

DOCUMENTS EN FORME ÉLECTRONIQUE: ADMISSIBILITÉ EN PREUVE
ÉTATS-UNIS, QUÉBEC, CANADA

ÉCOLE DES HAUTES ÉTUDES COMMERCIALES
DESS JURICOMPTABILITÉ
TRAVAIL DIRIGÉ
PRÉSENTÉ PAR : LUC MARCIL, L.L.L., C.A.

TABLE DES MATIÈRES

Remerciements	Page 3
Introduction	Page 4
Partie 1	Documents en forme électronique : De quoi parle t'on?.....	Page 5
1.A.	Caractéristiques.....	Page 6
1.B.	Impact logistique.....	Page 7
1.C.	Autres considérations importantes.....	Page 8
Partie 2	Admissibilité en preuve.....	Page 11
2.A.	Considérations préliminaires.....	Page 11
2.B.	Les États-Unis (règles fédérales).....	Page 12
2.B.I.	Le cadre statutaire.....	Page 12
2.B.I. i.	L'obligation de produire les documents.....	Page 12
2.B.I.ii.	L'obligation de préserver les documents.....	Page 13
2.B.I.iii.	L'attribution des coûts.....	Page 14
2.B.II.	Le régime de preuve.....	Page 15
2.B.III.	Les documents en forme électronique.....	Page 20
2.C.	Le Québec.....	Page 30
2.C.I.	Le cadre statutaire.....	Page 30
2.C.II.	Le régime de preuve.....	Page 32
2.C.III.	Les documents en forme électronique.....	Page 39
2.D.	Le Canada (règles fédérales).....	Page 44
2.D.I.	Le cadre statutaire.....	Page 44
2.D.II.	Le régime de preuve à l'égard des documents en forme électronique.....	Page 45
Partie 3	Survol de quelques solutions technologiques.....	Page 51
3.A.	Acquisition, analyse et préservation de la preuve électronique.....	Page 51
	<i>EnCase ®Forensic et EnCase ® Forensic Edition</i>	
3.A.I.	<i>Professional Suites</i>	Page 51
3.A.II.	<i>New Technologies Inc. (Ni)</i>	Page 51
3.B.	Support au litige.....	Page 52
3.B.I.	<i>Summation ® IBlaze</i>	Page 52
3.B.II.	<i>Dataflight Software Inc.</i>	Page 52
3.B.III.	<i>CaseSoft</i>	Page 53
3.C.	Formation professionnelle.....	Page 53
Bibliographie	Page 55

REMERCIEMENTS

Je tiens à remercier le Conseil de recherches en sciences humaines du Canada (CRSH) pour la bourse d'étude en juricomptabilité qui m'a été octroyée par l'Alliance de recherche et la Chaire de gouvernance et juricomptabilité de HEC Montréal http://www.sshrc.ca/web/winning/stories/labelle_f.asp

INTRODUCTION

Une part de plus en plus grande de la documentation au sein des entreprises privées et publiques, de même qu'au sein des organismes gouvernementaux se retrouve maintenant en forme électronique. De plus, une grande partie de cette documentation se trouve strictement en forme électronique, sans aucune contrepartie en forme papier. Les courriers électroniques constituent le meilleur exemple de cet état de fait.

Cette nouvelle réalité impose des changements drastiques dans la recherche, l'acquisition et la mise en preuve de l'information aux fins des litiges civils, commerciaux et criminels. Les juricomptables doivent donc adapter leurs méthodes de travail en conséquence.

Les Etats-Unis ont été le moteur de la révolution informatique de la deuxième moitié du 20^{ième} siècle et à l'avant-garde des changements importants qui en ont résulté dans nos façons de faire. Il n'est pas surprenant de constater que c'est aux Etats-Unis que les approches que nous utilisons pour composer avec cette nouvelle réalité ont été développées pour être ensuite adaptées à nos besoins spécifiques.

Le présent ouvrage constitue un tour d'horizon et cherche à effectuer un survol des solutions adoptées aux Etats-Unis, au Québec et au Canada pour composer avec l'explosion de l'information en forme électronique. Nous définirons d'abord de quoi nous parlons lorsqu'il est question de documents en forme électronique. Par la suite, nous explorerons comment nos autorités juridiques appliquent ou adaptent nos règles de preuve à cette nouvelle réalité. Finalement, nous aborderons un survol de quelques solutions technologiques qui ont été développées pour recueillir et sauvegarder cette information sans l'altérer, tout en préservant sa valeur probante.

Le présent ouvrage ne se veut nullement une recherche exhaustive des règles de preuve ou des diverses solutions technologiques applicables aux documents en forme électronique mais sert plutôt à établir le cadre de référence dans lequel ces questions sont examinées et résolues. Il se veut d'abord et avant tout un guide pour les juricomptables afin de les pointer dans la bonne direction pour effectuer des recherches plus approfondies sur ces questions.

PARTIE 1. Documents en forme électronique : de quoi parle t'on ?

