

Afin d'y voir clair

Guide relatif à la gestion des documents technologiques

REMERCIEMENTS

Ce guide relatif à la gestion des documents technologiques évoque un droit récent sur un sujet, les technologies de l'information, qui paraît encore nébuleux pour beaucoup d'utilisateurs. Pour ces raisons, le soutien apporté par plusieurs intervenants a grandement contribué à rendre ces quelques pages plus justes et plus accessibles. Aussi, je tiens à remercier chaleureusement M^e Claire Morency (directrice générale, Fondation du Barreau du Québec) et M^e Guy Lefebvre (vice-doyen au développement et à la planification, Faculté de droit de l'Université de Montréal) pour leurs précieux conseils à toutes les étapes de la rédaction de ce guide. De la même manière, j'adresse mes plus sincères remerciements aux différentes personnes qui ont judicieusement commenté le présent guide, à savoir : Claudette Archambault (Sogique); Ugo Bellavance (étudiant, maîtrise en commerce électronique); Diane Campeau (Sogique); Mario Dallaire (Abitibi Consolidated); M^e Daniel Lafortune (Lafortune Leduc, Avocats); Christian Lavoie (Barreau du Québec); M^e Ghislain Massé (Faculté de droit de l'Université de Montréal); Daniel Poulin (Faculté de droit de l'Université de Montréal). Enfin, je remercie M^e Christian Saint-Georges (responsable de l'édition, Éditions Thémis) pour ses corrections éditoriales apportées à la version finale.

Électroniquement vôtre,

Vincent Gautrais
Avocat et professeur

Faculté de droit
Université de Montréal



TABLE DES MATIÈRES

4	1.0 Une évolution, une loi... un guide
5	1.1 Les technologies de l'information
5	1.2 La Loi concernant le cadre juridique des technologies de l'information
6	1.3 L'utilisation du présent guide
7	2.0 Les principes directeurs de la Loi
8	2.1 L'équivalence fonctionnelle
8	2.2 La neutralité technologique
9	2.3 L'intégrité
10	3.0 La gestion sécuritaire des documents technologiques
13	3.1 Comment transférer un document technologique d'un support à un autre
14	3.2 Comment conserver un document technologique
15	3.3 Comment s'assurer de rendre un document technologique accessible en tout temps
16	3.4 Comment s'assurer que la transmission d'un document technologique s'effectue en conformité avec la Loi
17	4.0 L'utilisation des documents technologiques en preuve
18	4.1 Un document technologique peut-il être présenté devant un juge?
19	4.2 Un document technologique peut-il valoir un « écrit »?
20	4.3 Une « signature » électronique est-elle légale?
22	4.4 Un document technologique peut-il être un « original »?
23	4.5 Un « contrat » électronique est-il légal?
24	5.0 Les responsabilités associées aux documents technologiques
25	5.1 Qui est responsable des documents technologiques en général?
25	5.2 Qui est responsable des documents technologiques confidentiels?
27	5.3 Quelles sont les responsabilités d'une entreprise de services en technologies de l'information?
31	6.0 Le cadre d'une entente de sécurité
32	Une entente de sécurité
36	Lexique
37	Références



Une évolution, une loi... **un guide**

La *Loi concernant le cadre juridique des technologies de l'information*¹ (L.R.Q., chapitre C-1.1) constitue la nouvelle référence législative au Québec qui encadre les documents utilisés dans ce que l'on appelle communément le commerce électronique. Ce texte majeur a été mis en œuvre pour tenir compte des bouleversements occasionnés par le passage du papier aux technologies de l'information et précise comment utiliser des documents technologiques de façon sécuritaire et légale.

La Loi s'applique à l'ensemble des technologies de l'information, actuelles et futures, telles que Internet, EDI, intranet, etc.

¹Dans le présent Guide, la *Loi concernant le cadre juridique des technologies de l'information* sera citée « Loi », avec une majuscule.

1.1 LES TECHNOLOGIES DE L'INFORMATION

Si le papier est depuis longtemps l'outil traditionnel pour communiquer et plus particulièrement pour commercer, et qu'après des siècles d'une tradition bien établie, les usagers savent désormais comment gérer de tels documents, il n'en est pas de même pour ces nouveaux supports. Les technologies de l'information quelles qu'elles soient, entraînent des changements en profondeur; aussi, il importe qu'elles permettent une même ou une meilleure facilité d'utilisation tout en instaurant une sécurité comparable.

Loin de nous l'idée de prétendre que les technologies de l'information ne permettent pas de transposer les avantages du papier! Nous le verrons, plusieurs solutions, technologiques, organisationnelles ou juridiques, assurent une qualité équivalente et souvent supérieure à un document papier. Il faut néanmoins souligner qu'un courriel, par exemple, qui ne dispose pas d'une protection particulière, présente les inconvénients suivants :

- il n'y a aucune assurance qu'il s'agit bien du détenteur de l'adresse de courriel qui l'a envoyé (identité de l'expéditeur);
- il n'y a aucune assurance qu'il s'agit bien du destinataire qui l'a reçu (identité du destinataire);
- il est facile de modifier le contenu d'un courriel (intégrité du document);
- il est parfois difficile de s'assurer que le document n'a pas été consulté par une personne non autorisée (confidentialité du document);
- il s'avère aisé pour l'expéditeur de prétendre plus tard ne jamais avoir envoyé un tel document (irrévocabilité de l'auteur).

Le courriel ordinaire présente des inconvénients de sécurité flagrants lorsqu'on le compare au support papier. Il peut donc être important, en certaines circonstances, de remédier à cette situation par des apports technologiques et organisationnels pour le sécuriser.

1.2 LA LOI CONCERNANT LE CADRE JURIDIQUE DES TECHNOLOGIES DE L'INFORMATION

La Loi est donc intervenue pour gérer cette nouvelle réalité. Ainsi, le gouvernement du Québec a voté, en 2001, comme partout ailleurs au Canada et dans la plupart des pays du monde, une loi spécifique relative aux documents technologiques. Ce texte poursuit trois objectifs fondamentaux :

Supprimer les barrières juridiques qui existaient dans certains textes législatifs ou réglementaires

Certaines lois font expressément référence à un écrit, à une signature, à un original, à un document papier ou plus indirectement à des circonstances sous-entendant le support papier. La convention d'assurance qui est constatée par écrit en est un bel exemple. Il fallait donc éviter que l'utilisation des technologies de l'information soit illégale par le seul fait d'une pareille disposition.

Préciser certains principes généraux afin d'assurer une gestion sécuritaire des documents technologiques

Bien que toutes les lois doivent être générales et impersonnelles, elles n'en encadrent pas moins des situations fort diversifiées. C'est ainsi que la sécurité d'une grande entreprise détenant des informations sensibles ne peut être comparable à celle nécessaire à une PME. Par conséquent, il importait de trouver des critères et des conditions qui puissent aider l'ensemble des acteurs impliqués à assurer la sécurité de leurs documents technologiques.

S'assurer que les technologies de l'information soient utilisées en respectant les principes fondamentaux attachés aux droits des personnes

La gestion de documents, quel qu'en soit le support, demande un traitement diligent étant donné, notamment, le caractère confidentiel de certaines informations. Par exemple, le détenteur de documents contenant des renseignements personnels sur un individu ne peut les traiter à la légère. Pour ces mêmes raisons, l'usage de certaines technologies comme la biométrie est soumise à un contrôle rigoureux de la Loi.

