **29.** 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.
>
> De même, nul n'est tenu d'accepter de recevoir un document sur un autre support que le papier ou au moyen d'une technologie dont il ne dispose pas.
>
> Lorsque quelqu'un demande d'obtenir un produit, un service ou de l'information au sujet de l'un d'eux et que celui-ci est disponible sur plusieurs supports, le choix du support lui appartient.

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 cocontractant. Des lois particulières peuvent imposer l'usage d'un support ou d'une technologie spécifique.

B. La détention et la garde

Celui qui a la garde de l'information – qui exerce la maîtrise physique et intellectuelle – sur le support de documents est tenu à des devoirs.

L'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* vise le cas où un document technologique est confié à un prestataire de services (par exemple, l'archivage de documents hors site) pour qu'il en assure la garde. 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.

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 a 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. En dehors des devoirs qui lui incombent, le prestataire n'a pas la maîtrise du document. Ainsi, selon le type de prestation qu'il s'oblige à assurer, il sera réputé exercer plus ou moins de contrôle sur le document et en supportera la responsabilité qui en découle.

C. La modification

Une disposition porte sur les situations où un document technologique est modifié durant la période pendant laquelle il doit être conservé. L'article 21 de la Loi se lit comme suit :

> **21.** Lorsqu'une modification est apportée à un document technologique durant la période où il doit être conservé, la personne qui a l'autorité pour faire la modification doit, pour en préserver l'intégrité, noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui et pourquoi la modification a été faite. Celle-ci fait partie intégrante du document, même si elle se trouve sur un document distinct.

On y précise les conditions qui doivent alors être respectées afin de préserver la valeur juridique du document en dépit de la modification. Si ces conditions n'étaient pas observées, il pourrait être considéré que la modification de l'information constitue une altération du document, ce qui porterait atteinte à son intégrité, et par le fait même, à sa valeur juridique.

Sous peine de faire perdre au document sa valeur juridique, la personne qui a l'autorité pour faire la modification doit noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui ainsi que la raison de la modification.

La modification ainsi effectuée fait partie intégrante du document même si elle se trouve sur un document distinct. Cela peut être dans une annexe ou son équivalent. Par exemple, une modification au registre de l'état civil ou une correction à une inscription sur un registre foncier doit se faire conformément à l'article 21 pour préserver l'intégrité des documents. Un dossier tenu sur une personne et qui ferait l'objet d'une modification doit être pareillement documenté. Par exemple, un dossier tenu par un employeur sur un employé auquel une modification serait apportée.

D. L'accès et la consultation

Le droit d'accéder aux documents ne va pas de soi. Il est prévu par des lois qui en délimitent la portée. La loi 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[30]. 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 par le recours aux technologies de l'information est intégrée dans la loi (par exemple, les articles 40, 50 et 60). De plus, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[31] est modifiée pour permettre l'accès aux documents des organismes publics à distance et non plus seulement par consultation sur place ou par obtention d'une copie[32].

E. La transmission

Les articles 28 à 37 de la *Loi concernant le cadre juridique des technologies de l'information* précisent les conditions à respecter pour transmettre des documents technologiques. On y prescrit des règles équivalentes, à l'égard des documents technologiques, à celles qui s'appliquent habituellement lorsqu'il s'agit de transmettre des documents sur support papier. Le document peut être transmis, envoyé ou expédié. On peut utiliser tout mode de transmission approprié à son support sauf si la loi exige l'emploi exclusif d'un mode spécifique de transmission. C'est le principe de la liberté des modes de transmission qui est ici affirmé. Cette liberté peut être limitée par la loi qui peut exiger un mode spécifique de transmission[33].

L'article 29 applique le principe de la liberté de se procurer ou non certaines technologies pour la transmission de documents. L'article 30 énonce les conditions pour que le document technologique reçu ait la même valeur que le document transmis. Pour ce faire, le mode de transmission choisi doit permettre de préserver

30. *Loi concernant le cadre juridique des technologies de l'information*, art. 23.
31. L.R.Q., c. A-2.1.
32. *Loi concernant le cadre juridique des technologies de l'information*, art. 82, 83, 84, 85.
33. *Ibid.*, art. 28.

l'intégrité, tant du document expédié que de celui qui est reçu. La documentation établissant la capacité d'un mode de transmission de préserver l'intégrité doit être disponible pour production en preuve, le cas échéant.