Les informations qui suivent sont extraites de l'ouvrage de Micheal R. Arkfeld, intitulé *Electronic Discovery and Evidence, 2003, Law Partner Publishing, LLC, Phoenix, Arizona.*

- D'après une étude réalisée par l'Université de la Californie, 93% de toute l'information générée aux Etats-Unis en 1999 l'a été sous forme digitale, sur des ordinateurs. Seulement 7% de l'information a été générée sur d'autres médias, dont le papier.¹
- En 1991, pour la première fois aux États-Unis, les entreprises ont dépensé plus en équipements voués à l'informatique et aux communications qu'en équipements industriels voués aux industries minière, agricole et de la construction. L'informatique est devenue aussi vitale que l'air que nous respirons.²
- Aujourd'hui, nous utilisons des ordinateurs dans toutes les facettes de nos vies: pour produire des graphiques, projets vidéo, films, composer de la musique, créer et réviser des documents, pour fins personnelles ou d'affaires, pour communiquer par voie du courrier électronique, pour faire des réservations d'hôtels, d'avion, pour participer à des discussions en temps réel, etc. Tout ça, grâce à l'ordinateur et à l'Internet.
- Avant les années 1990, la preuve devant les tribunaux était soumise presque exclusivement sous forme papier. Aujourd'hui, il est estimé que plus de 30% des communications corporatives aux Etats-Unis existent exclusivement en forme électronique sans aucune contrepartie en forme papier et que 97% de l'information est créée de façon électronique.³
- Ces changements ont un impact direct sur la façon dont nous recueillons la preuve aux fins du processus judiciaire. Historiquement, ceci se limitait aux dépositions, entrevues, interrogatoires et aux documents et registres en forme papier de la partie adverse. Aujourd'hui, il faut en plus composer avec de vastes quantités d'information en forme électronique.
- En fait, les experts prédisent que d'ici 5 à 7 ans, les documents en forme électronique remplaceront les documents en forme papier à titre de source primaire de la preuve aux fins des litiges commerciaux aux États-Unis.⁴ Il est donc devenu nécessaire d'examiner l'information imprimée et celle qui n'est pas reproduite sur support papier.

¹ *In re Bristol-Myers Squibb Securities Litigation, 205 F.R.D. 437, 440 n.2 (D.N.J. 2002)*

² Thomas A. Stewart, *The information Age in Charts, Fortune, April 4th, 1994, at 75 – 79.*

³ Peter V. Lacouture, *Discovery and Use of Computer-Based Information in Litigation, 45 R.I.B.J. (1996)*

⁴ Elizabeth Bacon Ehlers, et al., *E-Discovery, Chapter 2, Business, Law, and the Internet: Essential Guidance for You, Your Clients and Your Firm (2002).*

1. A Caractéristiques

Les documents en forme électronique possèdent plusieurs caractéristiques qu'il est utile de mentionner :

- ils ne se limitent pas strictement à du texte ou des données mais peuvent aussi contenir des bandes sonores, bandes vidéo, des graphiques, photos, etc. Il n'est pas rare que ces documents soient sous forme multimédia.
- ils peuvent reposer à plusieurs endroits différents, simultanément ou à diverses époques:
 - sur des serveurs centralisés;
 - sur des postes de travail individuels;
 - sur disques durs;
 - sur support magnéto-optique, disquettes, CD-ROM, DVD;
 - sur copie de secours (*backup copies*);
 - chez le client, ses employés, chez ses partenaires d'affaires, ses concurrents, auprès d'organismes publics, dans le domaine public.
- ils peuvent exister en plusieurs versions, captées aux diverses étapes de leur création et de leur révision.
- ils peuvent exister en plusieurs formats :
 - Microsoft Word;
 - Corel Wordperfect;
 - Rich Text;
 - HTML;
 - SGML;
 - ASCII;
 - Microsoft Outlook, Outlook Express ;
 - Qualcomm Eudora ;
 - Etc.
- En plus de l'information qu'ils sont destinés à contenir, les documents en forme électronique contiennent également ce qu'il est convenu d'appeler « Metadata », c'est-à-dire une description du contenu du document. Le « Metadata » constitue une mine d'or d'information et peut contenir les renseignements suivants :
 - le nom de l'auteur du document;
 - la date de création du document et les dates de révision;
 - le nom des différents individus qui ont participé à la création et/ou la révision du document et la date à laquelle chaque révision a été effectuée;
 - les informations insérées ou retirées par chaque révision;
 - la date où le document a été expédié par courrier électronique, l'identification de son ou ses destinataires, leur adresse Internet, les autres documents joints à l'envoi, etc.

- ils revêtent souvent un caractère informel (exemple: courriers électroniques), et sont donc plus propices à contenir certaines révélations plus franches et sincères. Les courriers électroniques sont d'ailleurs devenus l'outil par excellence pour asseoir la preuve d'un état d'esprit ou d'une intention coupable.
- ils sont pour la plupart du temps conservés en grandes quantités et en forme désorganisée. Ils peuvent même parfois être cryptés.
- Ils peuvent être reproduits aussi souvent qu'on le désire.
- Ils peuvent être facilement modifiés, altérés ou « supprimés ». La méthode usuelle pour les « supprimer » fait en sorte que seule leur inscription dans la table des matières du contenant où ils reposent est effacée, laissant ainsi intact le fichier qui les contient.

Du point de vue de leur valeur probante aux fins du processus judiciaire, les caractéristique les plus importantes des documents en forme électronique concernent certainement le « Metadata » qui les accompagne généralement, leur grand volume, leur structure désorganisée et le fait qu'ils sont susceptibles d'être altérés par le seul fait de leur avoir accès, de les ouvrir ou même, de lancer l'ordinateur sur lequel ils reposent.

1. B. Impact logistique

- Il faut d'abord trouver les documents en forme électronique recherchés et les rapatrier...

Tel qu'indiqué précédemment, les documents en forme électronique peuvent reposer à plusieurs endroits différents: sur des serveurs centralisés, sur des postes de travail individuels, sur des copies de secours, sur des supports magnéto-optiques, à l'externe, etc.

Ceci implique des recherches exhaustives sur plusieurs fronts géographiques. Une des conséquences à ne pas négliger concerne la responsabilité de ceux qui ont l'obligation légale de les produire aux fins du processus judiciaire.

- Il faut préserver leur authenticité et valeur probante, i.e. ne pas les altérer...

Il faut être excessivement prudent dans la méthode de cueillette des documents en forme électronique puisque le seul fait de lancer l'ordinateur sur lequel ils reposent ou d'ouvrir les fichiers électroniques qui les contiennent peut très bien en altérer le contenu de façon irrémédiable.