1.3 L'UTILISATION DU PRÉSENT GUIDE

À qui s'adresse-t-il?

Dans la mesure où tous les acteurs sociaux ou économiques sont susceptibles d'utiliser des documents technologiques, ils sont tous concernés par cette Loi, et ce, qu'il s'agisse de particuliers, de compagnies ou d'institutions publiques.

Toutefois, la Loi édicte des devoirs et des obligations qui peuvent varier selon la catégorie à laquelle on fait référence. Ainsi, le particulier, qu'il soit consommateur ou simple citoyen, n'a pas les mêmes responsabilités qu'une institution privée ou publique.

Étant donné l'importance de cerner l'impact des technologies de l'information dans la vie courante des affaires, le guide s'adresse donc en particulier :

- à la personne assignée à la gestion des documents technologiques d'une entreprise;
- aux informaticiens responsables d'un site Internet;
- aux dirigeants de PME;
- aux avocats;
- aux notaires; ou
- aux particuliers soucieux d'une gestion diligente des documents technologiques qu'ils utilisent.

Aussi, afin de compléter la compréhension de ce guide, la lecture de la Loi est fortement conseillée.

À quoi sert-il?

La Loi identifie certains critères permettant une gestion adéquate des documents technologiques. Le présent guide entend proposer des solutions concrètes qui permettent d'y répondre. Il faut toutefois noter que ces solutions technologiques ne sont proposées qu'à titre indicatif. En conséquence, elles ne sont ni uniques ni forcément adaptées à toutes les situations, car si la Loi propose des critères légaux, elle ne dit pas comment, concrètement, ces derniers pourront être remplis.

L'analyse qui suit vise donc à se faire l'écho de la Loi, d'une part, en identifiant l'importance d'une meilleure prise de conscience des avantages d'une bonne gestion documentaire et, d'autre part, en faisant mieux connaître les conditions légales qui y sont rattachées pour y parvenir.

Particuliers

Compagnies

Institutions
publiques



Les **principes** **directeurs** de la Loi



La Loi est souvent perçue par les analystes comme un texte technique avec des concepts nouveaux que l'on ne retrouve pas dans d'autres lois. Si un lexique propose des définitions à la fin de ce guide, il importe dès maintenant de clarifier les trois principes fondamentaux.

2.1 L'ÉQUIVALENCE FONCTIONNELLE

2.1

Définition Approche selon laquelle des exigences que l'on retrouve dans certaines lois telles que l'écrit, la signature ou l'original, puissent aussi être appliquées à un support technologique dans la mesure où ces exigences remplissent les mêmes fonctions que l'équivalent papier.

- Exemples**
- Écrit : un écrit est légal dès lors qu'il est intègre, et ce, quel que soit son support (voir paragraphe 4.2).
 - Signature : une signature peut légalement être utilisée sur papier ou avec une technologie de l'information dès lors qu'elle permet : 1) d'identifier une personne et 2) de manifester un consentement (voir paragraphe 4.3).
 - Original : un original remplit selon les cas trois fonctions fondamentales : être la source première d'un document; être un document unique; être la source première d'un document relié à une personne (voir paragraphe 4.4).

2.2 LA NEUTRALITÉ TECHNOLOGIQUE

2.2

Définition Caractéristique d'une loi qui ne favorise pas un moyen de communication (papier ou technologie de l'information) plutôt qu'un autre. Ainsi, dans une telle éventualité, le tribunal ne peut refuser de reconnaître un document du seul fait qu'il est sur support technologique.

- Exemples**
- Une vente de marchandises entre deux entreprises peut être conclue par un ou plusieurs documents technologiques. En cas de litige, l'une des parties pourrait valablement présenter ce ou ces documents dès lors qu'ils remplissent les conditions nécessaires. Le seul fait qu'il soit sur papier ou sur support électronique n'est pas un élément déterminant.
 - Toutefois, la Loi prévoit que certains contrats, comme une vente d'automobile à un consommateur ou un contrat de prêt à la consommation, requièrent le support papier. Pour ces contrats, la Loi n'est donc pas neutre sur le plan technologique.

*Sauf disposition contraire de la loi,
et sous réserve du respect des conditions
nécessaires, un document peut utiliser n'importe quel
support, technologique ou papier.*

2.3 L'INTÉGRITÉ

Définition Critère fondamental de la Loi assurant qu'un document, quel que soit son support, a une valeur juridique pleine et entière dès lors que son intégrité peut être constatée. Est intègre le document qui n'a pas été altéré, modifié.

Exemples Si cette caractéristique est difficile à prouver pour un courriel non protégé, il existe des solutions pour assurer l'intégrité d'un document technologique :

- des outils cryptographiques comme MD5 permettent de générer l'empreinte numérique d'un document. Le responsable peut ainsi les conserver en protégeant son intégrité, car toute modification montrerait la discordance entre le document et son empreinte;
- une infrastructure à clé publique permet d'assurer l'intégrité du document lors de son transport et de son stockage;
- l'outil PGP (ou autre outil de sécurité) peut être préconisé pour des organisations plus petites;
- un système de « notarisation » où, par exemple, un tiers archiveur conserve des documents pour assurer leur intégrité (voir paragraphe 5.3);
- un support qui n'est pas technologique, comme le papier, ce dernier présentant des qualités d'intégrité globalement meilleures qu'un support électronique non protégé et qu'il est également possible en certaines circonstances d'utiliser;
- l'utilisation de certains cédéroms peut aussi être une solution envisageable.

2.3



La **gestion sécuritaire** des documents technologiques

La sécurité est souvent considérée comme le premier obstacle à l'utilisation des technologies de l'information et l'on constate une grande diversité dans les façons de faire au sein de l'industrie. Par exemple, l'industrie bancaire a, depuis plusieurs décennies déjà, intégré une série de procédures sécuritaires très élaborées. Toutefois, cette diligence ne s'impose pas dans d'autres domaines moins à risque. Par ailleurs, cette sécurité doit être assurée tout au long du cycle de vie du document technologique, notamment lors des quatre opérations spécialement encadrées dans la Loi, soit : **le transfert** (3.1); **la conservation** (3.2); **la consultation** (3.3); **la transmission** (3.4).

La sécurité n'est pas la même dans toutes les circonstances. Elle s'apprécie au regard des risques. L'évaluation de ces considérations constitue l'étape préalable au choix des moyens à prendre.

Quatre opérations spécialement encadrées dans la Loi

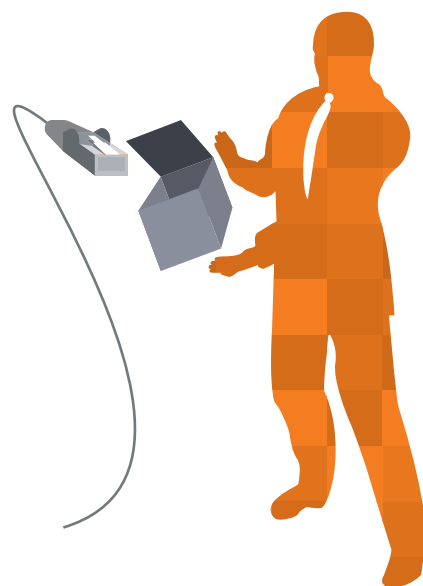


01 Transfert

- Faire passer un document technologique d'un support à un autre.
Le document sur le nouveau support a la même valeur juridique que l'ancien et le document sur l'ancien support peut par la suite être détruit.