On ne peut contraindre une personne à recevoir un document au moyen d'une technologie dont on ne dispose pas et exiger de quelqu'un qu'il se procure un support ou une technologie spécifique pour transmettre ou recevoir un document. Cependant, les parties à un contrat peuvent s'entendre sur le choix d'un support particulier pour la transmission d'un document. Aussi, conformément à l'article 2 de la loi, cette liberté de choix peut, dans certaines circonstances, être limitée par certaines lois qui imposent l'usage d'un support particulier.

Des présomptions aident à déterminer le moment de l'expédition et de la réception d'un document technologique[34]. Un document technologique est présumé transmis, envoyé ou expédié si deux conditions sont remplies :

- le geste qui marque le début de son parcours vers l'adresse active du destinataire est accompli par l'expéditeur ou sur son ordre ; et

- que ce parcours ne peut être contremandé ou, s'il peut l'être, n'a pas été contremandé par lui ou sur son ordre. Par exemple : cliquer sur le bouton « send » ou sur un icône alors que cette commande ne peut être annulée ou n'est pas de fait contremandée.

Une présomption d'intégrité existe en faveur des tiers pour les documents technologiques que les entreprises ou l'État mettent à leur disposition à partir d'un système ou d'un logiciel[35]. L'article 32 adapte l'obligation qui est faite dans une loi d'expédier plusieurs exemplaires d'un document au contexte des technologies de l'information : cette obligation peut être satisfaite au moyen d'un seul exemplaire ou copie.

F. La conservation

Dès lors qu'une personne est tenue de conserver un document, elle a le devoir d'en assurer l'intégrité et l'accessibilité. Elle

34. *Ibid.*, art. 31.
35. *Ibid.*, art. 33.

doit voir à la disponibilité du matériel permettant de le rendre accessible et de l'utiliser aux fins auxquelles il est destiné (art. 19). Par exemple, elle doit disposer du logiciel ou du matériel nécessaire pour que l'on puisse prendre connaissance du document. L'article 20 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[36]. 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, condition nécessaire au maintien de sa valeur juridique.

1. Le transfert de support

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. Les articles 17 et 18 traitent du processus de changement du support de l'information. Par exemple, on vise ici les opérations telles que celles consistant à 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.

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[37].

L'article 18 vient faciliter l'admission en preuve des documents résultant de tel transfert. Donnant effet au principe des lois uniformes sur le commerce électronique, cette disposition écarte toute règle de preuve pouvant s'opposer à l'admissibilité d'un document résultant d'un tel transfert.

36. *Ibid.*, art. 21.
37. *Ibid.*, art. 17.

L'article 20 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.

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

Si ces conditions sont rencontrées, le document qui a fait l'objet d'un transfert peut être détruit et remplacé par le document résultant du transfert. Cependant, tout document présentant une valeur archivistique, historique ou patrimoniale doit être conservé sur son support d'origine.

2. 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.

G. 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. Ces conditions sont de :

– 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- La protection des personnes

Les droits relatifs à l'information comportent une dimension axée sur la protection des intérêts des personnes. Ainsi, 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 »[38]. 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.

A. Les renseignements personnels

Le droit à la protection des renseignements personnels constitue une facette des régimes de protection de la vie privée[39]. 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[40]. 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[41].

---

38. 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.
39. 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.
40. *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1, art. 10 (ci-après désignée *Loi sur le secteur privé* ; *Loi sur l'accès*, art. 53 ; voir aussi le *Code civil du Québec*, art. 35 à 41.
41. *Loi sur l'accès*, art. 65 ; *Loi sur le secteur privé*, art. 6.

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 lesquelles 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[42].

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[43]. Il faut expliquer de

42. *Loi sur l'accès*, art. 59, 67 ; *Loi sur le secteur privé*, art. 13, 18.
43. *Loi sur le secteur privé*, art. 8 et 27 ; *Loi sur l'accès*, art. 65 et 83.

façon claire et simple quel type de renseignement personnel est recueilli, dans quel but et expliquer la manière dont cette information est traitée[44]. 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.

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[45]. 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[46]. Elle dispose d'un droit de recours auprès de la Commission d'accès à l'information lorsque ces droits lui sont déniés[47].

1. La protection de la confidentialité lors de l'accès

L'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* a pour objet de protéger les renseignements confidentiels lors de la consultation de documents technologiques.