Il existe diverses solutions techniques pour faire face à ces problèmes, dont quelques unes sont discutées à la Partie 3 du présent ouvrage.

L'approche commune à ces solutions techniques consiste à prendre une « image » du contenant, processus qui n'altère d'aucune façon les documents qui y sont contenus. Ces images consistent en une reproduction bit par bit du contenant. Généralement, plusieurs images du contenant sont effectuées ce qui permet d'en préserver au moins une à titre de copie authentique non altérée et de travailler avec les autres pour ouvrir et analyser le contenu des documents en forme électronique recherchés.

- Il faut ensuite les répertorier et les analyser pour pouvoir en extraire le contenu pertinent...

Il est très fréquent pour les moyennes et grandes entreprises de générer des quantités impressionnantes de documents en forme électronique. Cette situation ne peut être mieux illustrée que dans le cadre du litige *United States v. Microsoft*, aux fins duquel le Département de la Justice Américain a accumulé plus de 3 millions de documents en forme électronique, la plupart sous forme de courriers électroniques, pour les faire valoir contre Microsoft.⁵

Une telle quantité de documents et d'information constitue très certainement un défi logistique. Heureusement, la nature même des documents en forme électronique facilite leur examen et leur analyse à l'aide de divers logiciels de recherche spécialisés dont quelques-uns sont discutés à la Partie 3 du présent ouvrage.

Ces outils permettent une recherche des documents par mots clés, dates, noms, lieux et autres caractéristiques pertinentes. En plus, ils permettent d'examiner et d'analyser de grandes quantités de documents en forme électronique en relativement peu de temps.

- Tout ceci peut coûter très cher...

La cueillette des documents en forme électronique, leur préservation, leur examen et analyse et leur présentation devant les tribunaux peut représenter des coûts très importants pour les parties impliquées.

L'imputation des coûts reliés à la production de documents en forme électronique aux fins du processus judiciaire est discutée plus en détail à la Partie 2 du présent ouvrage.

⁵ Ken Auletta, *World War 3.0: Microsoft and Its Enemies* 55, 389 (2001).

1. C. Autres considérations importantes

- Confidentialité, secret professionnel, secrets commerciaux, etc.

Les documents en forme électronique peuvent contenir de l'information jugée confidentielle, propriétaire, ou faisant l'objet du secret professionnel. Il est donc crucial de les examiner minutieusement avant de les produire à la partie adverse. Insérer ou laisser filer de l'information confidentielle ou sujette au secret professionnel par inadvertance dans les documents en forme électronique produits devant les tribunaux et à la partie adverse peut constituer une renonciation au bénéfice du secret ou à la confidentialité de cette information.

Considérant la quantité souvent énorme de documents en forme électronique sujets à être produits devant les tribunaux et à la partie adverse, la tâche de les filtrer peut rapidement devenir très difficile et très onéreuse.

Les parties peuvent obvier à cette difficulté en concluant un accord en vertu duquel l'insertion par inadvertance d'information de nature propriétaire, confidentielle ou sujette au secret professionnel ne constitue pas une renonciation au bénéfice du secret ou de la confidentialité. Ce genre d'entente peut devenir cruciale dans le cadre de litiges impliquant de très grandes quantités de documents en forme électronique qui peuvent ainsi mettre en péril les secrets d'une organisation.

- « Metadata »

Tel qu'indiqué précédemment, la plupart des documents en forme électronique contiennent ce qu'il est convenu d'appeler le « Metadata », i.e. une description parfois très détaillée du contenu et des révisions apportées à ces documents. Il est donc préférable d'obtenir ces documents dans leur forme originale afin d'avoir accès au « Metadata ».

Certains auraient tendance à demander à la partie adverse d'imprimer les documents en forme électronique sur papier avant de les produire ou de les convertir en un format différent. Ceci est tout à fait contre indiqué puisque le destinataire perd l'avantage de pouvoir examiner le « Metadata ». De plus, obtenir ces documents sous forme papier rend la tâche de les examiner doublement plus difficile puisque les logiciels spécialisés de recherche ne peuvent pas être utilisés à moins de re-digitaliser ces documents.

- Fichiers « supprimés »

Certains documents en forme électronique contenus dans des fichiers qui ont fait l'objet de la fonction « supprimer » peuvent quand même être recouverts.

Effectivement, la fonction « supprimer » des systèmes d'opération prédominants comme Microsoft Windows ® ne fait que retirer la description du fichier de la table des matières du contenant. Le fichier comme tel demeure donc intact tant et aussi longtemps que l'espace physique qu'il occupe n'est pas utilisé par d'autres fichiers.

Plusieurs logiciels spécialisés ont pour fonction de retrouver et de réhabiliter les fichiers « supprimés » qui subsistent dans les divers contenants électroniques tels les disques durs. Il n'est pas rare de retrouver de véritables mines d'or sur les disques durs de la partie adverse ou même sur des disques durs abandonnés ou jetés aux rebuts.

Il faut donc tenir compte de cet état de faits lorsqu'on demande la permission au tribunal pour obtenir l'accès aux documents en forme électronique de la partie adverse. La meilleure façon de se pourvoir de cet avantage est de demander d'obtenir une image des divers contenants électroniques de la partie adverse. Ces images constituent une réplique exacte bit par bit de ces contenants et permettent ainsi de trouver et réhabiliter certains documents qui avaient par ailleurs été « supprimés ».

- Politique de rétention des documents en forme électronique

Malheureusement, la plupart des entreprises ont des politiques déficientes ou n'en ont tout simplement aucune quant à la rétention de leurs documents en forme électronique.