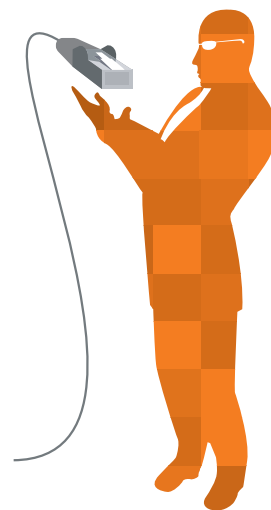
02 Conservation

- Remiser des documents d'une façon telle que l'on puisse les retrouver ultérieurement, sur demande, et sans qu'ils n'aient été altérés.
Pour des raisons fiscales, administratives ou légales, la plupart des entreprises ont une obligation de conserver certains documents.



03 Consultation

- Rendre disponible à des personnes habilitées un document présenté dans une forme intelligible.



04 Transmission

- Transmettre un document d'une personne à une autre en faisant appel aux technologies de l'information, sauf interdiction d'une loi ou d'un règlement.



3.1 COMMENT TRANSFÉRER UN DOCUMENT TECHNOLOGIQUE D'UN SUPPORT À UN AUTRE

Définition Faire passer un document technologique d'un support à un autre. Le document sur le nouveau support a la même valeur juridique que l'ancien et le document sur l'ancien support peut par la suite être détruit.

3.1

Exemple Une entreprise numérise des masses de documents papier, pour des raisons de coûts d'archivage ou pour faciliter les recherches, et les transfère ensuite sur un cédérom.

Conditions légales

- Documenter préalablement la façon dont le transfert va se réaliser. Une entreprise doit prévoir sa façon de faire en rédigeant une entente de sécurité (aussi dénommée politique, procédure, mesure, code de sécurité) explicitant comment elle va s'y prendre. Elle doit notamment préciser :
 - le format d'origine;
 - les garanties offertes par la solution choisie;
 - le procédé technologique utilisé.

- Préserver l'intégrité des documents transférés.

N.B. Le particulier n'est en revanche pas visé par ces obligations.

Solutions

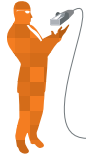
- Désigner une personne assignée au sein de l'organisation ou sous-traiter à un service d'intermédiaire.
- Effectuer cette opération de façon systématique pour tous les documents.
- Joindre la documentation lorsque vient le temps de prouver le document transféré.



3.2 COMMENT CONSERVER UN DOCUMENT TECHNOLOGIQUE

- Définition** Remiser des documents d'une façon telle que l'on puisse les retrouver ultérieurement, sur demande, et sans qu'ils n'aient été altérés. Pour des raisons fiscales, administratives ou légales, la plupart des entreprises ont une obligation de conserver certains documents.
- Exemples**
- Un particulier qui achète un produit en ligne peut avoir intérêt à garder une trace d'un accusé de réception qui lui a été envoyé par le commerçant après que le paiement ait été transmis et avant que ce produit ne soit en sa possession.
 - À des fins comptables, une entreprise peut avoir à conserver certains documents jusqu'à 10 ans.
- Conditions légales**
- Désigner une personne assignée, au sein de l'organisation, pour les questions de sécurité ou sous-traiter à un service d'intermédiaire.
 - S'assurer que les documents conservés soient :
 - intègres; et
 - disponibles pendant toute la durée de conservation (ce qui comprend les logiciels nécessaires à la lecture du document).
 - S'assurer que la personne assignée qui modifie un document conservé, et donc remet en cause sciemment son intégrité, indique dans le document lui-même ou dans un autre qui y est associé :
 - qui a fait la demande de modification;
 - qui a effectué la modification du document;
 - quand la modification a été faite;
 - pourquoi elle a été faite.
- Solutions**
- Mettre en place une structure organisationnelle où une personne assignée va statuer préalablement sur la façon de procéder. Ceci pourra notamment passer par la rédaction d'une entente de sécurité.
 - Choisir parmi les solutions préalablement identifiées pour satisfaire au critère de l'intégrité.
 - Utiliser les services d'un tiers archiveur.

3.2



3.3 COMMENT S'ASSURER DE RENDRE UN DOCUMENT TECHNOLOGIQUE ACCESSIBLE EN TOUT TEMPS

Définition Rendre disponible à des personnes habilitées un document présenté dans une forme intelligible.

- Exemples**
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* oblige les instances publiques à rendre accessibles aux citoyens les renseignements personnels qu'elles détiennent sur eux.
 - La *Loi sur la protection des renseignements personnels dans le secteur privé* oblige les entreprises à rendre accessibles aux usagers des documents contenant des renseignements personnels les concernant.
 - La *Loi sur les valeurs mobilières* oblige parfois les personnes morales à transmettre aux investisseurs certains documents relatifs à leur entreprise tels que des états financiers ou des communiqués de presse.

- Conditions légales**
- S'assurer que les documents sont intelligibles et lisibles.
 - Sauf exception, laisser à la personne qui dispose du droit d'accès, la liberté de choisir entre un document papier ou un document utilisant une technologie de l'information.
 - Organiser un accès particulier lorsque les documents qui doivent être rendus accessibles contiennent des renseignements personnels ou confidentiels, par essence plus sensibles, à savoir :
 - limiter l'accès aux seuls documents autorisés et interdire l'accès aux autres;
 - identifier une personne assignée;
 - faire en sorte qu'il soit impossible de faire de la recherche extensive, c'est-à-dire qu'il ne soit pas permis, par exemple, de vérifier dans une banque de données de décisions judiciaires les noms des parties;
 - mettre en place un encadrement sécuritaire suffisant;
 - s'assurer que les conditions qui s'appliquent pour les documents contenant des renseignements personnels soient respectées (voir paragraphe 5.2).

- Solutions**
- Empêcher qu'une personne qui est habilitée à consulter seulement certaines informations ne puisse en consulter d'autres.
 - Mettre en place un coupe-feu, un système de détection, un système d'authentification, une revue des journaux (log), etc. qui permettent de contrôler l'accès non autorisé.
 - Rédiger une entente de sécurité (voir chapitre 6.0) qui précise l'ensemble de ces solutions.



