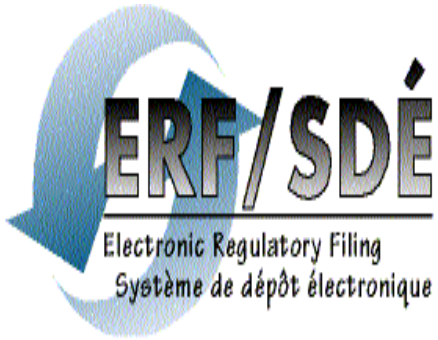
Projet de système de dépôt électronique

Un projet conjoint de l'Office national de l'énergie et de la Commission de l'énergie de l'Ontario

Questions et commentaires

Le 15 janvier 1999



Office national de l'énergie
444, Septième Avenue S.-O.
Calgary (Alberta) T2P OX8
(403) 292-4800
http://www.neb.gc.ca

Commission de l'énergie de l'Ontario
2300, rue Yonge
C.P. 2319
Toronto (Ontario) M4P 1E4
(416) 481-1967
http://www.oeb.gov.on.ca

TABLE DES MATIÈRES

1. Quel est l'objet du présent rapport?

L'Office national de l'énergie (ONÉ) et la Commission de l'énergie de l'Ontario (CÉO) se préparent à convertir leurs systèmes d'information du papier à l'électronique. En vertu du Système de dépôt électronique (SDÉ) proposé, tous les participants aux processus de réglementation de l'Office et de la Commission transmettront et recevront l'information pertinente au moyen d'ordinateurs. Les documents papier feront alors exception.

Nota : Le présent rapport[1] a pour objet de fournir des renseignements généraux sur le SDÉ. Les propos qu'il contient sont d'ordre général et ne constituent pas un avis juridique. Les lecteurs qui recherchent un tel avis devraient consulter leurs propres conseillers.

2. **Où en est le SDÉ?**

À la suite d'une étude de faisabilité achevée en mars 1993, l'Office et la Commission ont procédé avec prudence, effectuant des études coûts-avantages et franchissant progressivement les étapes d'analyse, de conception et de mise en œuvre de projets pilotes. Durant ce temps, les entreprises de services publics réglementées, les intervenants et autres parties intéressées aux instances de l'Office et de la Commission ont participé à des ateliers et des séances de planification sur le SDÉ. Un prototype fonctionnel a déjà fait l'objet d'une démonstration. La mise en oeuvre initiale est prévue pour la fin de 1999.

3. **Quelles questions ont été soulevées au sujet du SDÉ?**

Deux catégories de questions ont été soulevées : celles qui découlent de la nouveauté relative du SDÉ (p. ex. «Comment puis-je signer un document électronique?») et celles qui prévoient des changements fondamentaux dans la façon dont l'Office et la Commission fonctionnent (p. ex. «Le SDÉ mènera-t-il à un plus grand nombre d'audiences par voie de mémoires?»).

Les questions de nouveauté se résoudront par le biais de la formation et de la connaissance du système. Toute nouvelle technologie soulève inévitablement des préoccupations au sujet des risques. Lors de l'arrivée des photocopieurs, par exemple, les gens ont manifesté certaines inquiétudes au sujet de la précision de la reproduction. Quand les télécopieurs sont apparus, on en a scruté l'utilisation. Les préoccupations

[1]Robin Nunn a rédigé le présent rapport pour le compte de la Commision de l'énergie de l'Ontario et de l'Office national de l'énergie (il remercie particulièrement Stephen McCann, Charles Mathis et Claire McKinnon pour leur aide).

portaient sur la précision des télécopies, les coûts inhérents aux envois par télécopieur et la légalité des documents télécopiés. Dorénavant, ces deux technologies, soit la photocopie et la télécopie, sont courantes, bien connues et utilisées presque sans réserve, à l'instar d'autres technologies familières comme le téléphone et la télévision. Bien qu'il existe toujours des problèmes, la plupart des premières préoccupations ont été résolues non pas en modifiant considérablement la technologie, mais en la comprenant mieux et en perfectionnant les procédés connexes.

Tout comme des inquiétudes se manifestent toujours au sujet des risques potentiels d'une nouvelle technologie, les gens ont aussi tendance à supposer le contraire, c'est-à-dire que les nouvelles machines, les ordinateurs en particulier, sont infaillibles. Ils semblent croire que, si les ordinateurs ne sont pas parfaits, ils sont alors inutiles. Songez à la question suivante : «Quels sont les risques de perdre un document parmi des milliers d'autres dans un système informatique?». On se pose rarement cette question dans le cas du système actuel de documents papier. Tout le monde sait qu'il est possible de perdre du papier. Aucun système informatique ou papier fonctionnel n'est à l'abri des risques. Les systèmes que l'Office et la Commission utilisent actuellement (papier ou électronique) ne sont pas parfaits. Un document papier peut être classé au mauvais endroit ou envoyé à la mauvaise adresse. Les mêmes erreurs peuvent se produire dans un système informatique. Grâce à une conception adéquate toutefois, il est possible de repérer et de corriger les erreurs, qu'il s'agisse d'un système électronique ou non. Il faut cependant comparer les risques inhérents au système proposé avec ceux du système actuel et non considérer la question comme un idéal impossible à atteindre.

Entre les préoccupations relatives aux risques, d'une part, et les attentes de perfection, d'autre part, une question se pose : n'y a-t-il pas danger de reproduire le système actuel sous forme électronique? Il pourrait être possible par ailleurs, après examen des motifs qui sous-tendent les procédures actuelles, d'adapter uniquement les aspects nécessaires au SDÉ. Par exemple, on utilise maintenant des signatures manuscrites et des affidavits sur les documents déposés auprès de l'Office et de la Commission. Naturellement, on a tendance à chercher une analogie électronique, comme la reproduction numérique d'une signature manuscrite. Est-ce nécessaire? Comment une image, que quiconque peut reproduire, se compare-t-elle à une signature manuscrite que seule la main du rédacteur peut réaliser? La signature manuscrite est-t-elle l'unique moyen de s'assurer de la légalité d'un document? Examine-t-on les signatures et est-ce qu'on s'attend à ce qu'il y ait contrefaçon? Ces questions démontrent qu'il faut éviter de reproduire le système actuel et en concevoir un meilleur. Pour obtenir de plus amples détails au sujet de ces questions particulières, consultez la section du présent rapport décrivant la façon dont on signera les documents dans le SDÉ.

Les ordinateurs sont impersonnels. Aucun humain n'assure la protection de l'information dans un ordinateur. Un mot de passe ou autre dispositif technique joue alors ce rôle. En conséquence, on a tendance à remettre en question la façon dont la machine impersonnelle effectuera toutes les choses qu'une personne fait pour assurer l'honnêteté du système. On s'attend également à ce que les ordinateurs fassent honneur à leur réputation de rapidité et d'efficacité surhumaines. Par conséquent, le temps

devient un problème là où il ne l'est peut-être pas maintenant. Par exemple, les utilisateurs demandent s'il est possible d'accéder au système informatique 24 heures sur 24 tous les jours. Nous ne nous posons pas cette question au sujet des systèmes manuels existants qui ne sont disponibles que durant les heures normales de bureau. On s'attend à ce que les ordinateurs fournissent des enregistrements vérifiés et qu'ils confirment chaque étape. Dans le système de documents papier actuel, cependant, nous acceptons souvent les risques du courrier ordinaire au lieu d'utiliser le courrier recommandé. Les ordinateurs traitent également des quantités énormes d'informations, qui sont pourtant intangibles et invisibles jusqu'à leur affichage à l'écran ou leur impression sur papier. Nous faisons implicitement confiance au texte composé et relié d'un livre, car la contrefaçon exigerait de l'habilité et des frais, alors que tout le monde peut faire apparaître des mots sur un écran ou un imprimé. Qui peut affirmer qu'ils sont authentiques? C'est pourquoi on pose au sujet des ordinateurs des questions que l'on ne poserait pas si les processus étaient plus humains et tangibles, moins techniques et complexes.

Peu importe les raisons de ces préoccupations et le type de système qui sera un jour mis en oeuvre, tous les intéressés doivent avoir confiance en lui. On peut exprimer des réserves d'ordre juridique simplement pour déterminer s'il faut faire confiance au nouveau SDÉ. En fait, la confiance est l'un des thèmes sous-jacents du présent rapport (voir, par exemple, la section traitant des tierces personnes de confiance et de l'infrastructure des systèmes à clés publiques). Le papier inspire confiance. Les documents papier servent à établir la vérité. La technologie informatique est nouvelle et n'inspire pas autant la confiance; elle suscite donc un réexamen des notions de confiance et de vérité.

Comme nous l'avons indiqué précédemment, les gens ont tendance à avoir des attentes irréalistes en ce qui a trait aux ordinateurs. Certaines personnes peuvent s'imaginer des audiences durant lesquelles les participants communiquent uniquement en tapant sur des claviers dans un centre de réglementation futuriste où le papier est proscrit. Le SDÉ est plutôt conçu pour améliorer les processus de réglementation de façons particulières axées non pas sur la technologie, mais sur des documents structurés et normalisés.

- Les principales améliorations reposent sur le dépôt central des documents électroniques. Au moyen d'un format international appelé langage standard généralisé de balisage (LSGB), toutes les informations du dépôt central posséderont une structure formelle. Cette structure, nécessaire pour stocker les documents (comprise dans la définition du type de document), permettra un échange et une gestion efficaces de ceux-ci. On prévoit que les informations seront plus complètes et plus faciles à trouver et à utiliser.

- Comme les informations se trouvent dans un dépôt central, les participants peuvent choisir celles qui les intéressent. On prévoit ainsi épargner les coûts de distribution de toute l'information à tous les participants tout en fournissant l'information demandée plus efficacement. On peut extraire des documents du système au lieu d'avoir à les envoyer à chacun.

- S’appuyant sur le système de base, les systèmes informatisés de gestion de l’information peuvent faciliter la tenue des réunions et des audiences. C’est ce qu’on appelle la salle d’audience automatisée. Dans sa forme la plus simple, elle permettra à chaque personne présente dans la salle de chercher et de récupérer des documents par voie électronique. Il ne faut pas confondre cela avec la transcription assistée par ordinateur qui permet de reproduire mot à mot le contenu des audiences. Ces transcriptions ne représenteront qu’un type de document stocké dans le dépôt central du SDÉ. Une autre technologie permettra la participation à distance. Parmi les autres possibilités, notons l’utilisation de logiciels permettant à des groupes de travailler ensemble à des moments et des endroits différents. Ce dernier concept s’appelle la salle d’audience électronique.

- Une autre amélioration proposée consiste à utiliser des outils de gestion de cas et d’ordonnancement du travail pour traiter les documents et améliorer l’établissement du calendrier.

- Les concepteurs du SDÉ proposent également de fournir une aide complète, non seulement sur l’utilisation du système informatique, mais également sur l’essence même du processus de réglementation.