Il n'est pas rare que des entreprises sauvegardent leurs documents en forme électronique sur des périodes beaucoup trop longue sans même le savoir, rendant du même coup ceux-ci sujets à être produits devant les tribunaux. A l'opposé, certaines entreprises détruisent leurs documents en forme électronique beaucoup trop rapidement, les rendant inaccessibles en cas de litige. Ceci peut être très dangereux lorsque des litiges surviennent et que la partie adverse connaît l'existence de documents en forme électronique qui s'y rapportent et les requiert. Dans certains cas, le défaut de produire ces documents peut entraîner des jugements par défaut ou d'autres sanctions contre ceux qui ne sont pas en mesure de ce faire.

Une politique appropriée de rétention des documents en forme électronique joue donc un rôle crucial dans la localisation, l'identification, l'examen et la production des documents requis.

PARTIE 2. Admissibilité en preuve

2. A. Considérations préliminaires

Les juridictions de *Common Law*, dont les États-Unis et le reste du Canada, comportent un processus préliminaire au procès qui ne trouve pas de contrepartie identique dans la juridiction de Droit Civil du Québec. Ce processus sert à la découverte de la preuve de chaque partie au litige et contient plusieurs règles qui portent sur les documents et l'information qu'une partie peut demander à l'autre de produire avant de passer à l'audition du procès par un juge et/ou jury, selon le cas. Ce processus s'appelle « *Discovery Process* ».

La règle générale veut que tout ce qui est pertinent au litige puisse faire l'objet d'une requête en découverte aux fins du « *Discovery Process* ». Par ailleurs, la règle de la pertinence est quasi-universelle dans tous les régimes de droit en ce qui a trait à la preuve qui est recevable ou non devant les tribunaux, dans la mesure où celle-ci n'est pas contraire à l'ordre public, à l'intérêt national, ne cause pas un préjudice indu, ne sert pas à confondre ou embrouiller le tribunal ou n'est pas contraire à des dispositions spécifiques à cette fin.

En général, les documents qui peuvent faire l'objet d'une requête en découverte aux fins du « *Discovery Process* » dans les régimes de *Common Law* peuvent par la suite être soumis en preuve devant les tribunaux. Il en tient au juge du procès de les accepter ou non à titre de preuve admissible à la lumière des règles de preuve en vigueur dans chaque juridiction.

En droit Québécois, le Code de Procédure Civile du Québec (CPCQ) contient des dispositions permettant de demander à la partie adverse, aux témoins ou à des tierces parties, aux diverses étapes du processus judiciaire, de produire les documents pertinents aux fins du litige. Par exemple, l'article 311 CPCQ permet de demander à un témoin en possession d'un document visé de le produire à la Cour. L'article 402 CPCQ permet d'en faire autant dans le cas d'un document en possession d'une tierce partie.

Traditionnellement, les dispositions du CPCQ à l'égard de la production de documents n'ont pas eu une étendue aussi large que le « *Discovery Process* » dans les juridictions de *Common Law*.

2. B. Les États-Unis (règles fédérales)

2. B. I. Cadre statutaire

Les Règles Fédérales de Procédure Civile (RFPC) et les règles similaires de chaque État américain constituent le cadre juridique applicable à la procédure applicable à l'instruction des procès devant les tribunaux aux États-Unis.

Les RFPC régissent la procédure applicable à tous les procès de nature civile devant les Cours de District américaines. En règle générale, les règles de procédure civile de chaque État sont très similaires, sinon identiques, aux RFPC. Il faut tout de même référer aux règles de procédure de chaque État américain pour s'assurer de bien s'y conformer.

Dans la même veine, les Règles Fédérales de Preuve (RFP) régissent l'admissibilité des divers éléments de preuve soumis par les parties au litige, dont les documents en forme électronique.

Les tribunaux américains reconnaissent et supportent l'admission en preuve de documents en forme électronique en se basant sur la réalisation que ceux-ci reflètent l'évolution de la technologie dans le domaine des affaires.

*« Today, it is black letter law that computerized data is discoverable if relevant ».*⁶

*“Computers have become so commonplace in litigation that most court battles now involve discovery of some computer-stored information”.*⁷

2. B. I. i. L'obligation de produire les documents

Le sous alinéa 26(a)(1)(B) RFPC requièrent qu'une partie produise à l'autre :

« a copy of, or a description by category or location of, all documents, data compilations, and tangible things in the possession, custody, or control of the party and that the disclosing party may use to support its claim or defenses, unless solely for impeachment”.

L'alinéa 34(a) RFPC définit « document » comme:

« including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices, into reasonably usable form »

⁶ *Anti-Monopoly Inc. v. Hasbro Inc.* CIV.94-2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995).

⁷ *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 462 (D. Utah 1985).

Le comité consultatif constitué aux fins de l'élaboration et la mise à jour de ces règles a inclus ce qui suit en 1970 dans ses notes:

« *The inclusive description of « document » is revised to accord with changing technology »*

Plusieurs cas ont affirmé l'élargissement de la définition précitée de « document » pour inclure les documents en forme électronique. En voici deux exemples:

- *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*⁸
Les documents en forme électronique sont autant susceptibles d'être produits en preuve que les documents en forme papier.
- *United States v. Hutson*,⁹
« *Data compilations* » comprend des documents en forme électronique.

De plus, la règle 16(c) RFPC prévoit la procédure applicable spécifiquement à la découverte de documents en forme électronique.

2. B. I. ii. L'obligation de préserver les documents

À moins de dispositions statutaires spécifiques à cette fin, les tribunaux américains sont divisés quant au moment précis où survient l'obligation qu'ont les parties de préserver les documents pertinents aux fins des litiges.

Selon diverses causes entendues devant les tribunaux, cette obligation peut survenir à différents moments:

- Lorsqu'un litige est en attente, qu'il est devenu imminent ou raisonnablement prévisible;
- Lorsqu'un litige est anticipé ou qu'il y ait une vraisemblance de litige;
- Lorsqu'une plainte ou réclamation a été logée;
- Lorsqu'une ordonnance de préservation a été émise; ou
- Lorsqu'une requête pour découverte a été reçue.