---

44. AUSTRALIAN PRIVACY COMMISSIONER'S, *Guidelines for Federal and ACT Government Websites*, <http://www.privacy.gov.au/internet/web/index.html>.
45. Voir les articles 38 à 40 du C.c.Q ; *Loi sur le secteur privé*, art. 27 et s. ; *Loi sur l'accès*, art. 83 et s.
46. *Loi sur l'accès*, art. 89 et s. ; *Loi sur le secteur privé*, art. 28 ; art. 40 C.c.Q.
47. *Loi sur le secteur privé*, art. 42 à 53 ; *Loi sur l'accès*, art. 135 et s.

Il est fait obligation à la personne responsable de l'accès à un tel document technologique de prendre les mesures de sécurité propres à en assurer la confidentialité.

Au nombre des moyens qui peuvent être utilisés, il y a le contrôle d'accès effectué au moyen :

- d'un procédé de visibilité réduite (par exemple, rendre des données invisibles à l'écran) ;

- d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ; (par exemple, en exigeant que les personnes autorisées donnent un mot de passe avant d'accéder à l'information) ;

- ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder (par exemple, le système doit être configuré de manière à ce qu'il ne soit pas possible d'accéder de façon détournée à un document ou au renseignement confidentiel).

Ces obligations supposent de mettre en place des mécanismes qui segmenteront les accès selon les habilitations reconnues aux personnes. C'est en somme une invitation à mettre en place de façon systématique, des politiques relatives aux droits d'accès au sein des organisations.

2. La limitation des fonctions de recherche

L'article 24 de la *Loi concernant le cadre juridique des technologies de l'information* permet de restreindre l'utilisation des fonctions de recherche extensive à l'égard des documents technologiques comportant des renseignements personnels et rendus publics 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 renseignements personnels pour des fins autres que celles pour lesquelles ils ont été recueillis ou diffusés.

Dans l'univers des documents sur papier, la recherche est souvent longue puisque les documents doivent être examinés un à un. Pour les documents technologiques, les possibilités de recherche sont démultipliées, ce qui peut laisser craindre des abus.

Ainsi, la personne responsable de l'accès à ces documents doit voir à ce que les moyens technologiques soient mis en place pour assurer la protection des renseignements personnels contenus dans ces documents publics. Cette restriction de l'utilisation des fonctions de recherche est limitée à ce qui est nécessaire afin d'assurer le respect de la finalité pour laquelle ces documents ont été rendus publics.

À titre d'exemple de ce type de documents, il y a ceux contenus dans le registre foncier et le registre des droits personnels et réels mobiliers. Il est possible, pour la personne responsable de ces registres, de limiter les fonctions de recherche dans le but d'assurer la protection des renseignements personnels qui y sont inclus. Il lui est alors loisible de fixer des conditions pour l'utilisation de ces fonctions de recherche. Ces conditions doivent tenir compte des critères énoncés par le gouvernement.

Le paragraphe 2° de l'article 69 permet au gouvernement de déterminer par règlement « des critères d'utilisation de fonctions de recherche extensive de renseignements personnels dans les documents technologiques qui sont rendus publics pour une fin déterminée ». Ce pourrait être, par exemple, les critères d'utilisation des fonctions de recherche extensive dans le cas de la recherche historique. Il existe en effet des fins légitimes à la recherche dans un document technologique. Par exemple, la recherche historique n'est pas en soi une atteinte à la vie privée, du moins selon la conception qui en est généralement retenue.

Ce genre de mesure procède de l'idée suivant laquelle que dans l'univers des documents sur papier la recherche est souvent longue puisque les documents doivent être examinés un à un. Pour les documents technologiques, les possibilités de recherche sont démultipliées, ce qui peut laisser craindre des abus. Devant cette possibilité hypothétique d'abus, la solution retenue est d'imposer la mise en place de moyens technologiques pour assurer la protection des renseignements personnels contenus dans ces documents publics. Et cette protection est de limiter l'accès uniquement aux fins pour lesquelles un document est rendu public comme si ces fins étaient connues et spécifiées, ce qui n'est pas toujours facile à déterminer. Cette approche reflète une tendance à nier le caractère social des informations portant sur les personnes.