Il importe de ne pas confondre le SDÉ avec d’autres innovations technologiques. Il ne s’agit pas d’un système de transcription assistée par ordinateur permettant d’obtenir des comptes-rendus exhaustifs instantanément. Il ne s’agit pas d’un système d’échange électronique de documents comme ceux qu’on utilise pour les transactions commerciales d’achat et de vente automatisées au moyen de bons de commande et de factures standard. Le SDÉ n’est pas un système d’imagerie qui stocke des images de documents. Ces techniques ainsi que d’autres peuvent faire partie du système proposé, mais elles ne sont pas essentielles. Les principaux avantages du SDÉ devraient se situer sur le plan de la création et du traitement des documents courants. Il est possible d’automatiser les documents électroniques et il n’est pas nécessaire de les imprimer, de les reproduire, de les relier ni de les livrer.

Il est également important de distinguer le dépôt central de documents du SDÉ d’un système d’enregistrement. Un bureau d’enregistrement, par exemple, sert à enregistrer des documents officiels. Ceux-ci sont refusés s’ils ne sont pas présentés dans la forme prescrite et seuls certains types de documents sont acceptés. L’information déposée auprès d’un bureau d’enregistrement a une incidence directe sur les garanties juridiques. Comparons le modèle du bureau d’enregistrement avec le système proposé de documents informatisés du SDÉ servant principalement à échanger de l’information. De nombreux types de documents sont acceptés afin que les participants puissent présenter leurs arguments. La plupart des documents déposés auprès de l’Office et de la Commission n’ont pas d’incidence directe sur les garanties juridiques. En réalité, bon nombre d’entre eux sont déposés avant le début d’une audience et n’ont aucune valeur juridique avant d’être considérés comme preuves admissibles. Même ceux qui sont acceptés en preuve n’ont habituellement pas la portée des documents d’enregistrement qui ont des conséquences juridiques directes. Ces différences ont une importance

considérable dans la conception du SDÉ proposé (consultez également la section traitant des autres systèmes électroniques).

Conclusion : le SDÉ constitue un moyen d'améliorer la communication et non une modification de l'essence même du processus de réglementation.

4. **Quel est le fondement juridique du SDÉ?**

Lorsqu'on a utilisé des documents électroniques pour la première fois dans le cadre de procédures judiciaires, on s'est interrogé au sujet de leur valeur par rapport aux documents papier. Dans certains cas, les lois ont résolu ces questions. Par exemple, de nombreuses lois confèrent maintenant la même valeur aux fichiers informatiques et aux documents papier (*Loi sur l'accès à l'information*, L.R.C. (1985), ch. A-1, par. 4(3), *Loi sur les sociétés par actions*, L.R.C. (1985), ch. C-44, par. 22(1), *Loi sur la preuve au Canada*, L.R.C. ch. C-5, par. 30(12), *Loi sur les brevets*, L.R.C. (1985), ch. P-4, al. 8(1)*1*), *Loi sur les sociétés par actions*, L.R.O. (1990), ch. B.16, par. 139(1), *Loi sur l'enregistrement électronique*, L.R.O. 1991 ch. E.44, *Loi sur l'enregistrement des droits immobiliers*, L.R.O. (1990), ch. L.5, par. 166(1), *Loi sur l'enregistrement des actes*, L.R.O. (1990), ch. R.20, par. 16(1) — consultez également la législation dans un nombre croissant d'États américains qui ont suivi l'exemple de l'Utah relativement à l'adoption de lois qui stipulent que, dans la correspondance avec le gouvernement, une signature numérique équivaut à une signature manuscrite).

À l'échelon fédéral, le rapport du Comité directeur de la stratégie - sécurité de la technologie de l'information, remis au Conseil du renouveau administratif en juin 1995, formulait les recommandations suivantes :

> «Bien qu'aucun obstacle juridique n'empêche le gouvernement fédéral d'utiliser la technologie de l'information, de mettre en oeuvre une stratégie sur la sécurité de la technologie de l'information ou de mettre en place un système à clés publiques pour le chiffrement des signatures numériques et des documents confidentiels, le Comité directeur recommande *que la loi soit révisée et éventuellement modifiée dans les domaines suivants :*
>
> - La *Loi d'interprétation* et la *Loi sur la preuve au Canada* devraient faire l'objet d'une révision pour clarifier les exigences en matière de preuves relatives aux fichiers électroniques, en ce qui a trait notamment aux conditions prescrites concernant les documents originaux écrits, les copies certifiées ou notariées, etc.
>
> - Les ministères devraient revoir leur propre mandat et les lois applicables pour s'assurer que la législation comporte des dispositions relatives à l'utilisation de ces nouvelles technologies de l'information.
>
> - La *Loi sur l'accès à l'information* et la *Loi sur la protection de la vie privée* devraient faire l'objet d'une clarification en ce qui a trait aux exigences relatives à la technologie de l'information et notamment :
>
>   - les recherches et la surveillance par ordinateur;
>   - les cartes à mémoire;
>   - les pistes de vérification;

- la base de données centrale et les bases de données dont le contenu change fréquemment;
- les formalités relatives aux échanges d'information entre les institutions gouvernementales.

- Il faudrait adopter des lois concernant les systèmes à clés publiques pour définir les rôles et responsabilités des nombreuses parties en cause et restreindre la responsabilité financière du gouvernement fédéral. Il est important de nommer rapidement un ministre compétent relativement à l'application de telles lois.

- Il faudrait consulter le public au sujet des questions suivantes : l'utilisation de renseignements personnels sur les cartes à puce du gouvernement par exemple, l'échange de renseignements personnels entre les ministères ou entre les gouvernements fédéral et provinciaux et l'accès des forces de l'ordre aux renseignements chiffrés.

- Il faudrait clarifier les responsabilités juridiques des exploitants de babillards électroniques et des personnes qui diffusent de l'information sur des réseaux électroniques publics.

- Il faut réviser et probablement modifier les définitions des termes utilisés dans un contexte de communication électronique (p. ex., «communications privées», «place publique», «publication», «possession», «collection» et «divulgation»).

Un projet de loi fédéral, soit la Loi sur la protection des renseignements personnels et les documents électroniques (projet de loi C-54), traite de certaines de ces questions. La deuxième partie de ce projet de loi prévoit des solutions de rechange sur le plan électronique aux documents papier régis par les lois fédérales. Au lieu de modifier chaque loi fédérale séparément, le projet de loi modifierait l'ensemble de la législation. Les organismes gouvernementaux fédéraux seront autorisés à utiliser des moyens électroniques au lieu du papier, y compris les paiements, les formulaires et les dépôts électroniques.

L'ONÉ a présentement le pouvoir d'adopter des règles régissant la conduite de ses affaires (*Loi sur l'Office national de l'énergie*, L.R.C. (1985), ch. N-7, art. 8). Les *Règles de pratique et de procédure de l'Office national de l'énergie (1995)* (DORS/95-208), font explicitement référence au dépôt de documents. L'article 9 autorise tous les types de dépôts que l'ONÉ peut recevoir. Le même règlement rend toutefois obligatoire le dépôt de documents papier en plus des documents électroniques. Les règles font présentement l'objet d'une révision pour tenir compte des dépôts électroniques. La Commission de l'énergie de l'Ontario a également autorité sur le déroulement de ses audiences (*Loi sur l'exercice des compétences légales*, L.R.O. (1990), ch. S.22, art. 25.1) et les renseignements qui lui sont transmis (*Loi sur la Commission de l'énergie de l'Ontario*, 1998, art. 13). Ses règles font également l'objet d'une révision afin qu'elles accordent la même valeur aux dépôts de documents papier et de documents électroniques.

En l'absence de dispositions législatives plus précises sur le dépôt électronique, les principes de droits généraux établis en fonction des documents papier doivent être interprétés de nouveau dans un contexte électronique.

5. **Quels critères ont servi à la conception du SDÉ?**

Dès les premières étapes de planification, on a élaboré un ensemble de principes et de critères concernant le SDÉ, notamment :

- **!** les systèmes et les processus employés dans le cadre de cette initiative doivent être efficaces, fiables et sûrs;
- **!** les documents électroniques doivent satisfaire aux critères suivants :

  les documents électroniques doivent pouvoir durer et on doit être en mesure de conserver l'information documentaire (y compris la preuve) pendant la durée nécessaire à un tribunal d'archives;

  le chargement des documents dans le système doit être précis;

  le chargement des documents dans le système (c'est-à-dire le dépôt central des documents) doit se faire en temps opportun et nécessiter un minimum de manipulation;

  la présentation d'un document (c'est-à-dire les polices et la mise en page du document) déterminée par l'auteur doit, dans la mesure du possible, être conservée;

  les documents doivent être accessibles universellement, autrement dit, ils doivent être généralement récupérables et réutilisables peu importe le système ou le logiciel dont se sert l'utilisateur et qui est compatible avec les normes de systèmes ouverts;

  l'échange de documents doit être possible au moyen d'un éventail de véhicules de communication (p. ex., courrier électronique, disquettes, Internet, transfert de fichiers, CD-ROM);

- **!** dans la mesure du possible, l'initiative s'appuiera sur une politique et des normes de systèmes ouverts non brevetés;
- **!** les systèmes mis en oeuvre doivent être commandés par les utilisateurs et doivent satisfaire et équilibrer les besoins de tous les participants et du grand public;
- **!** les systèmes et les processus mis en place doivent permettre de réduire à long terme les coûts de la réglementation et les délais de traitement;
- **!** aux endroits où des services intérimaires sont offerts, ils doivent être rentables en soi et contribuer à la réalisation de l'objectif à long terme du SDÉ.

6. **Quel niveau de protection le SDÉ pourra-t-il offrir?**

Tous les systèmes informatiques nécessitent des mesures de sécurité. Quel type de sécurité est nécessaire et dans quelle mesure? La réponse dépend de questions incidentes, notamment : qui a accès aux ordinateurs et aux réseaux de communication? Qui possède un accès électronique? Qu'est-ce qui amènerait une personne à enfreindre la sécurité? Quelles infractions à la sécurité peut-on détecter? Quelles sont les conséquences des infractions à la sécurité? Quels sont les coûts inhérents à la protection? Quel niveau de protection offre le système papier actuel en comparaison? Les précautions en matière de sécurité entravent-elles l'utilisation normale du système? Et beaucoup d'autres questions détaillées.

Dans tout système informatique, il faut régler les questions suivantes :

- autorisation : l'autorisation d'utiliser le système (ce qui comprend non seulement les personnes, mais également les ordinateurs, c'est-à-dire les autres systèmes informatiques qui peuvent également accéder au système);

- authenticité : il faut déterminer si les utilisateurs sont réellement ceux qu'ils prétendent être et si l'information qu'ils fournissent est ce qu'elle doit être;

- disponibilité : il faut déterminer si le système est disponible et accessible lorsqu'il le faut;

- vérification;

- confidentialité;

- intégrité de l'information dans le système;

- respect de la vie privée.

Comme nous l'avons noté plus tôt, aucun système n'est parfait. Les systèmes de documents papier actuels ne sont pas parfaitement sûrs. Toutefois, on a jugé qu'ils étaient acceptables. Même les classeurs verrouillés derrière des portes verrouillées peuvent ne pas résister à un intrus déterminé. Le feu et l'eau peuvent endommager les dossiers papier comme les fichiers électroniques. Le système informatique d'un organisme peut subir des dommages non seulement de la part d'un individu utilisant la technologie, comme le légendaire pirate informatique, mais également d'une personne en mesure de perturber le fonctionnement de tout système, comme un employé mécontent. Il y a toujours un risque, mais aucune garantie de sécurité absolue.