Afin d'éviter les sanctions possibles pouvant découler du défaut de préserver les documents susceptibles de faire l'objet d'une requête pour découverte aux fins d'un

⁸ 205 F.R.D. 421, 428 (S.D.N.Y. 2002).

⁹ 821 F.2d 1015, 1019 – 1020 (5th Cir. 1987).

litige, il est préférable de les préserver dès qu'une partie est notifiée ou a pris connaissance (ou aurait dû prendre connaissance) qu'un litige peut survenir.

L'article 37 RFPC prévoit les sanctions possibles au défaut de préserver ou de produire les documents ou suite à la destruction délibéré ou par inadvertance de documents. Ces sanctions peuvent être :

- Une ordonnance enjoignant de produire certains documents;
- Des inférences ou présomptions défavorables découlant du défaut de produire les documents requis;
- Des sanctions pécuniaires;
- Des jugements par défaut.

Dans l'arrêt *In re Prudential Ins Co. Of Amer. Sales Practices Litig.*,¹⁰ la Cour du District du New Jersey a statué qu'après qu'une ordonnance de préservation a été émise, la direction de l'entreprise visée par une telle ordonnance devient responsable de mettre en œuvre un plan détaillé à cette fin et de le communiquer aux employés.

2. B. I. iii. L'attribution des coûts

Traditionnellement, aux États-Unis, les parties sont responsables des coûts qu'elles doivent encourir pour produire les documents et registres requis aux fins du « Discovery Process ». Cette règle s'applique également à la production de documents en forme électronique.¹¹

En fait, la philosophie prédominante veut que ce soit les entreprises elles-mêmes qui ont décidé d'avoir recours à des documents en forme électronique dans le cours de leurs affaires et, en conséquence, il leur incombe donc de rendre ceux-ci disponibles pour fins d'examen dans le cadre du « Discovery Process ».

Par contre, une partie peut invoquer la discrétion accordée au tribunal de district en vertu du paragraphe 26 (c) RFPC lorsque les demandes de la partie adverse lui imposent des dépenses trop élevées ou un fardeau trop lourd à supporter. En faits dans l'arrêt précité *Rowe Entertainment, Inc.*,¹² le tribunal a élaboré huit (8) critères à prendre en considération aux fins de l'attribution des coûts liés à la découverte de documents en forme électronique aux fins du « Discovery Process »:

- La spécificité des requêtes pour découverte;

¹⁰ 169 F.R.D. 598, 615 (D.N.J. 1997).

¹¹ *Oppenheimer Fund Inc. v. Sanders*, 437 U.S. 340 (1978).

¹² Voir à la note 8.

- La vraisemblance de trouver de l'information pertinente;
- La possibilité d'obtenir l'information demandée d'autres sources;
- Les raisons pour lesquelles l'intimée maintient l'information réclamée;
- le bénéfice relatif pour les parties d'obtenir l'information réclamée;
- Le coût total découlant de la production de l'information réclamée;
- L'habileté respective des parties à contrôler les coûts et les facteurs qui les incitent à ce faire; et
- Les ressources disponibles à chaque partie.

2. B. II Régime de preuve

En premier lieu, il est important de mentionner que le système judiciaire américain a la particularité de comporter des procès civils devant jury, ce qui n'est pas le cas au Québec et dans le reste du Canada.

La règle générale veut que le juge décide des questions de droit et le jury décide des questions de faits.

Le jury soupèse la preuve contradictoire et la crédibilité des témoins sur la base des faits qui lui sont présentés et des instructions reçues du juge. Une fonction importante du juge consiste à déterminer la preuve qui est admissible et qui peut être présentée au jury.¹³

Les Règles Fédérales de Preuve (RFP), adoptée en 1975, régissent l'admissibilité de la preuve aux fins des procès civils et criminels devant les tribunaux fédéraux américains. Plus de 30 États américains ont également adopté des règles similaires aux RFP. Le « *Federal Business Record Act* » (FBRA) régit spécifiquement l'admissibilité en preuve des registres maintenus dans le cours normal des affaires par les organismes gouvernementaux fédéraux. La plupart des États américains ont leur propre « *Business Record Act* » qui régissent les documents des organismes gouvernementaux de l'État.

Ainsi, dans l'arrêt *United States v. De Georgia*,¹⁴ le tribunal a statué que les RFP s'appliquent aux documents en forme électronique au même titre qu'aux autres éléments de preuve. Dans l'arrêt *United States v. Russo*,¹⁵ le tribunal a statué que le

¹³ *Colorado Nat. Bank v. First Nat. Bank & Trust Co.*, 459 F. Supp. 1366 (W.D. Mich. 1978)

¹⁴ 420 F.2d 889, 893 (9th Cir. 1969)

¹⁵ 480 F.2d 1228, 1239 (6th Cir. 1973).

FBRA s'applique autant aux registres des organismes gouvernementaux maintenus en forme électronique qu'aux registres conventionnels en forme papier.

Les documents en forme électronique présentent des défis uniques quant à leur admissibilité en preuve. Il faut établir leur authenticité et leur pertinence et surmonter les objections basées sur le ouïe dire qui sont nécessairement suscitées par leur introduction.

Les questions préliminaires suivantes, applicables à tous éléments de preuve, doivent d'abord être adressées:

- Est-ce que les documents en forme électronique introduits sont pertinents aux fins du litige? (RFP No. 401 – 404);

En vertu de la règle 401 RFP, une preuve est pertinente lorsqu'elle rend l'existence de tout fait ayant un impact sur la détermination du litige plus probable ou moins probable que ce qui aurait été le cas sans cette preuve.