Les décideurs vont devoir spécifier les finalités du caractère public d'une information : un exercice qui suppose de poser un jugement de valeur sur la légitimité des recherches que l'on peut faire à partir des données publiques. Il est en effet difficile de concevoir comment une telle démarche est possible sans porter un jugement *a priori* sur la légitimité de certaines recherches ; sans parler de la difficulté de déterminer, en l'absence de texte législatif, ce qui constitue la finalité du caractère public d'une information. En fait, lorsqu'une information est à caractère public, elle est de libre parcours, sauf à démontrer qu'on en fait un usage fautif ou contraire à une loi. On ne peut présumer, sans nier le caractère public d'une information, qu'une information ne doit servir qu'à certaines fins et pas à d'autres. La seule limite légitime à l'usage d'une information à caractère public est le caractère abusif de l'usage. Mais postuler *a priori* que des usages seraient abusifs laisse fort peu de place au droit à l'information.

B. Les informations biométriques

Les articles 43, 44 et 45 de la *Loi concernant le cadre juridique des technologies de l'information* édictent des mesures de contrôles à l'égard de l'utilisation des mesures biométriques[48] comme moyen d'identification d'une personne[49].

L'article 43 interdit d'exiger sans consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. C'est le principe de l'interdiction d'exiger l'utilisation d'un procédé ou d'un dispositif

48. La biométrie est la science qui étudie à l'aide des mathématiques statistiques, les probabilités et les variations biologiques à l'intérieur d'un groupe déterminé. Les mesures biométriques sont celles qui concernent l'ensemble des caractéristiques personnelles distinctives d'une personne. Elles peuvent être lues par des systèmes informatiques et utilisées afin d'identifier une personne. Les empreintes digitales sont l'exemple le plus connu de caractéristiques biométriques. Il est également possible d'utiliser la voix, les empreintes de la rétine, la démarche et même l'ADN d'une personne pour l'identifier. Voir : Daniel POULIN et Pierre TRUDEL, (dir.), *Loi annotée concernant le cadre juridique des technologies de l'information*, *glossaire* <http://www.autoroute.gouv.qc.ca/ loi_en_ligne/glossaire/glossaire.html>.
49. Voir : Marc CHASSÉ, *La biométrie au Québec : les enjeux, document d'analyse*, Québec, Commission d'accès à l'information, juillet 2002, CAI <http://www.cai.gouv.qc.ca/home_00_portail/thema_biometrie.html>.

qui porte atteinte à son intégrité physique pour établir l'identité d'une personne. Ce peut être par exemple, une puce implantée dans le corps ou le 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 limite le recours à l'identification biométrique. Le consentement exprès de la personne est exigé. 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. 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 à la suite de 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. 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.

L'article 46 de la loi 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.

La création et l'existence d'une banque de caractéristiques ou de mesures biométriques qu'elle soit ou non en service doit être préalablement divulguée à la Commission d'accès qui 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. La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction.

La Commission d'accès à l'information 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.

5- L'identification des personnes

L'identification est un processus inhérent à la vie sociale. Le processus d'identification est essentiellement une démarche visant à réduire les risques et l'incertitude qui peuvent exister lorsqu'on veut entrer en relation avec une autre personne. Le cadre juridique de l'identification se présente, pour une bonne part, comme un ensemble de moyens et mécanismes afin de réduire l'incertitude et d'assurer un niveau acceptable de risques aux personnes désireuses de devenir partie à une transaction. La cryptographie et les autres moyens qui peuvent être utilisés afin d'identifier les personnes dans les transactions se déroulant sur Internet ou dans d'autres réseaux sont autant de mécanismes afin de procurer les informations nécessaires pour identifier correctement les parties à une transaction.

Pour assurer le déroulement de la plupart des activités, il est nécessaire de 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 qui l'on a affaire. C'est pourquoi on définit l'identification comme 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.

Essentiellement, l'identification est un processus destiné à réduire l'incertitude. Il vise à procurer la quantité optimale d'information à l'égard d'une personne afin de pouvoir procéder à la transaction avec un niveau de risque acceptable. Par exemple, on va requérir plus ou moins d'information selon que l'on se propose de réaliser une transaction avec un inconnu ou avec une personne que l'on connaît de longue date. De la même façon, plus la transaction envisagée comporte des enjeux importants, plus on voudra disposer d'informations afin de s'assurer de l'identité du cocontractant. Inversement, pour les transactions à enjeu mineur ou dérisoire ou encore lorsque l'identité du cocontractant n'a pas d'importance, on ne va pas rechercher les informations relatives à l'identification du cocontractant. Dans ce dernier cas, l'analyse que l'on fait des risques de la transaction porte à conclure qu'il ne faut qu'un minimum d'informations.