3.4 COMMENT S'ASSURER QUE LA TRANSMISSION D'UN DOCUMENT TECHNOLOGIQUE S'EFFECTUE EN CONFORMITÉ AVEC LA LOI

- Définition** Transmettre un document d'une personne à une autre en faisant appel aux technologies de l'information, sauf interdiction d'une loi ou d'un règlement.
- Exemples**
- Le courriel est un moyen usuel pour transmettre une pièce jointe.
 - L'industrie transmet très souvent des documents électroniques : échanges de documents informatisés, transferts électroniques de fonds, etc.
- Conditions légales**
- Pour que le document expédié ait la même valeur que celui qui a été reçu, s'assurer :
 - de l'intégrité des deux documents; et
 - de documenter la façon de faire pour parvenir à cette fin.
 - Présumer qu'un document technologique est transmis lorsque l'expéditeur n'a plus le contrôle de celui-ci. Pour plus d'assurance, un bordereau d'envoi peut être généré par le système de l'expéditeur.
 - Présumer qu'un document technologique est reçu lorsqu'il est accessible au destinataire. Pour plus d'assurance, un accusé de réception peut être généré par le système du destinataire.
 - S'assurer qu'un document qui contient des informations confidentielles :
 - soit transmis par un moyen jugé approprié; et
 - que la transmission soit documentée.
- Solutions**
- Utiliser une infrastructure à clé publique qui va notamment assurer :
 - l'intégrité du document;
 - l'authentification de l'expéditeur et du destinataire;
 - la confidentialité de l'information;
 - l'irrévocabilité de l'expéditeur qui ne peut dire que ce n'est pas lui qui a envoyé le document.
- Ces critères seront plus ou moins assurés selon la qualité de l'ICP.
- Utiliser PGP.

3.4



L'utilisation des documents technologiques en **preuve**

Sécurité et preuve sont les deux côtés d'une même médaille. Plus un document technologique est géré de façon sécuritaire et plus sa recevabilité en preuve sera grande. En effet, en cas de litige, il y a fort à parier qu'un juge ou un arbitre qui doit apprécier la preuve présentée par les parties, donnera priorité à celle qui a été établie avec le plus de diligence. Ainsi, il importe dans ce chapitre de regarder comment les nouvelles dispositions de la Loi s'intègrent dans les façons habituelles de faire du droit de la preuve.

De plus, il faut tenir compte du fait que les lois évoquent souvent des conditions particulières pour qu'un document puisse être présenté devant un juge. Ainsi,

1. certains contrats ne peuvent se faire que par écrit (comme des licences de droit d'auteur, contrats d'un certain montant, clauses d'arbitrage, etc.);
2. certains documents doivent être signés; et
3. certaines opérations exigent des originaux.

Il est donc important de savoir comment ces conditions peuvent être respectées dans un environnement technologique.

4.1 UN DOCUMENT TECHNOLOGIQUE PEUT-IL ÊTRE PRÉSENTÉ DEVANT UN JUGE?

Principe Un document technologique ne peut être refusé par un juge au seul motif qu'il est technologique. Il peut donc constituer un élément de preuve recevable au même titre qu'un document papier.

- Exemples**
- Une entreprise peut conclure des contrats par courriel. Néanmoins, il faudra parfois lui conseiller qu'elle y joigne des procédés technologiques adéquats pour rendre ce document plus sécuritaire.
 - Un enregistrement sur une « webcam » ou une photographie numérique peuvent aussi être recevables en preuve.

- Conditions légales**
- S'assurer que le document soit intègre. L'intégrité s'apprécie au regard des circonstances et de la sensibilité des informations contenues dans le document. Relativement à ce critère d'intégrité, la Loi précise que :
 - il n'est pas obligatoire de prouver que l'environnement du document est convenable; la preuve de l'intégrité du document suffit;
 - le document provenant d'une entreprise ou de l'État est présumé intègre. Ainsi, par exemple, un consommateur pourra présenter en preuve une impression papier ou une disquette d'un courriel d'une entreprise et ce document sera présumé intègre. À charge pour l'entreprise d'éventuellement prouver le contraire.
 - S'assurer, lorsque le document n'est pas signé, de l'identité de l'auteur du document.

- Solutions**
- Le logiciel Adobe par exemple génère des documents « pdf » standards qui peuvent, lorsque les enjeux et les risques sont faibles, être un type d'outil suffisant. Attention : il est néanmoins possible de modifier un pareil document.
 - Plusieurs produits logiciels, utilisant des technologies diverses, offrent des solutions pour assurer le respect de l'intégrité.
 - Voir également les solutions proposées lors de l'analyse du critère d'intégrité au paragraphe 2.3.

Un document technologique est soumis à l'appréciation du juge. Ainsi, plus celui qui présente un tel document aura agi avec diligence pour le gérer, plus le juge sera enclin à le considérer comme étant admissible et probant.

4.2 UN DOCUMENT TECHNOLOGIQUE PEUT-IL VALOIR UN « ÉCRIT »?

Principe	Compte tenu du principe de l'équivalence fonctionnelle (voir paragraphe 2.1), la Loi permet l'écrit électronique, ce dernier pouvant être réalisé sur n'importe quel support, papier ou technologique.
Exemples	<ul style="list-style-type: none">■ De nombreux documents doivent être rédigés par écrit. C'est le cas notamment pour :<ul style="list-style-type: none">- un testament;- un contrat d'assurance.■ Attention : certains contrats de consommation qui exigent également un écrit, comme un contrat de vente d'automobile ou un contrat de prêt à la consommation, ne peuvent pas être rédigés sur un support faisant appel aux technologies de l'information, car la Loi prévoit expressément que cela ne peut se faire que sur papier.
Conditions légales	<ul style="list-style-type: none">■ S'assurer que le document soit intègre.■ Plus généralement, déterminer de qui le document provient, quelle est son origine.
Solutions	<ul style="list-style-type: none">■ Voir les solutions visant à assurer l'intégrité d'un document au précédent paragraphe 4.1.

4.2

Un écrit n'est plus nécessairement synonyme de « papier ». Un écrit électronique est donc possible dès lors qu'il remplit les mêmes fonctions que le papier.

4.3 UNE « SIGNATURE » ÉLECTRONIQUE EST-ELLE LÉGALE ?

Définition Un outil représentant une marque personnelle qui est utilisée de façon courante par une personne pour manifester un consentement. La définition de la signature n'est pas attachée à un support en particulier (papier ou technologie de l'information).

Exemple

- Plusieurs documents ne sont valides que s'ils sont signés, notamment :
 - le testament;
 - le mandat;
 - certains contrats.

Conditions légales

- Permettre d'identifier une personne.
- Permettre à cette personne de manifester son approbation, son engagement, son consentement.
- Utiliser un degré de fiabilité de la signature qui corresponde aux enjeux, aux circonstances, aux habitudes ou à la confiance entre les parties.


Conditions légales et propres à la biométrie La Loi exige un encadrement très strict concernant l'identification d'une personne par l'entremise de certaines caractéristiques physiques telles que l'empreinte digitale, la rétine de l'œil, l'ADN ou encore la reconnaissance vocale.

- Gérer avec attention les données biométriques au cours de leur utilisation et plus particulièrement :
 - protéger les données biométriques de l'interception et plus généralement de l'usurpation d'identité;
 - préserver l'intégrité de ces données biométriques;
 - journaliser les utilisations des données biométriques;
 - détruire les données biométriques lorsque l'utilisation est terminée.
- Demander, préalablement à l'utilisation de données biométriques, le consentement manifeste de la personne en cause. Sauf avis contraire de la loi, nul n'est tenu d'utiliser un tel outil.
- Déclarer auprès de la Commission d'accès à l'information le fait d'utiliser des données biométriques. Cet organisme dispose d'un droit de contrôle sur ces dernières.