En vertu de la règle 402 RFP, toute preuve pertinente est admissible sauf disposition contraire dans la Constitution des États-Unis, une loi du Congrès, une règle à cette fin dans les RFP ou une disposition statutaire de la Cour Suprême des États-Unis.

En vertu de la règle 403 RFP, une preuve autrement pertinente peut quand même être écartée si elle n'est pas utile à la résolution du litige, si elle cause un préjudice indu, si elle tend à confondre ou à embrouiller les questions en litige ou si elle constitue une perte de temps pour le tribunal. Dans l'arrêt *Old Chief v. United States*, le tribunal a statué que la décision par un juge d'exclure une preuve autrement pertinente peut être sujette à révision.¹⁶

- Est-ce qu'à leur face même, les documents en forme électronique introduits contiennent assez d'information, en quantité et en qualité, pour être admis par le juge à titre préliminaire? (RFP No. 104);

Toute question préliminaire à l'admissibilité d'un élément de preuve demeure du domaine du juge. Certains éléments de preuve sont admissibles seulement si certaines conditions sont rencontrées. Par exemple, l'introduction d'un document électronique au soutien d'une vente par Internet repose sur la condition qu'il a été institué par le vendeur et accepté par l'acheteur et qu'il concerne cette transaction spécifique. C'est au juge à déterminer si ces conditions sont remplies pour déterminer, de façon préliminaire, si ce document peut être accepté en preuve et présenté au jury, le cas échéant.

¹⁶ 519 U.S. 172 (1997).

Un corollaire de cette approche se retrouve à la règle 106 RFP, où il est spécifié que lorsqu'une portion de document ou d'enregistrement est introduite en preuve, la partie adverse peut demander que la totalité du document ou de l'enregistrement soit examinée pour éviter l'introduction de preuve hors contexte.

Également, en vertu de la règle 201 RFP, un juge peut adjudiquer un fait comme était généralement reconnu (« *Judicial Notice* ») parce qu'il est reconnu dans le territoire de juridiction de la cour et qu'il peut facilement être prouvé à partir de sources dont la crédibilité ne peut raisonnablement pas être mises en doute.

Ainsi, dans l'arrêt *People v. Rivera*,¹⁷ le tribunal a conclu que le juge de première instance a correctement qualifié comme étant généralement reconnu le fait que les ordinateurs I.B.M. sont des ordinateurs standards et fiables.

- Est-ce que les documents en forme électronique introduits peuvent être authentifiés? (RFP No. 901);

L'exigence de démontrer l'authenticité d'un élément de preuve comme condition préalable à son admissibilité est rencontrée par une démonstration suffisante que l'élément ainsi introduit est bien ce qu'il est censé être (règle 901 (a) RFP).

Le processus par lequel la preuve est reliée à la question en litige constitue l'authentification ou l'identification.

Par exemple, l'authentification d'un document en forme électronique implique qu'il soit démontré que le document est bien ce qu'on prétend qu'il est et qu'il y ait une relation entre ce document, un individu et la question en litige.

- Est-ce que les documents en forme électronique introduits constituent du ouïe dire non admissible, ou se qualifient-ils dans le cadre des exceptions prévues à cette fin? (RFP No. 801 – 807);

En gros, le ouïe dire se résume à l'introduction d'un élément de preuve par un individu qui ne l'a pas constaté directement mais qui rapporte ce qu'un autre a constaté. Ce genre de preuve n'est généralement pas accepté parce que la partie adverse n'a pas l'opportunité de contre-interroger la partie qui a constaté la preuve directement, ce qui rend cette preuve moins probante.¹⁸

Les règles 801 – 807 RFP contiennent la définition de ouïe dire et l'énumération de plusieurs exceptions (au-delà de trente) à cette règle.

Pour les besoins du présent ouvrage, il m'est apparu inutile de « plonger » dans ces nuances qui peuvent être fastidieuses, difficiles à comprendre et porter à confusion.

¹⁷ 182 Ill. App. 3d 33, 42, 537 N.E.2d 924, 931 (1989).

¹⁸ *California v. Green*, 90 S.Ct. 1930, 1935 (1970).

En somme, ces règles ont un impact à l'égard des documents en forme électronique, comme par exemple les registres informatisés d'entreprises, pour la simple et bonne raison que ces registres sont souvent compilés par un ou des individus autres que celui ou ceux qui sont impliqués directement par les transactions qui les concernent et autres que celui ou ceux qui les présentent devant le tribunal en cas de litige. Une stricte application des règles afférentes au ouïe dire aurait pour résultat de prohiber la mise en preuve de ces documents à moins de les introduire par le ou les individus qui ont été directement impliqués dans chacune des transactions qui les concernent. Comme ces registres peuvent concerner plusieurs transactions impliquant plusieurs individus différents, ceci pourrait causer des problèmes logistiques très importants.

C'est pour cette raison que l'une des exceptions prévues à la règle du ouïe dire porte sur les documents, compilations ou registres tenus dans le cours normal des affaires d'une entreprise commerciale par une personne informée. Les américains réfèrent à cette exception au titre du « *Business Records exception* » (règle 803 (6) RFP). Il s'agit des registres qui se rapportent aux activités conduites régulièrement et normalement par les entreprises dans le cours normal des affaires. Ceux-ci peuvent être introduits devant les tribunaux sur la base du témoignage de la ou des personnes qui participent à leur préparation, lorsqu'il peut être démontré qu'ils sont constitués dans le cours normal des affaires et non à des fins ad hoc aux fins du litige.

- Est-ce que la règle de la meilleure preuve requiert l'original du document produit? (RFP No. 1001 – 1008).