Pour effectuer ces évaluations 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. Ces rappels montrent bien que l'identification est une activité visant essentiellement à réduire ou gérer les risques inhérents à une transaction. Mais cela met également en lumière le fait que l'identification se présente sous plusieurs facettes puisque les transactions auxquelles nous prenons part ne sont pas toutes de même importance.

Aux termes de la *Loi concernant le cadre juridique des technologies de l'information*, 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[50].

La loi 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[51]. Des protections de l'intégrité et de la vie privée de la personne entourent les modes d'identification et de localisation. Il est interdit

50. *Loi concernant le cadre juridique des technologies de l'information*, art. 41.
51. *Ibid.*, art. 42.

d'exiger que l'identité d'une personne soit 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[52].

6- Le lien entre une personne et un document

La loi ne précise pas les moyens ou procédés pour établir un lien entre personnes et documents. 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.

Ainsi, pour ajuster le cadre juridique aux caractéristiques des documents établis en faisant usage de technologies de l'information, la loi québécoise 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. L'article 38 traite des qualités que doivent posséder les moyens utilisés pour associer une personne avec un document. Il se lit comme suit :

> **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 :
>
> 1º 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 ;
>
> 2º d'identifier le document et, au besoin, sa provenance et sa destination à un moment déterminé.

La loi québécoise, pas plus que la loi uniforme, 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

52. *Ibid.*, art. 43.

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.

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[53]. La signature est l'un des moyens pour établir le lien entre une personne et un document.

A. La signature

L'article 2827 du Code civil du Québec définit ainsi la signature :

> La signature consiste dans l'apposition qu'une personne fait sur 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 notion de signature électronique apparaît au premier abord comme une métaphore pour désigner les mécanismes par lesquels les parties à une transaction réalisée par le truchement des moyens de communication électronique vont marquer leur consentement ou authentifier un acte ou une transaction.

L'article 39 de la *Loi concernant le cadre juridique des technologies de l'information* précise que :

> **39.** Quel que soit le support du document, la signature d'une personne peut servir à l'établissement d'un lien entre elle et un document. La signature peut être apposée au document au moyen de tout procédé qui permet de satisfaire aux exigences de l'article 2827 du Code civil.

53. *Ibid.*, art. 40.

> La signature d'une personne apposée à un document technologique lui est opposable lorsqu'il s'agit d'un document dont l'intégrité est assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est maintenu.

Cette disposition vient supprimer les doutes qui pouvaient subsister quant à la possibilité d'utiliser une signature afin d'établir un lien entre une personne et un document technologique.

Le principe de l'article 39 est complété par l'article 75, une disposition interprétative qui vient confirmer le principe du libre choix des moyens pour apposer une signature sur un document :

> **75.** Lorsque la loi prévoit qu'une signature peut être gravée ou imprimée ou apposée au moyen d'un fac-similé gravé, imprimé ou lithographié ou qu'une marque peut l'être au moyen d'une griffe, d'un appareil ou d'un procédé mécanique ou automatique, elle doit être interprétée comme permettant, sur support papier, d'apposer la signature autrement que de façon manuscrite ou de faire apposer la marque personnelle par quelqu'un d'autre. Une telle disposition n'empêche pas de recourir à un autre mode de signature approprié à un document, lorsque ce dernier n'est pas sur support papier.

Ce qui importe, c'est que la signature constitue une marque personnelle et soit utilisée de façon courante pour manifester le consentement de la personne. C'est une conception large de la signature mettant l'accent sur ce que celle-ci accomplit plutôt que les mécanismes techniques par lesquels elle est obtenue. Cette notion de signature, incluant la signature électronique par équivalence, est englobante et neutre technologiquement.

B. 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 »[54]. 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, *i.e.* à établir ou à confirmer un fait.

---

54. Paul ROBERT, *Le nouveau Petit Robert : dictionnaire alphabétique et analogique de la langue française*, Paris, Dictionnaire Le Robert, 1993.

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[55].

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 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.

La *Loi concernant le cadre juridique des technologies de l'information* organise le cadre juridique de l'activité des prestataires de services de certification et dans cette veine, elle prévoît un régime de responsabilité spécifique pour les parties impliquées à un certificat.

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[56]. 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.

---

55. Pierre TRUDEL et Serge PARISIEN, *L'identification et la certification dans le commerce électronique*, Montréal, Éditions Yvon Blais, 1996, 270 p.
56. *Loi concernant le cadre juridique des technologies de l'information*, art. 57.