En utilisant des techniques de sécurité informatiques acceptables, le SDÉ proposé peut s'avérer plus sûr que le système actuel. Présentement :

- le document papier peut parvenir à la mauvaise adresse ou se perdre dans le courrier;

- le public peut manipuler les documents originaux auxquels il a accès et peut, par conséquent, les endommager, les modifier ou les perdre;

- les dossiers existants peuvent être incomplets;

- il peut être difficile de retrouver les dossiers anciens;

- les dossiers papier actuels peuvent comporter des erreurs;

- il n'y a pas de système de secours ou de sauvegarde analogue à celui d'un système électronique dont on peut se servir après un sinistre ou durant des interruptions courantes, comme le déménagement vers un nouvel emplacement;

- même les documents ayant un statut particulier, comme les affidavits signés, ne sont pas particulièrement sûrs de nos jours. Il serait inhabituel pour un tribunal de confirmer l'identité ou l'autorité de la personne qui a signé ou de comparer les signatures sur l'affidavit avec toute autre pièce d'identité, comme un permis de conduire ou un passeport.

Tout comme le papier pose des problèmes de sécurité particuliers (accès aux locaux, cadenas à combinaison, clés), les systèmes informatiques ont aussi les leurs (mots de passe, copies de sauvegarde, panne de courant). Un système informatique bien conçu offre autant sinon plus de sécurité qu'un système papier. Comme tous les documents se présentent sous forme électronique, il est possible d'en fournir des copies identiques au besoin. On peut contrôler et vérifier l'accès aux fichiers. Les techniques de vérification par ordinateur peuvent réduire les erreurs. La normalisation des formats peut améliorer la cueillette et la récupération des données. L'automatisation peut réduire les erreurs humaines.

Comme il est possible de rendre les systèmes informatiques plus sûrs que les systèmes papier, la sécurité informatique ne consiste pas uniquement à protéger le système, mais également à trouver un équilibre entre la sécurité et la facilité d'utilisation. Une sécurité trop importante peut s'avérer aussi inefficace qu'une sécurité insuffisante. Par exemple, on peut rendre un système informatique très sûr en attribuant un mot de passe unique à chaque document et en utilisant un programme particulier pour y accéder. Un intrus devrait connaître dix mots de passe et savoir comment utiliser dix programmes pour lire dix documents. Il est techniquement facile de créer une telle barrière. Malheureusement, les utilisateurs autorisés seraient également confrontés à ce même obstacle. Personne ne voudrait utiliser un tel système sûr, mais inefficace. En effet, les utilisateurs autorisés oublieraient probablement un bon nombre des mots de passe ou les noteraient sur une feuille et créeraient ainsi un nouveau problème de sécurité à l'égard de la protection de la liste des mots de passe.

Les documents papier sont si familiers que nous nous informons rarement des exigences en matière de sécurité. Quels éléments nous inspirent confiance à leur égard? Les mêmes s'appliquent aux documents numériques, notamment :

- l’authenticité de la personne — un document devrait indiquer qui l’a signé;

- l’authenticité du document — un document devrait indiquer ce que la personne a signé.

Prenons une lettre ordinaire signée par la personne qui l’a rédigée. De nombreux éléments pourraient servir à en prouver l’authenticité : un graphologue pourrait témoigner au sujet de la signature, un expert en matériaux pourrait analyser le papier et l’encre, alors que l’adresse, l’adresse de retour, le cachet de la poste, le timbre et le contenu pourraient tous contribuer à nous inspirer une confiance absolue en ce document. Chacun de ces éléments pourrait toutefois être contrefait. L’écriture peut tromper même un expert ou être tout simplement illisible. Les témoins peuvent mentir.

Dans un système informatique, les techniques d’authentification doivent être conçues de manière à prévenir la contrefaçon. Le système doit faire en sorte que la personne qui signe le document ne puisse nier l’avoir fait. Toute technique utilisée couramment devrait être efficace. À l’instar d’une signature manuscrite, cela devrait être facile à faire. On peut appliquer aux ordinateurs bon nombre des techniques employées dans les systèmes papier, y compris l’accusé de réception (comme dans le cas du courrier recommandé) et la vérification du trafic de messages (suivi et enregistrement du courrier).

Les documents électroniques sont-ils sûrs? Bien qu’aucune décision définitive n’ait été prise au sujet des programmes de sécurité particuliers à utiliser avec le SDÉ, la conception du système de documents électroniques proposé prévoit des logiciels servant à prévenir les modifications non autorisées des documents. Le système sera en mesure de détecter si l’information a été modifiée, à quel moment elle l’a été la dernière fois et par qui. À cet égard, les documents papier, qui sont faciles à modifier, sont moins sûrs que les documents électroniques du SDÉ proposé.

Les documents électroniques peuvent-ils être contrefaits? Dans le cas des instances réglementaires, la contrefaçon des documents est peu probable. Le secrétaire de l’Office ou de la Commission n’examine pas présentement la signature manuscrite de l’avocat ou du témoin qui dépose un document papier afin d’être certain qu’il s’agit d’une signature authentique. Un document électronique, par contre, peut comporter un code de sécurité (une signature numérique, dont on parlera ailleurs dans le présent rapport) servant de signature manuscrite.

Un système électronique doit également être en mesure de s’assurer que la personne qui envoie un document ne puisse nier l’avoir fait et qu’une personne recevant un document ne puisse nier l’avoir reçu. Le SDÉ proposé comporte là encore des éléments relatifs à la non-répudiation et à la vérification des transactions.

L’authentification d’un document est étroitement liée à la vérification du contenu. Les techniques de signature des documents devraient offrir un moyen de vérifier non seulement à quel document se rapporte la signature, mais aussi que le document signé est complet et authentique.

Dans certains systèmes informatiques, même les mesures de sécurité qui protègent le système sont confidentielles, et l'emplacement ou peut-être même l'existence des systèmes sont tenus secrets. Dans la région, par exemple, un grand immeuble de banlieue non identifié abrite les systèmes informatiques d'une importante société multinationale. L'immeuble ne porte pas de nom, seulement une adresse. Toute organisation, même pourvue d'une sécurité aussi serrée, doit être prête à divulguer au besoin les détails nécessaires au sujet de son système informatique pour prouver l'authenticité de fichiers informatiques en cour (consultez également la section traitant de la preuve informatique).

De nombreuses organisations ont recours aux mêmes techniques de sécurité informatique, y compris les banques et les forces de l'ordre, qui ont également besoin de systèmes sûrs.

7. **Quels formats électroniques utilisera-t-on pour les documents du SDÉ?**

De préférence aux formats exclusifs, le SDÉ utilise des formats ouverts internationaux lorsque cela est possible. En conséquence, le SDÉ n'accepte pas les formats propres à des produits comme Word de Microsoft ou WordPerfect de Corel. Comme la plupart des documents déposés contiennent du texte (c'est-à-dire des mots, des tableaux, des graphiques, etc.), l'architecture sous-jacente repose sur le langage standard généralisé de balisage (LSGB) international. On prévoit également que les formats XML et HTML serviront également à distribuer de l'information, bien que les documents acceptés au dépôt central doivent être en LSGB. On peut stocker certains documents contenant par exemple des données numériques volumineuses dans des formats courants de base de données relationnelles. Bien que les images de documents produites par lecture optique ou par télécopie directe puissent servir dans des cas exceptionnels, l'architecture du SDÉ repose sur des formats à base de caractères se prêtant à des recherches. (Consultez également le glossaire de l'annexe C pour obtenir de l'aide concernant les termes techniques utilisés dans la présente section).

Il n'existe pas de format de document parfait ni de moyen infaillible pour chercher de l'information dans un grand dépôt central. L'Office et la Commission ont choisi un format permettant de coder de l'information contextuelle dans le document même. Cette information supplémentaire, outre les mots, peut servir à chercher des documents, à les convertir d'un format à l'autre ou à effectuer d'autres traitements au moyen des informations additionnelles codées dans le document. Grâce au LSGB les documents peuvent être exploités comme des bases de données, au lieu d'être simplement stockés.

On peut procéder à des recherches mot à mot avec les autres formats, mais la recherche plein texte familière est susceptible de se buter à des problèmes de parasites et autres concepts connexes issus de la théorie fondamentale de l'information. En deux mots, lorsqu'on cherche dans un grand dépôt central, on obtient trop ou pas assez d'information, mais rarement l'information exacte nécessaire. Les transcriptions de témoignages, par exemple, compliquent la recherche mot à mot étant donné toutes les

subtilités du langage humain. Un témoin peut parler souvent de «il», par exemple, en le décrivant en détail, alors que seule une référence indirecte située bien avant dans le texte explique ce qu'est «il». Les mots clés qui apparaissent fréquemment dans une base de données sur l'énergie, comme «gaz naturel», ne sont pas plus utiles pour trouver des passages pertinents que des mots comme «il». On peut indexer de nombreux formats de document séparément pour améliorer la recherche, mais cet index n'est pas contenu dans le format même du document. L'indexage par mot clé présente aussi des inconvénients, surtout s'il est mécanique. Par contre, on peut indexer un document en LSGB pendant sa création, les éléments et les attributs voulus étant intégrés dans le document par l'auteur.

Les formats qui combinent la mise en forme et le contenu, comme ceux des logiciels de traitement de textes et Adobe Portable Document Format (PDF), sont conçus pour bien faire paraître le texte et les graphiques sur une page. Ils tentent de reproduire électroniquement le document papier. Cependant, la mise en forme en souffrira si le dispositif de sortie, habituellement l'imprimante ou l'écran, ne peut reproduire les caractères et d'autres caractéristiques utilisées par l'auteur du document. Ils produisent également des documents beaucoup plus volumineux que le LSGB et consomment plus de ressources en matière de communication et de stockage. La séparation de la forme et du contenu qu'offre le LSGB augmente les possibilités de réutilisation des documents; la conversion entre documents LSGB ou du LSGB à d'autres formats, comme le PDF, est beaucoup plus facile qu'à partir d'un format contenant moins d'informations intégrées.

Le LSGB est devenu une norme internationale arrivée à maturité, contrairement aux formats exclusifs qui changent fréquemment. L'Office et la Commission ont noté les problèmes éprouvés par d'autres tribunaux aux prises avec de prétendues mises à niveau. Par exemple, lorsqu'une nouvelle version du logiciel de traitement de texte approuvé arrive sur le marché, les règles des tribunaux et les systèmes informatiques de tous les participants peuvent nécessiter des modifications pour utiliser le nouveau format.

Le LSGB est complexe et cette complexité augmente les coûts d'analyse, de conception, de développement et de maintenance. Le coût initial d'un système LSGB peut être beaucoup plus élevé que celui d'un système reposant sur des formats exclusifs, en raison notamment de l'élaboration de la définition du type de document, et le LSGB peut nécessiter des outils logiciels supplémentaires pour en permettre l'utilisation. Toutefois, les documents LSGB sont indépendants du logiciel qui les a créés. Les outils peuvent être différents, mais les documents au coeur du système peuvent être consultés par tous les participants, que ce soit maintenant ou dans l'avenir, peu importe les outils brevetés dont ils se servent. De plus, la puissance des outils LSGB a augmenté rapidement alors que leur coût diminuait.