Solutions

- Une signature peut donc être valide en inscrivant simplement son nom à la fin d'un courriel. Le procédé n'est en revanche pas très fiable, car il est facile de signer pour autrui en faisant passer un courriel comme provenant de quelqu'un d'autre.
- La biométrie et les certificats électroniques sont souvent considérés comme des outils technologiques qui permettent d'identifier une personne avec assurance.
- Plus commun, un « clic » (fait de cliquer sur une icône « j'accepte ») peut aisément être considéré comme un mode de signature valide. La condition d'identification est davantage respectée si le signataire appose un identifiant comme un mot de passe, un numéro d'identification personnel (NIP), voire un numéro de carte de crédit.
- Une infrastructure à clé publique est un procédé qui peut évidemment convenir comme mode de signature dès lors que la manifestation de volonté n'est pas équivoque.

*Une signature peut évidemment se faire
avec un crayon mais aussi par
un « clic », un numéro
d'identification personnel ou son nom
en bas d'un courriel. Toutefois, dans tous
les cas, il faut s'assurer
de l'identité du signataire et que
l'action représente bien le
consentement de celui-ci.*



4.4 UN DOCUMENT TECHNOLOGIQUE PEUT-IL ÊTRE UN « ORIGINAL »?

Définition Un document physique correspondant à sa rédaction première qui est souvent utilisé pour prouver un acte ou un fait. Généralement associé au papier, la Loi établit des conditions légales pour que, lorsque certaines lois exigent un original, ce dernier puisse être satisfait par un document technologique.

L'original est susceptible de remplir trois fonctions.

- Conditions légales**
1. Pour que le document remplisse la première fonction de l'original, à savoir être la source première d'une copie, par exemple un contrat signé en deux copies, il faut :
 - Assurer l'intégrité du document.
 - Conserver le document.
 - Permettre de consulter le document ultérieurement.
 2. Pour que le document remplisse la deuxième fonction de l'original, à savoir être un document unique (par exemple un chèque, un connaissance maritime, un titre au porteur), il faut :
 - Assurer l'intégrité du document.
 - Intégrer une solution d'ordre technologique*.
 - Intégrer notamment une composante exclusive ou mettre en place un procédé empêchant toute forme de reproduction.
 3. Pour que le document remplisse la troisième fonction de l'original, à savoir être la source première d'un document relié à une personne (par exemple un testament, un certificat numérique), il faut :
 - Assurer l'intégrité du document.
 - En affirmer le caractère unique.
 - Identifier la personne à laquelle le document est relié*.
 - Maintenir ce lien pendant tout le cycle de vie du document.

Même s'il s'agit d'un concept traditionnellement associé à un document papier, un original technologique est possible. Il faut, en revanche, s'assurer que les fonctions qui lui sont normalement dévolues ont été respectées dans cet environnement.

* Pour les situations deux et trois, le législateur fait référence à des solutions technologiques devant être déterminées par une norme technique reconnue. Un tel standard pourrait par exemple provenir d'organismes internationaux comme l'ISO (Organisation internationale de normalisation) ou l'IETF (Internet Engineering Task Force). Certains organismes nationaux seraient également en mesure d'agir de la sorte tels que, par exemple, le CCN (Conseil canadien des normes) ou le BNQ (Bureau de normalisation du Québec).

4.5 UN « CONTRAT » ÉLECTRONIQUE EST-IL LÉGAL?

Principe Un contrat est un échange de volontés qui peut se conclure quel qu'en soit le support, dès lors que les parties ont manifesté leur consentement. Il est donc légal de contracter en utilisant toutes sortes de médias pour communiquer les deux éléments constitutifs d'une transaction, soit l'offre et l'acceptation.

Une signature peut être utilisée pour manifester un consentement mais un contrat peut être conclu autrement, dès lors que la manifestation de volonté est apparente.

Exemple Un contrat peut donc se conclure par l'échange de courriels, de télécopies, par téléphone, voire en remplissant un formulaire sur une page Internet.

Conditions légales

- Rédiger une offre claire et non équivoque.
- Organiser une acceptation en ligne où la personne qui s'engage manifeste clairement une volonté libre et éclairée. Par exemple :
 - au moyen d'un « clic » sur une icône « j'accepte »;
 - éventuellement, au moyen d'une mention sur le site qui explique que le seul fait de naviguer sur un site Internet constitue une acceptation des conditions qui suivent. Cette façon de faire paraît contestable.

Conditions légales propres au contrat automatisé

- Il est possible que des partenaires contractuels s'engagent mutuellement par l'entremise d'agents électroniques ou autres procédés technologiques. Ces outils peuvent avoir des degrés de sophistication divers :
 - par des logiciels évolués qui ont été programmés pour passer certains actes (comme l'EDI);
 - par des formulaires que l'on trouve sur un site Internet et qui donnent lieu à une acceptation par un bouton « j'accepte ».
- La Loi oblige la personne qui utilise un tel procédé, sous peine de nullité :
 - à permettre au partenaire de corriger les erreurs qui se seraient glissées;
 - à offrir des instructions claires sur la façon de procéder.

Par exemple, un accusé de réception pourrait satisfaire à ces conditions.

Un contrat peut se conclure oralement, sur papier ou électroniquement. Il suffit seulement qu'une offre soit acceptée.



Les responsabilités associées aux documents technologiques

Nous avons vu qu'il existe à plusieurs égards une obligation de gérer certains documents en respectant un degré donné de sécurité. Par conséquent, son manquement doit pouvoir être sanctionné et de nombreux exemples pourraient être présentés tels que :

- le « cybermarchand » qui laisse des tiers non autorisés accéder aux renseignements personnels de ses clients; ou encore
- la personne qui oublie de vérifier la validité du certificat numérique du partenaire avec lequel elle compte faire affaire.

5.1 QUI EST RESPONSABLE DES DOCUMENTS TECHNOLOGIQUES EN GÉNÉRAL?

5.1

Principe De manière générale, toute personne, qu'elle soit une entreprise, une institution publique ou un particulier, peut être tenue responsable des dommages causés à autrui du seul fait qu'elle détient des documents technologiques.

Exemple

- Une personne qui adresse un document technologique contenant un virus pourrait être tenue responsable du dommage causé si :
 - une faute est commise;
 - un dommage est causé;
 - un lien peut être établi entre la faute et le dommage.

Conditions légales Il n'existe pas d'obligation de sécurité de manière générale. En revanche, celui qui ne prend pas un soin particulier à gérer ses documents technologiques se verra dans l'incapacité de faire valoir ses droits par absence de preuve. La Loi précise des conditions impératives dans certains cas. C'est le cas, par exemple, lors de la gestion de documents technologiques confidentiels (voir paragraphe 5.2) et lors de la gestion d'un certificat numérique (voir paragraphe 5.3).

5.2 QUI EST RESPONSABLE DES DOCUMENTS TECHNOLOGIQUES CONFIDENTIELS?

5.2

Principe Un document confidentiel ne peut être accessible qu'aux personnes qui y sont autorisées. Les personnes qui détiennent ces documents ont l'obligation d'assurer un degré de sécurité adéquat.

Exemples

- L'entreprise qui détient des renseignements personnels sur ses clients tels que leur numéro de carte de crédit, doit se conformer à une obligation de sécurité.
- Les membres de la plupart des ordres professionnels comme les avocats, les médecins ou les architectes, doivent traiter certaines informations confidentiellement.