La règle de la meilleure preuve a pour but de minimiser le risque de fraude, de fausses représentations ou de falsification du contenu des écrits. De plus, cette règle requiert que lorsqu'une preuve de meilleure valeur existe quant à l'objet à prouver, il faille y avoir recours plutôt que de recourir à une preuve de moindre valeur.

La règle 1002 RFP indique que pour prouver le contenu d'un écrit, un enregistrement ou une photographie, l'original de cet écrit, de cet enregistrement ou de cette photographie doit être produit, sauf lorsqu'il en est autrement prévu dans les RFP ou une loi du Congrès.

La règle 1003 RFP prévoit qu'une copie est admissible en preuve au même titre que l'original à moins que 1) des questions légitimes ne soient soulevées quant à l'authenticité de l'original ou 2) il serait injuste, dans les circonstances, d'admettre la copie plutôt que l'original.

La règle 1005 RFP stipule que les copies certifiées conformes de documents publics peuvent être admissibles en preuve

La règle 1006 RFP prévoit que le contenu d'écrits, d'enregistrements ou de photographies qui sont trop volumineux pour être examinés devant le tribunal sans poser d'inconvénients peut être mis en preuve sous forme de diagramme, sommaire ou de calculs dans la mesure où les originaux ou des copies de ceux-ci soient mis à la disposition des parties pour examen, pour copie ou les deux à un endroit et à un moment raisonnables. Le tribunal peut toutefois ordonner que ces éléments de preuve soient tout de même produits devant le tribunal.

En général, la règle de la meilleure preuve requiert la production de l'original de tout écrit, enregistrement ou photographie présenté en preuve devant les tribunaux.

Aux fins des documents en forme électronique, la règle 1001 (3) RFP prévoit que lorsque les données sont emmagasinées sur un ordinateur, toute reproduction imprimée de celles-ci (« *Printout* ») ou toute reproduction de celles-ci qui soit lisible à l'œil constitue un original qui satisfait la règle de la meilleure preuve s'il peut être démontré à la satisfaction du tribunal que ces reproductions représentent fidèlement leur contenu.

La règle 1007 RFP prévoit que dans certains cas, la preuve d'écrits peut se faire par témoin, comme par exemple lorsque la partie adverse admet l'existence et le contenu d'un écrit lors de son interrogatoire ou contre-interrogatoire.

Pour résumer, en ce qui a trait aux documents en forme électronique, les règles 1001 (3) et 1006 RFP permettent l'admissibilité en preuve de « *Printouts* » et de sommaires. Dans la plupart des cas, ces règles permettent donc de satisfaire à l'exigence de la meilleure preuve.

Tout comme les « *Printouts* », les images électroniques d'un document, tels les documents reproduits en format TIFF ou PDF, devraient aussi satisfaire la règle de la meilleure preuve.

Une des questions d'actualité consiste à se demander si les représentations de documents en forme électronique sans le « *Metadata* » qui leur est afférent satisfont la règle de la meilleure preuve.

Cette question a été abordée dans l'arrêt *Armstrong v. Executive Office of the President, Office of Admin.*,¹⁹ où il a été décidé que même si les reproductions imprimées de documents en forme électronique peuvent être admises en preuve, celles-ci ne peuvent servir de remplacement des documents en forme électronique originaux puisqu'elles ne contiennent pas la totalité des informations contenues dans ceux-ci et ne sont donc pas identiques :

¹⁹ 1 F.3d 1274, 1283, 1285 (D.C.Cir. 1993)

« The mere existence of the paper printouts does not affect the record status of the electronic materials unless the paper versions include all significant material contained in the electronic records. Otherwise, the two documents cannot accurately be termed “copies” – identical twins – but are, at most, “kissing cousins.” Since the records shows that the two versions of the documents may frequently be only cousins – perhaps distant ones at that – the electronic documents retain their status as federal records after the creation of the paper printouts... Our refusal to agree with the government that electronic records are merely “extra copies” of the paper versions amounts to far more than judicial nitpicking. Without the missing information, the paper printouts – akin to the traditional memoranda with the “to” and “from” cut off and even the “received” stamp pruned away – are dismembered documents indeed.»

La reproduction imprimée de documents en forme électronique ou les images électroniques de ceux-ci (format TIFF ou PDF) ne constituent pas nécessairement une représentation complète et fidèle de ceux-ci. On peut donc conclure que seule l'information, en sa forme électronique, incluant le « *Metadata* », constitue un original aux fins de la Loi.

2. B. III Les documents en forme électronique

Chaque élément soumis en preuve doit d'abord satisfaire aux règles générales régissant l'admissibilité en preuve. Que ce soit des écrits conventionnels ou des documents en forme électronique, les règles de preuve demeurent les mêmes. En gros, il s'agit de satisfaire aux exigences quant à la pertinence, l'authenticité, le ouïe dire et la règle de la meilleure preuve.

Les documents en forme électronique possèdent par contre certaines caractéristiques particulières qui ont une influence sur leur admissibilité en preuve. En voici quelques unes à titre d'exemple.

- **Courriers électroniques**

- **Authenticité**

L'accès à l'ordinateur ou au logiciel de courrier électronique est-il assujéti à l'insertion d'un mot de passe ? Est-ce que ce mot de passe, le cas échéant, doit être modifié de façon périodique ? Ceci influence la valeur probante à donner à ces courriers électroniques quant à l'identité de l'auteur des courriers qui émanent de ce logiciel ou de cet ordinateur et de leur authenticité.

Le « *Metadata* » afférent au courrier électronique est-il disponible ? Celui-ci peut contenir une information cruciale quant à l'auteur, le destinataire, leur adresse Internet respective, le moment de l'envoi, le moment de la réception, une preuve ou avis de réception, etc.