Bien qu'il soit simple et portable, le langage HTML n'est pas extensible et ne peut pas s'adapter à un contenu particulier. Par conséquent, comme nous l'avons indiqué précédemment, la capacité de recherche d'un document HTML particulier dans un grand dépôt central est limitée. Notons en outre que le langage HTML ne peut

accepter que les formulaires simples à remplir et les liens hypertextes unidirectionnels. Bien que chaque nouvelle version du langage HTML en augmente la capacité, les modifications logicielles permettant d'intégrer les nouvelles versions exigent du temps et des ressources. De toute façon, toutes les versions de ce langage combinent la mise en forme et le contenu dans une définition unique du type de document.

Contrairement au HTML, le XML offre un grand nombre des avantages du LSGB. Sans décrire en détail ces langages de balisage, il est préférable de choisir le XML plutôt que le HTML pour les raisons suivantes notamment : la séparation du contenu de la mise en forme, la possibilité d'utiliser des feuilles de style différentes, l'amélioration des liaisons, la liberté de définir les types de documents et l'utilisation croissante du XML dans l'industrie. Comme le XML est plus simple que le LSGB, le développement des logiciels sera également plus facile.

Malgré l'intérêt croissant que l'on porte au XML comme remplaçant du HTML, la capacité ultime de formaliser la structure des documents réside dans le LSGB. Comme il s'agit du métalangage sous-jacent à ces autres formats, l'utilisation du LSGB ouvre implicitement la porte à celle du HTML et du XML. La mise en oeuvre du LSGB par l'Office et la Commission sera compatible avec le XML. Parmi les autres formats ouverts pris en charge, mentionnons le JPEG, le MPEG et le CGM, qui permettent de stocker un éventail d'éléments graphiques et d'informations multimédias sans compromettre les exigences relatives à l'archivage. D'autres formats ouverts seront pris en charge au besoin.

8. **Comment signera-t-on les documents dans le SDÉ?**

Pendant des siècles, diverses lois ont exigé que les mots soient écrits, signés, certifiés, notariés ou même présentés dans une forme prescrite. Ces exigences ont permis de prévenir les différends sur le contenu exact de ce qui avait été dit. L'obligation de consigner par écrit n'équivaut cependant pas nécessairement à celle de signer. Un écrit peut ne pas être signé. Il permet de saisir les idées à de nombreuses fins, y compris l'utilisation à titre de preuve. Les signatures identifient et lient formellement une personne à l'écrit de façon que, en l'absence de contrefaçon, elle ne puisse renier l'écrit.

Les documents ayant une valeur juridique sont souvent signés à la main. Il semble naturel, par conséquent, d'exiger que le système informatique comporte une analogie électronique à la signature manuscrite. Avant d'aller de l'avant, toutefois, il faut d'abord noter qu'une signature manuscrite ne constitue pas l'unique moyen ou même le moyen le plus courant de conférer une valeur juridique à un document. Une signature représentant un nom écrit à la main n'est pas toujours nécessaire. Une marque comme un «X» servant de signature peut être acceptable. Un timbre ou un fac-similé peut être accepté, comme on le voit couramment sur les chèques et autres effets de commerce. Une signature créée mécaniquement peut être considérée en droit comme une signature humaine. Les tribunaux au Canada, au Royaume-Uni et aux États-Unis ont statué que les timbres mécaniques et autres signatures reproduites ont

force de loi. Même une signature illisible a été acceptée (consultez, par exemple, *R. v. Kapoor* (1989), 52 C.C.C. (3d) 41). En outre, le mandant n'est pas tenu de signer un document. Un mandataire peut le faire à sa place. Une procuration peut autoriser une personne à signer de nombreux documents. Au niveau gouvernemental, la loi peut accorder des pouvoirs de signature.

La loi a généralement fait preuve d'une souplesse suffisante pour s'adapter à la nouvelle technologie en acceptant les nouvelles formes d'écriture et de signature ou même en évitant tout simplement ce type d'exigence. Aux niveaux fédéral et provincial, l'interprétation des dispositions de la loi relatives à l'écriture tient compte depuis longtemps de divers médias, comme l'exprime l'extrait suivant :

> «écrit» Mots pouvant être lus, quel que soit leur mode de présentation ou de reproduction, notamment impression, dactylographie, peinture, gravure, lithographie ou photographie. La présente définition s'applique à tout terme de sens analogue. (*Loi d'interprétation*, L.R.C. (1985), ch. I-21, art. 2).

Comme nous l'avons indiqué ailleurs dans le présent rapport, une définition comme celle-ci peut s'avérer trop restrictive dans le cas de l'informatique, mais elle illustre la souplesse des concepts.

On a adopté des lois particulières pour éliminer les obligations relatives à l'écriture et à la signature. Le gouvernement fédéral et certaines provinces ont mis en application la Convention des Nations Unies sur les contrats de vente internationale de marchandises, qui stipule que les contrats de vente ne doivent pas obligatoirement être écrits. L'Ontario, par exemple, a éliminé cette exigence dans sa *Loi sur la vente d'objets* (L.R.O. (1990), ch. S.1; consultez également la *Loi sur la vente internationale de marchandises*, L.R.O. (1990), ch. I.10).
Dans un système informatique, comme dans un système papier, les signatures manuscrites ne constituent pas nécessairement l'unique moyen d'authentifier des documents. Selon les circonstances, il est possible de le faire au moyen d'un marquage électronique, comme l'information contenue dans une adresse électronique, d'un nom tapé dans le texte du message, d'un fac-similé de signature sous forme d'image numérique ou de processus nécessitant des mots de passe et des numéros d'identification personnelle. Dans certains systèmes de dépôt électronique, comme SEDAR (décrit ailleurs dans le présent rapport), le déposant doit conserver une feuille signée à la main à l'appui du dépôt électronique. Revenu Canada utilise une technique similaire pour les déclarations de revenus transmises par voie électronique. Le déposant, qui conserve la signature manuscrite du contribuable, agit à titre de représentant de Revenu Canada pour authentifier la déclaration.

Aux fins de l'examen de la question de la signature, on considère qu'aucune des formules mentionnées ci-dessus ne constitue une signature numérique, car il ne s'agit pas d'un concept visuel. La signature numérique résulte plutôt d'un calcul mathématique appliqué au document. Autrement dit, elle utilise un «code secret». Il n'est pas nécessaire que l'expéditeur soit mathématicien; il a simplement besoin d'un logiciel qui effectue le calcul approprié et joint la signature au document. Celle-ci ne

modifie pas le contenu du document, mais s'y ajoute. Dans certains systèmes, le code peut servir à brouiller (chiffrer) le document entier afin de le rendre confidentiel, mais le chiffrement des documents ne fait pas nécessairement partie d'un système de signatures numériques. Que le message soit chiffré ou non, une signature numérique peut néanmoins servir à déterminer si des modifications non autorisées ont été apportées au texte du message.

Le concept de signature numérique est probablement déroutant et certainement nouveau pour la plupart des gens. C'est pour cette raison qu'on en traite dans une section distincte, bien qu'il soit étroitement lié à d'autres questions, comme la sécurité des systèmes et l'admissibilité de la preuve.

Pour être efficace, le code de signature est calculé de manière qu'il identifie le signataire, que personne ne puisse le créer outre le signataire et que le destinataire du document puisse le vérifier. Il convient de noter que le logiciel du destinataire n'a pas besoin du code secret de l'expéditeur, appelé clé privée, mais seulement de la clé publique correspondante servant à vérifier la signature.

Un logiciel de signature numérique a habituellement recours à des concepts mathématiques complexes, comme les propriétés des nombres premiers, les fonctions de condensation et le chiffrement asymétrique, qui dépassent le cadre de la présente analyse. Du point de vue des utilisateurs, la signature numérique peut se résumer à l'ajout d'une chaîne de caractères inintelligibles au bas d'un message électronique. Le logiciel du destinataire traite cette chaîne de caractères pour authentifier la signature et le message. La caractéristique fondamentale d'une signature numérique, c'est qu'il est possible de l'associer à la personne qui l'a créée. Seul le détenteur de la clé privée peut produire la signature. Il n'est pas nécessairement possible d'associer à leur auteur les formes de signatures non mathématiques indiquées plus haut, comme un nom dactylographié ou un fac-similé numérique, car quiconque peut les reproduire.

Les motifs fondamentaux de l'utilisation des signatures sont plus importants que le simple aspect mécanique. Une signature sert à attester l'authenticité d'un document. Elle prouve que le signataire a approuvé le contenu du document et qu'il en accepte les conséquences. Le signataire ne peut répudier une signature valide. Tout système (papier ou électronique) doit indiquer de façon efficace qui a signé (authentification du signataire) et ce qui a été signé exactement (authentification du document) afin que les frais inhérents à l'utilisation des signatures soient minimes.

En règle générale, dans les instances de réglementation, le destinataire d'un document ne vérifie pas la signature qui y apparaît, bien qu'il puisse le faire en cas de besoin. C'est plutôt le processus au moyen duquel le document est créé et remis au destinataire qui lui confère sa valeur. Une preuve déposée au préalable, comme une prévision économique par exemple, doit être authentifiée durant l'audience. La signature qui y est apposée a peu de valeur tant qu'un témoin n'a pas attesté le document et eu l'occasion de l'expliquer, de le corriger ou de le mettre à jour.

Des procédures appropriés peuvent remplacer une signature manuscrite. En voici des exemples courants :

- la banque électronique à domicile,
- le paiement par carte de crédit au téléphone,
- l'enregistrement de valeurs mobilières en ligne,
- l'achat de valeurs mobilières auprès d'un courtier.

Chacun de ces exemples utilise différents systèmes de protection pour s'assurer qu'une personne ou son mandataire est lié par l'opération, malgré l'absence de signature manuscrite.

Comme il n'y a présentement aucune méthode formelle à l'Office et à la Commission permettant de détecter la fraude ou la contrefaçon de documents signés, le système informatique proposé ne peut augmenter de façon importante les risques à cet égard. Le système permet plutôt d'automatiser le processus de vérification des signatures. Une disposition générale relative au préjudice peut exempter un participant des exigences du système selon les circonstances.

Pour les signatures numériques, il est nécessaire d'utiliser un système à clés publiques avec des tierces personnes de confiance ou des autorités certificatrices. On peut associer une signature manuscrite à une personne en la regardant signer et en comparant des échantillons d'écriture. Une signature numérique est simplement une chaîne de chiffres. On peut l'associer à quelqu'un en demandant à un tiers de conserver des registres permettant de vérifier si la chaîne de chiffres a été attribuée à la personne qui prétend posséder la signature numérique en question. Autrement dit, un tiers peut être responsable de l'émission et de la révocation des signatures numériques et surveiller de façon générale le système.

Le projet de loi C-54 du gouvernement fédéral (traité ailleurs dans le présent rapport) prévoit des règles qui considèrent certaines technologies comme étant acceptables pour les signatures électroniques sécurisées. Certaines des questions dont on doit tenir compte dans l'élaboration de ces règles sont exprimées en ces termes :

> «Le gouverneur en conseil ne peut prévoir une technologie ou un procédé que s'il est convaincu qu'il peut être établi ce qui suit :
> a) la signature électronique résultant de l'utilisation de la technologie ou du procédé est propre à l'utilisateur;
> b) l'utilisation de la technologie ou du procédé pour l'incorporation, l'adjonction ou l'association de la signature électronique de l'utilisateur au document électronique se fait sous la seule responsabilité de ce dernier;
> c) la technologie ou le procédé permet d'identifier l'utilisateur;

d) la signature électronique peut être liée au document électronique de façon à permettre de vérifier si le document a été modifié depuis que la signature électronique a été incorporée, jointe ou associée au document.» (par. 48(2)).