Conditions légales relatives à la protection des renseignements personnels

- Élaborer une politique de vie privée explicitant le traitement et la finalité des renseignements personnels.
- Détenir un intérêt sérieux et légitime pour constituer un dossier.
- Ne recueillir que les renseignements nécessaires à la finalité recherchée.
- Permettre aux individus, sauf exception, l'accès (voir paragraphe 3.3), la correction ou le retrait de leurs propres renseignements personnels.
- Interdire la transmission des renseignements personnels à autrui sauf consentement manifeste de l'intéressé.

Un renseignement personnel est une information qui permet d'identifier un individu. Ce peut être, par exemple : son nom, son adresse, un rapport médical, un historique bancaire, un numéro de carte de crédit.

Sauf consentement de l'intéressé, une entreprise ne peut utiliser le renseignement à une fin autre que celle qui a justifié la prise d'information. Pour sa part, un particulier a le droit de savoir quelle information l'entreprise ou l'institution publique détient sur lui.

Conditions légales relatives à la sécurité

- Mettre en place des mesures de sécurité qui soient proportionnelles et appropriées aux circonstances.
- Empêcher que le devoir d'accès à des documents technologiques puisse nuire à la confidentialité de certaines informations. Notamment face à des données publiques, il est possible de mettre en place un système de visibilité réduite qui interdirait de faire des recherches trop efficaces par mots-clés (voir paragraphe 3.3).
- S'assurer en cas de transmission de renseignements confidentiels :
 - que les partenaires qui les reçoivent disposent aussi d'un encadrement sécuritaire adéquat;
 - que l'opération est documentée.

Solutions

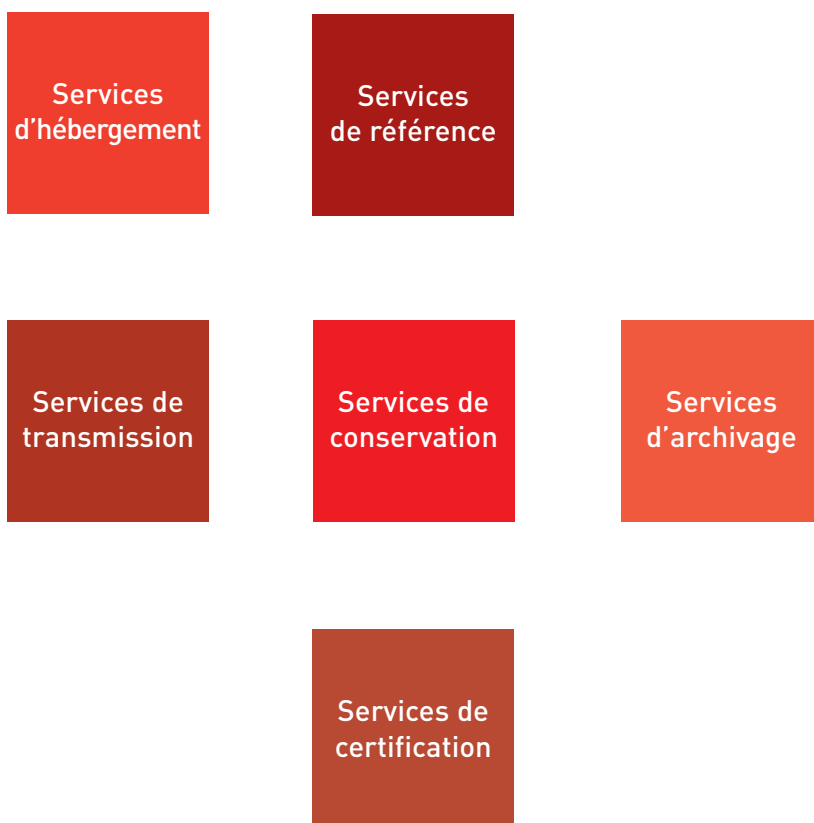
- Mettre en place une entente de sécurité pour expliciter les mesures de sécurité à prendre telles que :
 - la mise en place de moyens matériels, serrures ou portes fermées;
 - la mise en place de moyens organisationnels, contrôles d'accès ou d'identification de personnes assignées;
 - la mise en place de moyens technologiques comme le chiffrement ou des mots de passe;
 - l'information et la sensibilisation du personnel à l'importance de la confidentialité de ces documents.

5.2

5.3 QUELLES SONT LES RESPONSABILITÉS D'UNE ENTREPRISE DE SERVICES EN TECHNOLOGIES DE L'INFORMATION?

Malgré le fait que la Loi mette en place un régime général d'exonération au profit des intermédiaires, sauf exception, leur rôle se limitant à offrir un support technique, certains services qui font appel aux technologies de l'information sont soumis à des règles de responsabilité particulières.

Nous analyserons les suivantes :



Services d'hébergement

L'hébergement consiste en l'opération d'un prestataire de services qui laisse à la disposition d'autrui un espace disque afin de diffuser des sites dans Internet. Or, des documents illégaux sont parfois disponibles dans Internet, que ce soit des propos haineux, diffamatoires, contraires aux règles d'ordre public ou portant atteinte à la vie privée; il s'agit alors de savoir qui est responsable entre l'auteur ou l'hébergeur.

- Régime général d'exonération. Le rôle de l'hébergeur se limite à permettre une diffusion de pages Internet sans qu'aucun contrôle ne soit exercé, et ce, même s'il dispose de la possibilité de le faire.
- Responsabilité possible dans le cas où :
 - il a connaissance d'activités illicites de la part des personnes hébergées par lui, notamment quand on le lui fait savoir en lui adressant une lettre ou un courriel;
 - il a connaissance de circonstances qui rendent apparentes des activités illicites de la part des personnes hébergées par lui;
 - il n'a rien fait pour empêcher que des activités illicites de la part des personnes hébergées par lui soient perpétrées.


Services de référence

Les opérations liées aux activités de pages de liens hypertextes, de moteurs de recherche, d'index ou d'autres répertoires d'information sont appelées des services de référence. Ces derniers disposent d'un régime de responsabilité similaire à ceux des services d'hébergement.

Services de transmission

Par services de transmission, il faut comprendre l'action purement technique par laquelle un prestataire de services transporte des documents technologiques d'un point à un autre.

- Régime général d'exonération. Son rôle se limite à une action technique.
- Responsabilité possible dans le cas où :
 - il est à l'origine de la transmission;
 - il sélectionne ou modifie le document transmis;
 - il sélectionne la personne qui transmet, reçoit ou accède au document posant problème;
 - il conserve le document plus longtemps que ne l'exige la transmission.



Services de conservation Il faut comprendre par services de conservation l'action de conserver des documents afin d'assurer une meilleure efficacité de la transmission de documents technologiques. Cela correspond à deux situations principales que sont :

- la fonction « cache » (ou antémémorisation) qui consiste à stocker les éléments d'une page Internet sur un ordinateur ou un serveur afin de faciliter un accès ultérieur;
 - la conservation de documents nécessaires à l'utilisation de serveur à accès contrôlé, d'Intranet (notamment pour des raisons de sécurité).
- Régime général d'exonération. Un régime de responsabilité similaire au précédent s'applique aux prestataires de services de conservation.
 - Responsabilité possible dans le cas où :
 - dans l'une des quatre situations qui s'appliquent à la responsabilité du transmetteur (voir Services de transmission);
 - le prestataire ne respecte pas les conditions d'accès au document;
 - le prestataire empêche la vérification de qui a eu accès au document;
 - le prestataire ne retire pas promptement du réseau ou ne rend pas l'accès au document impossible alors qu'il avait connaissance :
 - qu'un tel document a été retiré de son emplacement initial;
 - qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès;
 - qu'une autorité compétente en a exigé le retrait.