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[57]. 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 (voir art. 50). En effet, un certificat peut être annulé ou suspendu pour des raisons confidentielles ou pouvant porter atteinte à la réputation de la personne.

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[58].

Ces exigences viennent compléter les principes énoncés dans la législation québécoise sur la protection des renseignements personnels. 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.

Le recours à des autorités de certification, ou tiers certificateurs ou tiers de confiance vise à renforcer la fiabilité et la sécurité des mécanismes de signature basés sur la cryptographie à clé publique. L'UIT-T définit la notion d'autorité de certification comme étant une « autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat »[59].

La notion d'autorité de certification ne se comprend que dans le cadre d'une architecture à clé publique ou, autrement dit, de signature numérique. Dans une telle architecture, l'utilisation de la clé publique permet de vérifier une signature numérique réalisée à l'aide de la clé privée correspondante. Néanmoins, il importe de s'assurer que ces clés correspondent bel et bien à l'identité avérée du signataire. Il est en effet possible d'imaginer qu'une personne utilise une paire de clés asymétriques en présentant frauduleuse-

57. *Ibid.*, art. 47.
58. *Ibid.*, art. 52.
59. UIT-T, *Recommandation X.509, Annuaire – Cadre d'authentification*, Fasc. VIII.8, 1988, art. 3.3c).

ment celles-ci comme correspondant à l'identité d'un tiers ou d'une personne fictive. L'utilisation de certificats, émis par une autorité de certification, permet de pallier cette difficulté.

Les articles 61 et 62 de la *Loi concernant le cadre juridique des technologies de l'information* organisent la responsabilité du prestataire de services de certification et de répertoire ainsi que la responsabilité du titulaire visé par le certificat et la personne qui agit en se fondant sur le certificat.

L'article 61 prévoit que chacune des personnes parties à un certificat a une obligation de moyens. En conséquence, elles doivent prendre les moyens raisonnables pour satisfaire aux obligations que leur impose la loi. Leur obligation de moyens signifie qu'il leur faut prendre toutes les mesures qu'une personne raisonnable aurait prises dans des circonstances analogues. Par conséquent, elles doivent se conduire en conformité avec la loi ainsi que les usages professionnels reconnus relatifs à l'activité de certification.

L'article 62 précise et répartit 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.

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[60]. 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.

60. Art. 1518 C.c.Q.

Si aucune faute ne peut être reprochée à l'une ou l'autre des personnes impliquées, la responsabilité pour la réparation du préjudice est alors assumée à parts égales. 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.

En d'autres termes :

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. Un contrat qui stipulerait des règles de responsabilités différentes de celles prévues par la Loi serait sans effet.

CONCLUSION

Dans l'univers numérique, les lois identifient les qualités que doivent posséder les artefacts utilisés pour réaliser les actes juridiques. Elles s'inscrivent dans le contexte d'un dialogue entre les techniques et les fins recherchées par le droit. Les principes juridiques s'expriment donc de façon passablement différente dans un univers marqué par la vélocité des changements au plan des technologies de l'information.

L'information en tant qu'objet de droits et de devoirs se trouve encadrée au moyen de principes généraux et de standards énoncés dans des lieux qui fonctionnent en réseaux. Le sens des principes juridiques ne peut plus toujours être trouvé uniquement dans une lecture formaliste et positiviste de la loi envisagée de manière étroite : des normativités techniques imposent leurs logiques qui doivent être prises en compte par le juriste qui doit assurer la conformité au droit d'un ensemble informationnel.

Les normativités découlant de la loi et des autres sources de normes sont ainsi relayées jusqu'aux acteurs qui les explicitent et les appliquent de façon à gérer les risques associés à leurs activités. C'est manifestement ce qui explique le procédé retenu par le législateur québécois dans la *Loi concernant le cadre juridique des technologies de l'information*.

Pour appréhender les défis découlant de la généralisation des technologies de l'information, les juristes ont le choix. Soit qu'ils se donnent des outils cohérents capables de prendre en compte les environnements techniques à évolution accélérée, soit qu'ils se cantonnent dans des concepts hérités des époques antérieures et multiplient les incantations proclamant que rien ne change ! Dans cette dernière hypothèse, le risque est considérable que les normativités encadrant les technologies de l'information se pensent et s'appliquent suivant des logiques tendant à exclure de plus en plus les valeurs que le droit a vocation à garantir.