Le projet de loi établit également un lien entre le concept de signature électronique sécurisée et la loi de la preuve en ces termes (consultez également la section traitant de l'authentification) :

«Le gouverneur en conseil peut prendre des règlements établissant des présomptions relativement aux documents électroniques portant une signature électronique sécurisée, y compris des règlements visant :
a) l'association de signatures électroniques sécurisées à des personnes;
b) l'intégrité de l'information contenue dans un document électronique portant une signature électronique sécurisée;
c) la manière de prouver toute question visée aux alinéas a) ou b).»(art. 31.4).

Le projet de loi C-54 fait une distinction entre les signatures sécurisées en général et la technologie particulière des signatures numériques. Il se peut aussi que l'on établisse ultérieurement par règlement d'autres technologies de signature sécurisée, comme la transmission de données biologiques. Le projet de loi définit la «signature électronique» et la «signature électronique sécurisée», cette dernière exigeant l'emploi de la technologie prescrite. Une signature électronique sécurisée satisferait également aux exigences de la loi relatives aux sceaux.

La loi proposée ferait en sorte que les documents électroniques satisfassent aux exigences des lois énumérées en annexe. Si la loi exige un document original, la version électronique nécessiterait une signature électronique sécurisée. Les déclarations faites sous serment, comme les affidavits, pourraient l'être de façon électronique au moyen de deux signatures électroniques sécurisées, soit celle de la personne qui fait la déclaration et celle de la personne autorisée à l'assermenter. De même, les documents qui doivent être signés par un témoin pourraient comporter deux signatures électroniques sécurisées, soit celle du signataire et celle du témoin.

Si les signatures sécurisées sont plus sûres que les signatures écrites, nous avons maintenant de nouvelles catégories de confiance. Dans un monde de documents papier, nous utilisons couramment la signature et occasionnellement la protection supplémentaire d'un témoin. En vertu de certaines lois, n'importe qui peut servir de témoin. D'autres lois exigent un témoin officiel, comme un commissaire à l'assermentation ou un notaire. La signature électronique sécurisée fait intervenir un nouveau type de témoin, soit l'autorité certificatrice. Certaines situations pourraient toujours exiger l'équivalent électronique d'un affidavit, mais, dans bon nombre de cas, une seule signature sécurisée pourrait suffire. Par exemple, la présence d'un témoin impartial peut s'avérer nécessaire pour confirmer l'état mental du signataire. Cependant, lorsque le témoin impartial ne fait que confirmer la signature du document sans vérifier les intentions du signataire, seule une signature sécurisée pourrait être nécessaire. En d'autres mots, l'idée de la signature numérique d'un témoin soulève la question suivante : de quoi la seconde signature témoigne-telle?

Les systèmes qui traitent les signatures électroniques sont complexes. L'une des façons les plus efficaces de passer du papier aux documents électroniques consiste alors à éliminer toute signature inutile. Les règles de l'Office et de la Commission devraient peut-être faire l'objet d'un examen pour s'assurer que les signatures ne sont pas exigées simplement parce qu'elles l'ont toujours été. Par exemple, la signature sous serment des affidavits et des documents notariés peut constituer un moyen de relier des sanctions pénales au dépôt de faux. Le même objectif peut être atteint au moyen d'une règle ou d'un règlement général autorisant l'utilisation de systèmes informatiques pour produire des signatures, accompagné de sanctions pour le dépôt de faux, sans exiger des serments distincts pour chaque document (consultez, par exemple, les Règles de l'assurance-emploi DORS/96-332, art. 90, 91).

9. **Les documents du SDÉ seront-ils conformes aux règles de preuve?**

La preuve sur laquelle la décision d'un tribunal se fonde doit être pertinente et fiable. Si elle n'est pas pertinente, elle ne peut pas aider le décideur. Si elle n'est pas fiable ou s'il n'existe aucun moyen d'en déterminer la fiabilité, elle ne peut pas servir à établir les faits entourant la cause. Toute preuve inappropriée ou douteuse est tout simplement rejetée ou admise sans toutefois être prise en compte dans la décision. Dans le cas du SDÉ proposé, la question consiste alors à déterminer s'il fournira des preuves pertinentes, fiables et admissibles.

Parmi les diverses catégories de preuves utilisées pour démontrer le bien-fondé d'une cause, comme le témoignage oral, la preuve écrite, la preuve matérielle, etc., c'est la preuve documentaire qui s'avère la plus pertinente à l'égard du SDÉ proposé. Avant qu'un document puisse être admis en preuve et versé au dossier, il doit passer plusieurs épreuves. Par exemple, il faut l'authentifier, c'est-à-dire démontrer qu'il est authentique. La soi-disant règle de la meilleure preuve nécessite également le document original s'il est disponible. Ces règles de preuve, entre autres, comportent de nombreuses exceptions. Les documents très anciens, par exemple, sont généralement considérés comme étant authentiques.

Les documents informatiques sont admissibles en cour à titre de preuves documentaires en vertu des principes de la *common law.* En outre, il existe une disposition législative spécifique pour les documents, y compris les documents informatiques, créés dans «le cours ordinaire des affaires» (*Loi sur la preuve au Canada*, L.R.C. ch. C-5, art. 30, *Loi sur la preuve*, L.R.O. (1990), ch. E.23, art. 35).

Les termes employés dans la *Loi sur la preuve au Canada* ne précisent pas la façon de s'assurer de l'admissibilité des documents informatiques. Même s'ils sont admissibles, il n'existe aucune norme particulière permettant de s'assurer que le tribunal y accordera l'importance voulue dans ses délibérations. Les tribunaux examineront l'ensemble des circonstances relatives à la création des documents. En règle générale, l'admissibilité et l'importance des documents informatiques dépendent de la fiabilité des processus de saisie, de mise en mémoire et de récupération de l'information :

> «La nature et la qualité de la preuve présentée au tribunal doivent refléter les faits entourant l'ensemble du processus de tenue des dossiers et, dans le cas des documents informatiques, des méthodes et procédés relatifs à la saisie des données, à la mise en mémoire ou à l'information ainsi qu'à sa récupération et à sa présentation» (*R. c. McMullen* (1979) 47 CCC (2d) 499 à 506, 25 OR (2d) 301, 100 DLR (3d) 671).

Autrement dit, il n'existe aucun moyen de *garantir* qu'un document informatique particulier sera admissible et qu'on y accordera l'importance voulue. Évidemment, un tribunal de réglementation n'est pas une cour de justice soumise à toutes les nuances de la loi sur la preuve.

De toute façon, l'enquête dans un différend sur la validité des documents du SDÉ ne porterait pas essentiellement sur une feuille de papier ou un document informatique donné. Elle porterait sur le système de tenue de dossiers qui a produit le document. C'est donc dire que le SDÉ, soit l'ensemble du processus de tenue de dossiers dont il est question ci-dessus, doit être fiable et satisfaire aux normes de l'industrie.

Bien que les lois fédérale et provinciales sur la preuve fassent référence aux documents informatiques, elles ne font pas de distinctions subtiles, comme la différence entre l'imagerie et la reconnaissance optique des caractères. Le systèmes d'imagerie copient les documents sans séparer les parties distinctes de l'image en lettres et en chiffres. L'imagerie peut comporter des erreurs qui se produisent durant la saisie de l'image et à cause de la capacité limitée des systèmes numériques. C'est-à-dire que les images du monde réel peuvent contenir plus d'information qu'il n'est possible d'en saisir dans un espace de stockage raisonnable dans le monde numérique. Contrairement à l'imagerie, la reconnaissance optique des caractères tente de séparer les parties significatives de l'image, mais elle prête à interprétation, comme par exemple, est-ce qu'un point est un signe de ponctuation ou simplement une tache sur l'image? On crée encore une autre forme de document informatique en copiant un fichier d'un disque à un autre. À moins de vérifier la copie octet par octet, on ne peut pas supposer qu'elle soit exacte, même si elle l'est habituellement. Ces différentes façons de créer de tels documents sont regroupées sous la rubrique documents informatiques. Cependant, leur fiabilité varie. Il est possible de vérifier l'exactitude du dernier type de copie, mais peu d'utilisateurs de la reconnaissance optique des caractères pourraient s'attendre à un texte parfait chaque fois. L'imagerie se situe quelque part au milieu de l'échelle de la fiabilité selon la qualité des documents papier originaux, le perfectionnement du matériel d'imagerie, les algorithmes d'imagerie utilisés (p. ex., sans perte ou compression avec perte) ainsi que la taille et le format des images stockées. (À cet égard, il convient de remarquer que Revenu Canada a publié une circulaire d'information dans le but d'inclure l'imagerie comme méthode de conservation des dossiers fiscaux. Consultez la Circulaire d'information 78-10R2SR du 10 février 1995, qui exige que les dossiers soient conservés conformément aux normes établies dans le document intitulé «Microfilms et images électroniques - preuve documentaire» (CAN/ONGC - 72.11-93) de l'Office des normes générales du Canada.

En ce qui a trait aux copies, il n'y a aucun moyen d'être certain de ce qu'un tribunal dirait au sujet de la destruction d'originaux utilisés pour créer des documents informatiques. Si la destruction fait partie du cours ordinaire des affaires, les

documents pourraient alors réussir cette épreuve. Dans le cas contraire, elle pourrait être considérée comme une entrave et une supercherie (consultez également la section traitant des questions d'exercice professionnel). La *Loi sur la preuve* comporte des dispositions particulières concernant la destruction de documents signés que l'on a photographiés (c'est-à-dire microfilmés), mais n'inclut pas de façon précise les documents numériques (*Loi sur la preuve au Canada*, L.R.C. (1985), ch. C-5, art. 31, *Loi sur la preuve*, L.R.O. (1990), ch. E.23, art. 34).

D'autres principes pourraient s'appliquer en matière de preuve outre le cours ordinaire des affaires mentionné ci-dessus. La nécessité de soumettre des faits exacts au tribunal sous-tend tout le droit de la preuve. Pour satisfaire à cette exigence, les tribunaux préfèrent :

- des documents réalisés à la même époque que les événements qu'ils décrivent (car la mémoire humaine oublie);

- des documents fondés sur la connaissance personnelle (et non sur des ouï-dire potentiellement douteux);

- des faits et non des opinions (la phrase familière «seulement les faits, s. v. p.», laissant les opinions aux experts et au tribunal);

- des documents originaux plutôt que des copies (principe qui a vu le jour dans un monde de documents papier où les copies ne sont pas identiques aux originaux);

- des documents réalisés de façon régulière et parce que la personne y était obligée (pas des document préparés à des fins intéressées).