Services d'archivage Afin de conserver certains documents importants, il est possible de recourir à des professionnels qui archivent pour autrui.

- À la différence de plusieurs autres services, celui-ci ne bénéficie pas d'un régime général d'exonération.
- Au contraire, le prestataire de services en archivage :
 - est assujéti à une obligation générale de sécurité;
 - doit préserver l'intégrité des documents dont il a la garde;
 - doit préserver les conditions liées à la conservation (voir paragraphe 3.2).
- De son côté, l'utilisateur de ces services d'archivage a l'obligation de faire savoir au prestataire que les documents qu'il lui confie doivent :
 - être interdits d'accès à toute personne non autorisée;
 - être tenus confidentiels.

Services de certification Les services d'une autorité de certification correspondent au fait de certifier l'identité ou l'une ou plusieurs qualités d'un certifié et de permettre à un tiers de s'assurer que le certifié est bien celui qu'il prétend être.

■— Obligations de l'autorité de certification :

- rédiger une politique de certification explicitant les considérations techniques essentielles (contenu du certificat, périodicité de révision, durée, modalités de délivrance, modalités pour assurer la confidentialité, traitement des plaintes);
- rendre publique la politique de certification;
- présenter des garanties d'impartialité;
- inscrire promptement sur le répertoire prévu à cet effet tout certificat invalide;
- assurer l'intégrité du certificat.

■— Obligations du certifié :

- garder secret tout dispositif qui permet d'utiliser le certificat, toute utilisation de ce dernier étant présumée faite par lui;
- dévoiler à l'autorité de certification tout motif qui laisserait croire que le dispositif est compromis par un tiers;
- informer l'autorité de certification de tout changement à son statut.

■— Obligations du tiers :

- vérifier l'identité des intervenants;
- vérifier au répertoire mis en place par l'autorité de certification, la validité du certificat.

■— Répartition des responsabilités :

- responsabilité non démontrée. Les parties sont toutes responsables;
- responsabilité partagée. Chacun assume sa part mais au cas où l'une des parties ne peut le faire, sa part ne doit pas être prise en charge par les autres;
- responsabilité impossible à établir. La responsabilité est répartie à parts égales;
- responsabilité d'aucun. La responsabilité est assumée conjointement et à parts égales.

Quelle que soit la répartition, elle est d'ordre public et ne peut donc être modifiée par contrat.



Le cadre d'une **entente** **de sécurité**



La rédaction d'une entente de sécurité est souvent l'attitude à adopter pour disposer d'une gestion documentaire diligente.

UNE ENTENTE DE SÉCURITÉ

Une entente de sécurité peut notamment être rédigée lors des différentes occasions ou opérations suivantes :

- le transfert d'un document technologique (voir paragraphe 3.1);
- la conservation d'un document technologique (voir paragraphe 3.2);
- lorsque le document technologique est confidentiel (voir paragraphe 5.2);
- la transmission d'un document technologique (voir paragraphe 3.4);
- lorsque l'on souhaite améliorer la preuve d'un document technologique;
- lorsque l'on cherche à préciser les obligations des intervenants au sein d'une entreprise (qui fait quoi!).

Quelles que soient les appellations que les partenaires utilisent pour qualifier ce document (entente de sécurité, politique de sécurité, protocole de sécurité, procédure de sécurité, mesures de sécurité, code de sécurité), les objectifs recherchés dans une entente de sécurité sont les suivants :

1. respecter les dispositions légales applicables;
2. permettre une bonne compréhension par les utilisateurs en cause;
3. offrir un degré de sécurité jugé adéquat à la sensibilité des documents technologiques;
4. permettre de la souplesse afin qu'elle puisse être utilisable dans un grand nombre de cas.



Une entente de sécurité est un outil permettant d'identifier les obligations en matière de sécurité, soit de la part des employés de l'entreprise, soit de celle des partenaires avec lesquels on fait affaire.

Quant à sa nature juridique, une entente de sécurité va parfois correspondre à un contrat que des partenaires signent entre eux ou à un document à portée interne au sein d'une institution précisant les obligations de chacun des intervenants.

Enfin, quant à la structure d'une entente de sécurité, il faut d'abord préciser que les circonstances vont avoir une influence majeure sur la façon de rédiger un pareil document. Selon le degré de confiance entre les parties, la sensibilité des documents traités, les risques inhérents aux activités, les moyens disponibles, la qualité des parties, ce document va être plus ou moins élaboré et plus ou moins précis.

Néanmoins, il est possible de proposer certains types de clauses que l'on peut trouver dans une entente de sécurité. Il y a, en premier lieu, des clauses « classiques » que l'on retrouve dans de très nombreux contrats (objet, définitions, protection des renseignements personnels, responsabilités). On peut également trouver, en second lieu, des clauses liées à l'entente proprement dite, à la gestion des documents et à la sécurité de l'environnement.



ÉLÉMENTS CONSTITUTIFS D'UNE ENTENTE DE SÉCURITÉ

Identification des parties Clause qui permet d'identifier les personnes intéressées par l'entente avec leur nom, adresse, coordonnées, etc.

Objet de l'entente Clause ayant pour objectif de préciser la portée et le but de l'entente. Les objectifs et les obligations peuvent donc être résumés ici.

Définition Aider les parties à l'interprétation ou à la définition de certains termes.

Conclusion de l'entente Organiser la relation entre les parties. Il faut distinguer l'entente de sécurité elle-même et ce qu'elle demande de faire. Il est donc nécessaire de prévoir les modalités de formation de l'entente telles que :

- sa portée;
 - les modalités de conclusion (signature);
 - les modalités de modification ou de renouvellement;
 - sa durée.
-

Gestion des documents durant leur cycle de vie Identifier les documents et les opérations à encadrer. L'entente est faite pour encadrer un certain nombre de documents et d'opérations (par exemple un contrat). Pour chacun, identifier les fonctions de sécurité qui s'appliquent, et ce, durant leur cycle de vie. Ce dernier concept fondamental nous suggère d'organiser la gestion des documents concernant :

- leur création;
- leur transfert;
- leur consultation;
- leur transmission;
- leur conservation;
- leur destruction éventuelle;
- les documents constitutifs d'un contrat.

Sécurité de l'environnement

Prévoir les modalités relatives à l'encadrement organisationnel telles que :

- — déterminer une personne assignée;
- — informer, responsabiliser (par contrat) et éduquer les employés;
- — rapporter les intrusions non autorisées dans l'environnement;
- — prévoir un plan de contingence, c'est-à-dire un document qui prévoit la procédure d'intervention à suivre en cas de problèmes de sécurité;
- — faire contrôler par une entreprise externe (audit) et faire des tests;
- — revoir périodiquement les modalités relatives à l'encadrement organisationnel;
- — évaluer les risques.