Il arrive souvent que les systèmes informatiques ne puissent pas satisfaire à ces normes apparemment simples. Comme nous l'avons indiqué précédemment, les ordinateurs sont impersonnels. Les fichiers sont souvent tenus à jour et manipulés par une personne qui ne sait rien de leur création. Il est possible de les récupérer de nombreuses années après la survenance des événements enregistrés. Les fichiers d'un système informatique peuvent être un amalgame d'informations créées au sein d'une organisation et de renseignements provenant d'autres systèmes informatiques échappant au contrôle, à la connaissance ou à la responsabilité d'une seule personne. Les faits stockés dans un ordinateur peuvent faire partie d'un système logiciel servant à les manipuler, comme dans le cas d'un tableur pouvant produire d'innombrables variations à partir des mêmes données. Il est clair que la loi sur la preuve devra évaluer pour tenir compte de l'archivage des documents électroniques.

La Conférence sur l'uniformisation des lois au Canada a récemment approuvé une ébauche de la *Loi sur la preuve électronique*. Ce document traite de nombreuses questions concernant la preuve, comme l'authentification, la règle de la meilleure preuve et les procédures courantes. Pour obtenir de plus amples renseignements, consultez le site http://www.law.ualberta.ca/alri/ulc/current/eueaa.htm.

En vertu du projet de loi C-54 du gouvernement fédéral, traité ailleurs dans le présent rapport, un document électronique pourrait satisfaire aux exigences des lois fédérales mentionnées en annexe qui exigent des copies. Le projet règle les questions relatives aux documents originaux en considérant que les documents électroniques sont satisfaisants si «le document électronique comporte une signature électronique sécurisée, ajoutée lors de la production originale du document électronique dans sa forme définitive, pouvant être utilisée pour établir que le document électronique n'a pas été modifié depuis». Cet énoncé peut prêter à diverses interprétations, y compris ce qu'on entend par «production originale» et «forme définitive», avec toutes les versions intermédiaires possibles.

Le projet de loi C-54 traite des questions relatives à l'authentification et à la meilleure preuve en ces termes :

> «31.2 (1) Tout document électronique satisfait à la règle de la meilleure preuve dans les cas suivants :
> a) la fiabilité du système d'archivage électronique au moyen duquel ou dans lequel le document est enregistré ou mis en mémoire est démontrée;
> b) une présomption établie en vertu de l'article 31.4 s'applique.
> (2) Malgré le paragraphe (1), le document électronique sous forme de sortie imprimée satisfait à la règle de la meilleure preuve si la sortie imprimée a de toute évidence ou régulièrement été utilisée comme document relatant l'information enregistrée ou mise en mémoire.
> 31.3 Pour l'application du paragraphe 31.2(1), le système d'archivage électronique au moyen duquel ou dans lequel un document électronique est enregistré ou mis en mémoire est réputé fiable, sauf preuve contraire, si, selon le cas :
> a) la preuve permet de conclure qu'à l'époque en cause, le système informatique ou autre dispositif semblable fonctionnait bien, ou, dans le cas contraire, son mauvais fonctionnement n'a pas compromis l'intégrité des documents électroniques, et qu'il n'existe aucun motif raisonnable de mettre en doute la fiabilité du système d'archivage électronique;
> b) il est établi que le document électronique présenté en preuve par une partie a été enregistré ou mis en mémoire par une partie adverse;
> c) il est établi que le document électronique a été enregistré ou mis en mémoire dans le cours ordinaire des affaires par une personne qui n'est pas partie à l'instance et qui ne l'a pas enregistré ni ne l'a mis en mémoire sous l'autorité de la partie qui cherche à le présenter en preuve.
> 31.4 Le gouverneur en conseil peut prendre des règlements établissant des présomptions relativement aux documents électroniques portant une signature électronique sécurisée, notamment des règlements visant :
> a) l'association de signatures électroniques sécurisées à des personnes;
> b) l'intégrité de l'information contenue dans un document électronique portant une signature électronique sécurisée;
> c) la manière de prouver toute question visée aux alinéas a) ou b).
> 31.5 Afin de déterminer si, pour l'application de toute règle de droit, un document électronique est admissible, il peut être présenté un élément de preuve relatif à toute norme, toute procédure, tout usage ou toute pratique touchant la manière

d’enregistrer ou de mettre en mémoire un document électronique, eu égard au type de commerce ou d’entreprise qui a utilisé, enregistré ou mis en mémoire le document électronique ainsi qu’à la nature et à l’objet du document.»

La juxtaposition du droit de la preuve et des ordinateurs soulève de nombreuses questions. Au fur et à mesure que les institutions gouvernementales confieront leurs documents aux ordinateurs, les questions traitées dans la présente section seront résolues. Entre-temps, la conception du SDÉ tient compte de ces questions, y compris celles qui sont sans réponse.

10. Quelle sera l’incidence du SDÉ sur les renseignements confidentiels déposés auprès de l’Office et de la Commission?

On peut fournir des renseignements commerciaux confidentiels à l’Office et à la Commission (comme ceux indiqués à l’article 16.1 de la *Loi sur l’Office national de l’énergie* ou à la partie VII de la *Loi sur la Commission de l’énergie de l’Ontario*, 1998). D’autres principes d’application générale, comme les obligations fiduciaires, peuvent également s’appliquer comme ils le font présentement. On ne prévoit pas que le SDÉ proposé aura une incidence sur la confidentialité. Les différences entre le système de documents papier existant et le SDÉ proposé sont principalement liées à la sécurité informatique par rapport à la sécurité existante, traitée ailleurs dans le présent rapport.

11. Quelle sera l’incidence du SDÉ sur la justice naturelle et l’équité de la procédure?

Les concepts de justice naturelle et d’équité de la procédure permettent de faire en sorte que les parties concernées connaissent la cause qui sera entendue et qu’elles puissent présenter leurs preuves et leurs arguments devant un tribunal impartial. Les normes de procédure particulières qui permettront de s’en assurer dépendent de nombreux facteurs, dont le type de tribunal et les conséquences de la décision. Les tribunaux ont statué que les concepts d’équité et de justice naturelle ne devaient pas nécessairement s’appliquer à chaque tribunal, mais plutôt selon les circonstances. Les différents types de tribunaux accomplissent différentes choses, de la détermination des droits individuels, d’une part, aux recommandations de principe de portée générale, d’autre part. On applique des règles de procédure moins strictes aux questions de principe. On a rédigé de nombreux traités volumineux sur ces concepts qui ne feront pas l’objet d’une définition plus approfondie dans le présent rapport.

Dans la mesure où le SDÉ correspond simplement à l’automatisation de la création, de la transmission, de la mise en mémoire et de la récupération de documents, il ne devrait avoir aucun effet sur les normes de procédure. Autrement dit, l’Office et la Commission continueront de tenir des audiences, de prendre des décisions, etc. Cependant, plusieurs aspects du SDÉ méritent des remarques particulières.

La première a trait à la question de l'équité envers les personnes, les petits groupes d'intervenants et ceux qui n'utilisent pas les ordinateurs présentement. Est-ce qu'un système reposant sur l'utilisation de l'informatique aura pour effet d'exclure des gens? Non.

La plupart des participants aux instances de l'Office et de la Commission sont représentés par des avocats qui ont accès aux ordinateurs. Un sondage mené auprès d'eux indique qu'ils utilisent différents types de systèmes informatiques. On a procédé au sondage au début des étapes de planification du SDÉ et il ferait certainement état d'un perfectionnement technique encore plus poussé aujourd'hui. Il y a aussi des intervenants non représentés, principalement préoccupés par des questions comme la construction sur leur propriété, et un plus grand nombre de personnes non représentées qui n'interviennent pas, mais qui présentent leurs points de vue en transmettant leurs commentaires par la poste.

Quiconque participe aux audiences en vertu du présent système doit être en mesure de lire l'une ou l'autre des langues officielles, de respecter les règles de l'Office et de la Commission et de communiquer par courrier ou par télécopieur ou d'assister en personne. Ces exigences ne sont pas perçues comme étant injustes. Le système proposé crée peu de changements à cet égard. Il est possible de convertir les documents papier sous une forme électronique compatible avec les normes de l'Office et de la Commission. Même si une personne ne possède qu'un stylo et du papier ou une machine à écrire, elle peut soumettre un document papier et le SDÉ peut mettre en mémoire une version numérique de ce dernier.

Réciproquement, pour aider le public à obtenir des documents stockés dans le système, on mettra des ordinateurs à sa disposition pour permettre la recherche en ligne. Est-ce que cela exclut les citoyens qui ne savent pas comment chercher des documents dans un système informatique? Le régime actuel sert toujours de base de référence à la comparaison. Les gens savent-ils comment trouver des documents dans le système actuel? Ils doivent prendre le temps de comprendre les règles, le processus et les documents papier. Les rapports d'étape et les études sur le SDÉ laissent entendre que la récupération des documents sera grandement améliorée avec le système proposé. De plus, le tribunal a le pouvoir de réglementer ses procédures et, en particulier, d'exiger que l'information soit déposée avec des index, des résumés, des renvois et autres techniques pouvant réduire la complexité des causes même les plus considérables.

Il convient aussi de se demander si l'utilisation de l'informatique éloignera encore plus l'Office et la Commission du public. Les ordinateurs ne sont désormais plus des outils spécialisés conçus pour les experts — pas à une époque où les enfants des écoles publiques utilisent Internet en classe, où les compagnies de téléphone et de câblodistribution font en sorte que le courrier électronique soit aussi répandu que le téléphone et la télévision, et où de nombreux organismes gouvernementaux annoncent leurs sites Web. Le SDÉ proposé rapprochera l'Office et la Commission de la population à de nombreux égards : l'accès à l'information s'améliorera, grâce non seulement à la recherche automatisée, mais aussi à l'uniformisation accrue du dépôt des documents et du marquage des mots clés. Le SDÉ peut également fournir aux

personnes handicapées des formes d'accès qui ne leur sont pas offertes présentement, y compris l'informatique hors site, l'affichage à gros caractères, le braille et la synthèse vocale. Le SDÉ rapprochera l'Office et la Commission des participants situés en région éloignée.

En fait, l'accès électronique peut ouvrir les portes de l'Office et de la Commission à de nouveaux publics. Un dépôt central de documents électroniques peut fournir de l'information publique à toute personne reliée à Internet. Les gens ont toujours pu consulter les documents publics, mais seulement aux bureaux de l'Office et de la Commission. L'information accessible et consultable instantanément est un nouveau phénomène, peut-être même une nouvelle catégorie d'information publique.

Il se peut qu'il faille revoir les règles actuelles de pratique et de procédure pour les adapter au SDÉ. Elles sont présentement conçues pour un monde de documents papier. Il faudra réexaminer, par exemple, des mots comme «original» et «copie» dans le contexte du dépôt électronique. Les règles, les directives et les procédures devront évidemment tenir compte des droits et des besoins des participants qui ne possèdent pas d'ordinateur ou qui ont de la difficulté à les utiliser. L'Office et la Commission fourniront un accès à toute personne, selon les besoins, par le biais des ordinateurs ou des documents papier classiques. Ceux qui ne possèdent pas d'ordinateur ne seront pas laissés pour compte.

La question des avis est un aspect qui mérite une attention particulière. La justice naturelle et l'équité de la procédure exigent que les parties éventuelles soient averties de la tenue des audiences de l'Office et de la Commission. Le défaut de fournir un avis raisonnable peut invalider une décision. Il n'est pas nécessaire de remettre en main propre un avis rédigé sur papier (consultez également la section traitant, de façon générale, de la signification des documents). Au contraire, comme il y a énormément de gens concernés, l'Office et la Commission publient habituellement leurs avis d'audience dans les journaux. Aucun tribunal canadien n'a statué sur l'utilisation d'un site Internet ou du courrier électronique pour avertir le public de la tenue des audiences. Par analogie avec des décisions déjà rendues, cependant, il est probable qu'un tribunal cherchera à savoir si les moyens électroniques utilisés pour signifier les avis sont raisonnables dans les circonstances. Jusqu'à ce que l'utilisation d'Internet et de la technologie informatique devienne aussi courante que la lecture des quotidiens, toutefois, l'Office et la Commission continueront d'employer les moyens classiques, outre les moyens électroniques, pour aviser le public.

12. **Comment les documents seront-ils signifiés avec le SDÉ?**

Aujourd'hui, on crée la plupart des documents de façon électronique au moyen de logiciels de traitement de textes ou d'autres applications comme les tableurs et les logiciels de courrier électronique. Ils sont ensuite imprimés, déposés et signifiés sous forme de papier aux parties à l'audience. Certains participants peuvent alors numériser le document afin d'en faciliter la mise en mémoire, la recherche et la récupération sous

forme électronique. Le dépôt central des documents du SDÉ peut éliminer certaines de ces conversions et permettre l'extraction des documents du système, au besoin.

Dans un système papier, les documents sont non seulement déposés auprès du tribunal, mais également signifiés aux parties intéressées. Le dépôt et la signification permettent de s'assurer que les parties savent que des documents existent et qu'elles y ont accès. De plus, elles ne peuvent pas prétendre qu'elles ignoraient l'existence des documents déposés. Voilà un exemple où tous les documents sont toujours remis à toutes les parties, peu importe leurs intérêts particuliers dans l'instance en question.

Dans un système électronique, l'automatisation permet différents types de signification ou son élimination complète. Les parties peuvent passer l'information au crible en fonction de leurs propres intérêts. Elles peuvent recevoir des documents par courrier électronique. Ou, plutôt que de recevoir des documents complets, elles peuvent simplement être avisées que certains documents ont été déposés. Elles pourraient alors extraire des documents du dépôt central, au besoin. Elles pourraient encore se passer complètement de la signification et vérifier la présence de nouveaux documents dans le dépôt central soit manuellement, soit au moyen d'un logiciel automatique à la recherche des mises à jour périodiques.

Aucun tribunal canadien n'a statué sur la légalité de la signification des documents numériques ou l'élimination complète de la signification au profit de l'extraction des documents. Compte tenu de la jurisprudence relative aux technologies, comme le télécopieur et le télégraphe, un tribunal aurait tendance à examiner la technologie en question et les circonstances. De toute façon, l'Office et la Commission ont le pouvoir de modifier leurs règles de procédure, ils ne sont pas liés par les exigences procédurales des tribunaux et ils ont prescrit leur propres règles en matière de dépôt et de signification (Règles de pratique et de procédure de l'Office national de l'énergie, 1995, DORS/95-208, art. 8 et 9, Commission de l'énergie de l'Ontario - Règles de pratique et de procédure, février 1997, art. 11 et 20).

Comme dans le cas du système de documents papier actuel, si les parties connaissent tous les documents déposés et qu'elles y ont accès, compte tenu de dispositifs de protection appropriés, comme les messages d'accusé de réception, il serait alors possible d'atteindre les objectifs de la signification des documents par voie électronique. Bien qu'aucune spécification finale n'ait été précisée, le SDÉ est conçu de façon à réaliser ces objectifs.

13. L'Office et la Commission ont-ils tenu compte de l'incidence du SDÉ sur la pratique du droit?

Voici des déclarations d'avocats publiées dans *La revue des juristes de l'Ontario*, en février 1997, par le Barreau du Haut-Canada, qui régit la pratique du droit en Ontario :

> «La pratique du droit est très conservatrice.... nous ne serons pas les premiers à vouloir déterminer l'admissibilité d'un document électronique en cour.»

> «C'est comme retourner vers le passé, mais je ne me sens pas à l'aise face à ce monde entièrement électronique si ma carrière doit reposer sur le fait que la télécopie que j'ai envoyée à partir de mon ordinateur a été effectivement transmise.»

Les questions relatives à la pratique du droit comprennent la nécessité de déterminer si les instructions des clients doivent être signées sur papier. Des directives transmises par courrier électronique pourraient-elles suffire? Le cas échéant, pendant combien de temps faudrait-il conserver les vieux messages électroniques? Certains avocats peuvent croire que seuls les documents papier peuvent les protéger contre les réclamations pour faute professionnelle et qu'il faut conserver tous les documents à perpétuité. Ce genre de questions entre avocats et clients n'aboutît généralement pas devant un tribunal de réglementation. Néanmoins, des avocats comme ceux cités ci-dessus peuvent croire qu'ils doivent échanger du papier et non des électrons par excès de prudence.

D'ici la mise en oeuvre complète du SDÉ, on prévoit que les avocats utiliseront les ordinateurs dans d'autres secteurs de leurs activités et qu'ils auront adopté des politiques en matière de documents électroniques et d'archivage. Entre-temps, toute mise en oeuvre du SDÉ devra tenir compte dans une certaine mesure des responsabilités professionnelles des avocats par rapport à la tenue des dossiers.

14. Cela signifie-t-il que l'Office et la Commission ont répondu à toutes les questions au sujet du SDÉ?

Non. Le SDÉ est nouveau. D'ici à ce qu'il soit mis en oeuvre et testé, il y aura naturellement des questions et des problèmes à résoudre. Comme nous l'avons indiqué au début, de nombreuses questions seront résolues lorsque la nouvelle technologie sera mieux connue au fil du temps. Si des questions demeurent sans réponse, l'Office et la Commission accueilleront volontiers les commentaires et les suggestions.

15. Annexe A : Autres organismes et gouvernements

Bien que le SDÉ et les questions qui en découlent soient nouveaux dans la réglementation de l'énergie au Canada, l'Office et la Commission ne sont pas seuls. D'autres organismes et gouvernements passent également des documents papier aux systèmes électroniques.

Exemples du gouvernement fédéral canadien

Le gouvernement du Canada a mis en place de trop nombreux programmes électroniques pour pouvoir tous les énumérer ici (on peut en consulter la liste à http://www.gc.ca/programs/pgrind_f.html). Elle comprend :

AGENCE CANADIENNE D'ÉVALUATION ENVIRONNEMENTALE (ACÉE)

L'Agence canadienne d'évaluation environnementale, en vertu de l'article 55 de la *Loi canadienne sur l'évaluation environnementale,* tient un registre public. Ce dernier a pour objet de faciliter l'accès du public aux documents concernant les évaluations environnementales et d'assurer un accès convenable à la population. Le registre public comprend l'Index fédéral des évaluations environnementales, une liste de documents du ministère et des documents.

OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA (OPIC)

L'Office de la propriété intellectuelle du Canada permet les recherches en ligne dans la Base de données sur les brevets canadiens. Voici la description qu'en donne le site Internet :

> «La Base de données met à votre disposition la description et la reproduction des documents de brevets déposés au cours des soixante-quinze dernières années. Vous pouvez rechercher, interroger et étudier plus de 1 400 000 documents de brevets.»

L'OPIC offre également la Base de données sur les marques de commerce canadiennes, qui est décrite ainsi :

> «vous offre maintenant accès à la Base de données sur les marques de commerce canadiennes. L'information qui se trouve dans cette base de données peut inclure des dessins de marques de commerce, les marchandises et services, les noms des propriétaires et plus.»

SIGNATURES NUMÉRIQUES

Le gouvernement fédéral utilise déjà la technologie des signatures numériques, comme dans le cas d'une nouvelle application décrite en ces termes :

> Le 5 juin 1998, M. Mah Bow Tan, ministre des communications de Singapour, a utilisé une signature numérique pour signer un protocole d'entente entre son pays, le Canada et l'État de la Pennsylvanie. La signature a eu lieu lors d'une réunion de l'Organisation de coopération économique Asie-Pacifique sur l'industrie des télécommunications et de l'information. M. John Manley, ministre canadien de l'Industrie, et M. Tom Ridge, gouverneur de la Pennsylvanie, qui n'étaient pas présents à la réunion, avaient signé le document au préalable au moyen de la technologie des clés privées. Des représentants ont remis les documents ainsi signés au ministre Mah selon le cérémonial d'usage durant la réunion. Il a ensuite inséré une carte à puce contenant sa signature dans le lecteur et tapé son mot de passe pour «signer» le document. Les trois signatures ont ensuite fait l'objet d'une authentification pour créer un document officiel. Ce premier document gouvernemental international signé de façon numérique crée un consortium d'apprentissage mondial entre les deux pays et l'État pour promouvoir l'utilisation de la technologie des télécommunications et de l'information en éducation par l'intermédiaire d'un site Web commun. (http://www.tas.gov.sq)

Exemples de l'Ontario

En Ontario, parmi les premiers exemples d'utilisation des systèmes électroniques, mentionnons l'enregistrement des sûretés mobilières, l'enregistrement des noms commerciaux, l'enregistrement des titres fonciers, les procédures régissant les procès civils et les dépôts auprès de la Commission des valeurs mobilières.

MINISTÈRE DU PROCUREUR GÉNÉRAL DE L'ONTARIO

Un projet pilote autorisé en vertu de la *Loi sur les tribunaux judiciaires* (Règlement de l'Ontario 223-97) permet aux avocats de déposer un nombre limité de documents au civil par voie électronique. Le dépôt électronique fait partie d'un projet plus important de gestion des causes civiles au moyen d'un logiciel privé appelé Sustain permettant d'entrer les réclamations, de planifier les causes et de produire des rapports statistiques. Seuls les cabinets d'avocats et les services juridiques ayant reçu une formation sur l'utilisation du logiciel prescrit peuvent y participer. Dans le cadre du projet pilote, un avocat utilise le logiciel client Sustain pour créer, puis envoyer par voie électronique un fichier de traitement de texte d'une page au greffe du tribunal. Le logiciel vérifie le formulaire, débite les droits de dépôt directement du compte de l'avocat, émet un numéro de référence et envoie un reçu à l'avocat. Il est possible de signifier des documents entre les procureurs participants par l'intermédiaire du système informatique. Les formulaires prescrits ne nécessitent pas de signature, bien que l'avocat doive conserver une preuve signée de la signification. L'accès public aux documents déposés sera initialement offert par le biais des terminaux du tribunal et, ultérieurement, par accès à distance et on produira également des copies papier au besoin. Les plans à long terme, qui ne font pas partie du projet pilote, comprennent le dépôt des motions et des dossiers des procès en plus des documents simples d'une page.

Le système Sustain, contrairement au SDÉ, utilise des logiciels et des formats de données exclusifs. Un consortium de sociétés, dont Microsoft, fait la promotion du logiciel comme moyen d'établir des liens électroniques entre les avocats et les tribunaux. Le projet ministériel est également associé à un processus distinct de gestion des tribunaux administratifs.