Prévoir les modalités relatives à l'encadrement technologique telles que :

- — organiser la sécurité physique (porte, serrure);
- — contrôler l'accès aux documents;
- — protéger contre les virus;
- — s'assurer de la sécurité des transmissions (chiffrement).

Protection des renseignements personnels et confidentiels

Vérifier le respect de ce domaine du droit lorsque des documents permettent d'identifier des personnes physiques ou d'obtenir des renseignements confidentiels protégés par une loi, un règlement ou une convention.

Responsabilités

Prévoir des clauses de responsabilité et de non-responsabilité, voire de force majeure.

Annexes

Dans l'hypothèse d'ententes de sécurité plus complexes, mettre en place des annexes précisant les mesures techniques à suivre.

LEXIQUE

Biométrie	Science étudiant les variations biologiques qui permet d'identifier une personne selon certaines de ses caractéristiques physiques. Exemples : empreintes digitales, reconnaissance vocale, empreinte de la rétine, ADN, etc.
Certificat numérique	Document technologique émis par une autorité de certification contenant un certain nombre d'informations pertinentes constituant une sorte de pièce d'identité électronique.
Certificat d'un document	Procédé d'identification où une autorité de certification crée un lien entre une personne et un document appelé certificat. Sur la base du certificat numérique émis par cette autorité de certification, le certifié pourra s'identifier auprès de tierces personnes qui recevront ledit certificat. Ainsi, ces dernières seront assurées que le certifié est bien celui qu'il prétend être. Notons aussi que certains certificats sont dénommés comme étant d'attribution. Dans un tel cas, le certificat va assurer les tiers que le détenteur est bien titulaire d'une qualité. Exemple : on peut imaginer des certificats statuant qu'une personne est bien membre d'un ordre professionnel, dispose bien d'un crédit d'une banque, est bien employée d'une entreprise ou d'un gouvernement, etc.
Chiffrement	Technique employée pour assurer la confidentialité des documents électroniques : un algorithme transforme les données pour les rendre inintelligibles à qui n'a pas la clé nécessaire au déchiffrement.
Cycle de vie d'un document	Période qui s'étend du moment où un document est créé jusqu'à celui où il est détruit. Il comprend notamment les différentes étapes de la vie d'un document que sont son transfert, sa consultation, sa transmission ou sa conservation.
Document technologique	Élément constitué d'informations (document) qui utilise un support faisant appel à une ou plusieurs technologies de l'information. Cette technologie peut bien sûr être l'électronique mais pas uniquement. Il faut également inclure des supports magnétique, optique, etc. L'application de la Loi se veut donc large pour ne pas exclure de nouvelles technologies qui émergeraient demain. C'est donc pour ne pas oublier une technologie en particulier que la Loi évoque le terme de « document technologique » (technologie de l'information) et non seulement celui de « document électronique » (qui est un sous-ensemble du premier). Exemples : courriel, fichier Word ou Powerpoint, ruban magnétique, cédérom, fichier MP3.
EDI	(Échanges de documents informatisés) Application téléinformatique assurant la transmission de documents électroniques dans un format normalisé et structuré qui permet l'automatisation.
Infrastructure à clé publique ICP	L'infrastructure à clé publique est constituée de trois éléments : <ul style="list-style-type: none">- une clé privée pour chaque intervenant;- une clé publique correspondant à la clé privée;- un certificat délivré par une autorité de certification qui identifie une personne. L'infrastructure à clé publique est l'outil le plus souvent présenté comme la solution sécuritaire dans des environnements ouverts comme Internet. Elle permet en effet : <ul style="list-style-type: none">- de respecter l'intégrité d'un document lors de son transport;- de s'assurer que le document est transmis de façon confidentielle avec un système de chiffrement qui rend le document illisible lors de la transmission;- de savoir que le document origine bien de la personne désignée. Exemple : Alice adresse un document à Benoît en utilisant une infrastructure à clé publique. <ul style="list-style-type: none">- Alice chiffre (par l'entremise d'un outil cryptographique qui le rend illisible) le document à envoyer avec la clé publique de Benoît qui est accessible partout;- Benoît déchiffre le document envoyé par Alice avec sa clé privée. Ainsi, la confidentialité est assurée. Il est également possible d'assurer les deux autres fonctions d'intégrité et d'authentification de la façon suivante : <ul style="list-style-type: none">- Alice effectue un condensé du document à envoyer en utilisant sa clé privée et crée ce que l'on appelle une signature numérique;- Benoît va utiliser la clé publique d'Alice pour ouvrir la signature d'Alice. Si la signature devient un document lisible et identique au document envoyé, alors c'est bien Alice qui l'a envoyé. Pour être sûr qu'Alice et Benoît sont bien les personnes qu'ils prétendent être, ils peuvent utiliser un certificat émis par une autorité de certification qui, après vérification de leur identité, leur remettra un document les identifiant et contenant une clé publique.
Loi	Dans l'ensemble du document, « Loi » signifie <i>Loi concernant le cadre juridique des technologies de l'information</i> , L.R.Q., chapitre C-1.1.

RÉFÉRENCES

Site général relatif à la Loi concernant le cadre juridique des technologies de l'information (2001 - Québec)

http://www.autoroute.gouv.qc.ca/loi_en_ligne/

PME Québec Clic (site destiné aux affaires électroniques) (Québec)

<http://www.pmequebeclic.com>

Loi sur la protection des renseignements personnels dans le secteur privé (1994 - Québec)

<http://www.canlii.org/qc/legis/loi/p-39.1/20040901/tout.html>

Guide des droits sur Internet (Québec)

<http://www.droitsurinternet.ca/>

Loi sur la protection des renseignements personnels et les documents électroniques (2000 - Canada)

<http://www.canlii.org/ca/loi/p-8.6/index.html>

Guide de sécurité en ligne et de protection des renseignements personnels (2003 -Canada)

<http://www.guidievieprivee.icce.ca/>

Loi sur le commerce électronique (2000 - Ontario)

<http://www.canlii.org/on/legis/loi/2000c.17/20040901/tout.html>

Code de pratique pour la gestion de sécurité d'information (ISO/CEI 17799 - international)

ISBN 2-9808666-0-1

Dépôt légal - Bibliothèque nationale du Québec, 2005

Dépôt légal - Bibliothèque nationale du Canada, 2005

© La Fondation du Barreau du Québec, novembre 2005.

Tous droits réservés.





La Fondation du Barreau du Québec est un organisme sans but lucratif dont la mission comporte, entre autres choses, l'objectif de servir les intérêts des justiciables québécois en les informant de leurs droits et de leurs obligations. Ce guide a été réalisé pour tous ceux et celles qui s'intéressent à la gestion des documents technologiques.

fondation@barreau.qc.ca

Note sur l'auteur :

Vincent Gautrais est professeur à la Faculté de droit de l'Université de Montréal et avocat, membre du Barreau du Québec. Spécialiste en droit des affaires électroniques, il est actuellement directeur du programme de maîtrise en commerce électronique.

vincent.gautrais@umontreal.ca

Nos partenaires :



MEMBRE DU RÉSEAU
Entreprises Canada

MEMBER OF THE
Canada Business
Network