MINISTÈRE DE LA CONSOMMATION ET DU COMMERCE

En partenariat avec une société privée, Teranet, le ministère de la Consommation et du Commerce a mis au point un système électronique d'actes translatifs de propriété. Le ministère possède également un système électronique permettant de déposer les enregistrements de sûretés mobilières et un système pour l'enregistrement des noms commerciaux. Plus de 90 % des enregistrements de sûretés mobilières et 30 % des enregistrements de noms commerciaux en Ontario sont déposés par voie électronique. Ces systèmes utilisent des logiciels et des formats de données exclusifs. Dans la plupart des cas, seules les personnes désignées peuvent y participer. En vertu des règlements régissant ces systèmes, il n'est pas nécessaire que les documents soient signés. Contrairement au SDÉ, ces registres ne sont pas principalement destinés à la gestion des documents aux fins d'audiences et de décisions.

Exemple pancanadien

AUTORITÉS CANADIENNES DE RÉGLEMENTATION DES VALEURS MOBILIÈRES

Les autorités canadiennes de réglementation des valeurs mobilières ont adopté un système de dépôt électronique, le Système électronique de données, d'analyse et de recherche (SEDAR), qui a été mis au point afin de :

> «faciliter le dépôt électronique de l'information reliée à la réglementation des valeurs mobilières (prospectus, documents d'information continue, etc.) et le paiement des droits de dépôt aux autorités canadiennes de réglementation des valeurs mobilières;
>
> faciliter la diffusion publique de l'information reliée à la réglementation des valeurs mobilières rassemblée dans le cours du processus de dépôt;
>
> faciliter les communications électroniques (courrier électronique, etc.) entre les déposants par voie électronique, les agents de dépôt et les autorités en valeurs mobilières.»
> (Manuel du déposant SEDAR)

À moins de circonstances exceptionnelles, tous les documents déposés doivent maintenant être présentés sous forme électronique. Contrairement au SDÉ proposé, SEDAR n'utilise pas le langage standard généralisé de balisage (LSGB). Tous les documents SEDAR doivent être réalisés au moyen de l'un des trois formats exclusifs suivants : WordPerfect, Microsoft Word ou Adobe PDF.

Exemples des États-Unis

RULENET

RuleNet, une expérience innovatrice menée par la Nuclear Regulatory Commission (NRC) des États-Unis, était un forum électronique d'élaboration de règlements sur Internet. L'expérience visait à faire participer le public à la préparation de règles fondées sur le rendement en matière de protection contre l'incendie. Toute personne pourvue d'un navigateur Web pouvait observer, formuler des commentaires et accéder à des documents connexes. (http://nssc.llnl.gov/RuleNet/Help/Info.html)

FEDERAL COMMUNICATIONS COMMISSION (FCC)

En avril 1997, la FCC a lancé son initiative de dépôt électronique au moyen d'un avis de projet de réglementation (FCC 97-113) :

> Dans cet avis de projet de réglementation (avis), nous proposons de permettre aux parties de déposer leurs commentaires par voie électronique dans le cadre de toutes les instances (avis et commentaires) informelles de la FCC relatives à l'élaboration des règlements en vertu de l'article 553 du *Administrative Procedure Act*, sauf en ce qui a trait aux procédures d'attribution en matière de radiodiffusion. Ces dépôts électroniques se verront accorder un traitement et une importance identiques à ceux des commentaires déposés au moyen de documents papier. Nous avons conclu provisoirement que cette initiative permettra au public de communiquer ses points de vue beaucoup plus facilement à la Commission et d'analyser les commentaires que d'autres ont déposés. Nous croyons que le dépôt électronique permettra également à la Commission d'améliorer l'efficacité de ses propres processus au bénéfice du public.

AUTRES ORGANISMES UTILISANT LE LSGB

Voici une liste provenant de la page Web du LSGB (http://www.oasis-open.org/cover/ de novembre 1998) présentant les projets LSGB en cours dans les secteurs publics et privés :

- Office of Scientific and Technical Information (OSTI) du Department of Energy (DOE) des États Unis;

- IRS (Internal Revenue Service des États-Unis);

- National Library of Medicine (NLM);

- Library of Congress - Encoded Archival Description (EAD) (description des archives codées) - Finding Aid Pilot Project (projet pilote sur les instruments de recherche);

- Automotive and Truck Standard SAE J2008 (et T2008);

! Base de données SEC EDGAR;

! IETM (Interactive Electronic Technical Manuals) (manuels techniques électroniques interactifs);

! TCIF/IPI (Telecommunications Industry Forum Information Products Interchange) (échange réciproque de produits d'information sur les forums de l'industrie des télécommunications);

! Electronic Component Information Exchange (ECIX) (échange d'information sur les composants électroniques) - Pinnacles Component Information Standard (PCIS) (norme d'information sur les composants Pinnacles);

! Définitions des types de documents de l'Association du transport aérien;

! Railroad Industry Forum: Electronic Parts Catalog Exchange Standard (EPCES) (forum de l'industrie ferroviaire : norme d'échange des catalogues de pièces électroniques);

! CALS : Soutien continu des acquisitions et de leurs cycles de vie (anciennement : Groupe de travail - Acquisition et soutien logistique assisté par ordinateur; récemment : Commerce à la vitesse de la lumière);

! USAF SGML Repository (dépôt central des documents en LSGB des forces aériennes américaines);

! Norme militaire 2167A : FOSI et définitions des types de documents relatifs à la norme militaire 2167A;

! Documents MIL-M-28001B en LSGB(site des forces navales);

! Army SGML Registry and Library (ASRL) (registre et bibliothèque LSGB de l'armée);

! Technologie de recherche d'information du gouvernement - GIFT (Canada).

16. **Annexe B : Autres documents à consulter**

Aspects of Public Policy Regarding Crown Copyright in the Digital Age, W.T. Stanbury, 10 *Intellectual Property Journal* 131, mai 1996

Copyright and Confidential Information Law of Canada, G. F. Henderson édit., 1995, Carswell

Copyright and the State in Canada and the United States, David Vaver, 10 *Intellectual Property Reports* 187, mai 1996

Copyright in Legal Documents, David Vaver, 1993 *Osgoode Hall Law Journal*, vol. 31, n° 4, p. 662

Crown Copyright In Canada: A Legacy Of Confusion, Barry Torno, 1981, ministre des Approvisionnements et Services

Essentials of EDI Law, Peter Jones, Conseil canadien de l'échange électronique de données, 1992

The Internet Changes Everything: Revolutionizing Public Participation and Access to Government Information Through the Internet, Stephen M. Johnson, *Administrative Law Review*, 50:2, printemps 1998, pp. 277 et suivantes;

Management of Recorded Information, Directive 7-5-8, juin 1992, Conseil de gestion du gouvernement (Ontario)

Microfilms et images électroniques - preuve documentaire, CAN/ONGC - 72.11-93, Office des normes générales du Canada

La revue des juristes de l'Ontario, janvier/février 1997, vol. 1, n° 1, Barreau du Haut-Canada

Open Access Same-Time Information System, 18 CFR Part 37, 24 avril 1996, Federal Energy Regulatory Commission (FERC)

Policy, Practice and Who Gets to Own the Crown's Jewels: The Ownership of Intellectual Property in Crown Contracts, Martin P. J. Kratz, 10 C.I.P.R. 613

Practitioner's Guide to Electronic Filing in Utah Courts, 27 avril 1995, Utah Administrative Office of the Courts

Recorded Information Fact Sheet # 6 on Electronic Document Filing Fundamentals, Archives publiques de l'Ontario

Rapport du Comité directeur de la stratégie - sécurité de la technologie de l'information au Conseil du renouveau administratif, juin 1995 (http://www.cse.dnd.ca/GOCITSTRATEGY/).

Circulaire d'information de Revenu Canada, 78-10R2SR, 10 février 1995

SEDAR (Système électronique de données, d'analyse et de recherche), Commission des valeurs mobilières de l'Ontario (CVMO), bulletin du 15 novembre 1996, volume 19, nE 46, supplément du SEDAR

SGML Handbook, Charles F. Goldfarb, 1990, Oxford University Press

Normes relatives à la façon de rédiger, de distribuer et de citer les jugements canadiens sous forme électronique, mai 1996, Comité consultatif sur l'utilisation de l'informatique par les juges du Conseil canadien de la magistrature

Étude des questions de droit entourant la sécurité des renseignements électroniques, Stratégie pour la sécurité des technologies de l'information - groupe de travail sur les questions de droit, juin 1995, Conseil du Trésor du Canada

Sustaining Dialog, ministère du Procureur général, bulletin trimestriel relatif au projet Sustain de dépôt des documents juridiques

Who Owns Copyright in Law Reports? Gérard Snow, 64 C.P.R. (2d) 49

17. **Annexe C : Glossaire**

Authentification : légitimation des personnes et des machines.

Octet : huit chiffres binaires (bits, c'est-à-dire des uns et des zéros) pouvant représenter 256 nombres ou caractères (entre 0 et 255, représentés par 00000000 à 11111111); unité fondamentale de transmission ou de stockage de l'information dans un ordinateur.

CGM : Computer graphics metafile, un format de fichiers d'image.

Cryptographie : science de la sécurisation des messages.

Signature numérique : processus informatique conçu aux mêmes fins que la signature manuscrite; moyen électronique d'associer une personne à un document; résultat de l'utilisation de processus technologiques particuliers pour authentifier un document.

Définition de type de document : structure de document prescrite exprimée en langage LSGB (q.v.); la structure de tous les documents déposés en vertu du SDÉ doit être conforme à la définition du type de document prescrite.

Courrier électronique : courrier envoyé sous forme d'une chaîne d'octets (q.v.) d'un ordinateur à un autre par l'intermédiaire d'Internet (q.v.) ou d'un réseau privé; peut désigner le système ou les messages eux-mêmes.

SDÉ : Système de dépôt électronique, projet conjoint de l'Office national de l'énergie et de la Commission de l'énergie de l'Ontario visant à remplacer les processus reposant sur des documents papier par des systèmes numériques pour faciliter la création, l'échange, l'utilisation et la réutilisation de l'information réglementaire.

HTML : Hypertext Markup Language, sert à créer des pages Web sur Internet avec des liens, appelés hyperliens, vers d'autres pages Web; HTML est une définition de type de document (q.v.) décrite par le métalangage LSGB (q.v.).

Internet : réseau de réseaux informatiques utilisant un protocole de communication convenu, appelé Transmission Control Protocol/Internet Protocol (TCP/IP), qui facilite les services courants comme le courrier électronique, les pages Web et les transferts de fichiers.

JPEG : format de fichiers d'image provenant du Groupe mixte d'experts en photographie, également appelé fichiers JPG, permettant de stocker et de transmettre des photographies dans un système informatique.

MPEG : format de compression vidéo numérique provenant du Groupe d'experts pour le codage d'images animées permettant de stocker et de transmettre des films dans un système informatique.

PDF : Portable Document Format, format de fichiers de document exclusif de Adobe Systems Incorporated.

LSGB : langage standard généralisé de balisage, métalangage utilisé pour décrire des types de documents, comme HTML et XML (q.v.); sépare le contenu et la structure de la mise en forme et de l'aspect.

XML : Extensible Markup Language sous-ensemble du LSGB (q.v.); on prévoit qu'il sera le format des documents de prochaine génération sur le Web (q.v).

World Wide Web : documents liés stockés dans des ordinateurs branchés à Internet (q.v.), également appelé le Web, d'où l'expression page Web désignant un seul document; les adresses des documents commencent fréquemment par www, soit l'abréviation de World Wide Web, comme dans www.neb.gc.ca ou www.oeb.gov.on.ca.