Le réseau local sur lequel se trouve l'ordinateur duquel origine le courrier électronique concerné contient-il un journal (« log ») contenant l'information pertinente quant à l'accès au réseau de certains utilisateurs, le moment de cet accès, les activités effectuées par ceux-ci, etc. Ceci aussi peut servir à corroborer l'identité de l'auteur et l'authenticité des courriers électroniques.

Est-ce que le courrier électronique était encrypté ? Était-il accompagné d'une signature électronique ? Ceci exerce aussi une influence quant à l'identité de l'auteur et l'authenticité des courriers électroniques.

Comment les courriers électroniques concernés ont-ils été sauvegardés ? Ont-ils pu être altérés ? Ont-ils été récupérés par un expert indépendant ?

Dans l'arrêt *United States v. Scott-Emuakpor*,²⁰ le tribunal a statué que le standard à appliquer pour établir l'authenticité d'un élément de preuve ne consiste pas à faire la preuve hors de tout doute qu'il est bien ce qu'il est censé être mais plutôt d'établir avec une probabilité raisonnable qu'il est ce qu'il est censé être.

« To establish authenticity, the proponent need not rule out all possibilities inconsistent with authenticity or prove beyond any doubt that the evidence is what it purports to be. Rather, the standard for authentication is one of "reasonable likelihood" that the evidence is authentic. Generally, Rule 901 (a) is satisfied if the proponent makes a sufficient showing to allow a reasonable person to believe the evidence is what it purports to be. After the court is satisfied that this showing has been made and admits the evidence as authenticated, the jury decides what weight to give the evidence.... Thus, for example, the Government may meet the authentication requirement through the testimony of a witness who was present and observed the procedure by which the documents were obtained from Defendant's computers.»

Dans l'arrêt *Network Alliance Group, LLC v. Cable & Wireless USA, Inc.*,²¹ certains courriers électroniques n'ont pas pu être authentifiés en raison des incohérences dans les informations qui les concernent.

« C & W has noted a number of other inconsistencies within the alleged e-mail correspondence which suggest that the correspondence is not authentic. Most notably, the "date stamp" for one of the e-mail messages is Thursday, December 6, 2002. Obviously, December 6, 2002, has not yet arrived. Moreover, December 6, 2001, was a Thursday, but December 6, 2002, will be a Friday.»

Dans l'arrêt *Richard Howard, Inc. v. Hogg*,²² le tribunal a exclu des courriers électroniques parce que le témoin qui a été produit pour les authentifier n'en

²⁰ No. CR.99-1382000, 2000 WL 288443, at 13, 14 (W.D. Mich. Jan. 25, 2000)

²¹ No. CIV.02-2002, 2002 WL 1205734, at 1, (D. Minn. May 31, 2002)

était ni l'auteur, ni le destinataire et il n'a offert aucune information additionnelle permettant d'établir qu'il avait une connaissance personnelle du fait que ces courriers électroniques ont effectivement été envoyés et reçus par les parties concernées.

En vertu de la règle 36 RFP, une partie peut, par voie de requête, demander à l'autre d'admettre l'authenticité de certains éléments de preuve avant la tenue du procès. Si la partie adverse refuse et qu'une preuve d'authenticité à l'égard de ces éléments de preuve est subséquemment présentée avec succès au procès, la partie qui a refusé d'admettre l'authenticité de ces éléments de preuve peut être contrainte par le tribunal à défrayer les frais découlant de cette preuve.

Les questions d'authenticité peuvent également être résolues dans le cadre de la conférence préparatoire au procès par voie d'admission des parties. Il en va de même lors des interrogatoires au préalable.

- Pertinence

La pertinence est une question laissée à l'appréciation du juge.

Ainsi, dans l'arrêt *Strauss v. Microsoft Corp.*,²³ l'intimé a attaqué l'admissibilité en preuve d'un courrier électronique qui lui était dommageable en alléguant qu'il n'est pas pertinent au litige, qu'il cause un préjudice indu, qu'il tend à confondre ou à embrouiller le jury. Le tribunal a admis le courrier électronique en preuve puisqu'il le considère pertinent pour établir un motif en vertu duquel Microsoft a failli à son obligation de faire la promotion des affaires du demandeur (question en litige) et que la valeur probante de ce courrier électronique est plus importante que son effet préjudiciable.

- Le ouïe dire

La question du ouïe dire est souvent invoquée en regard des courriers électroniques. La résolution de ces questions dépend de l'identité de l'auteur, du contenu du message et de la disponibilité d'un témoin pour authentifier le courrier électronique concerné.

Il arrive souvent que les courriers électroniques relatent des faits ou des informations qui n'ont pas été observés directement par leurs auteurs ou leurs destinataires et qui leur ont été relatés par des tierces parties. Il s'agit alors de double ouïe dire. Les courriers électroniques peuvent aussi contenir des témoignages d'opinion, ce qui n'est généralement pas admissible en preuve.

²² No. 12-95-5, 1996 WL 689231, at 3 (Ohio APP. Nov. 19, 1996)

²³ No. CIV. 91-5928, 1995 WL 326492, at 1 (S.D.N.Y., Jun. 1, 1995)

La partie qui veut introduire des courriers électroniques en preuve doit donc établir que ceux-ci ne constituent pas du ouïe dire ou qu'ils sont couverts par les exceptions prévues à la règle du ouïe dire.

Par exemple, une des exceptions à la règle du ouïe dire porte sur les admissions qui sont contraires aux intérêts de celui, de celle ou de ceux qui les ont faites (804 (b) (3) RFP). La logique de cette exception se trouve dans le fait qu'une admission par une partie qui est tellement nuisible à ses propres intérêts possède une valeur probante suffisante pour contrer le fait qu'elle a pu être faite par une partie qui n'est pas directement interrogée aux fins du litige.

Ainsi, dans l'arrêt *Vermont Elec. Power Co., Inc. v. Hartford Steam Boiler Inspection and Ins. Co.*,²⁴ le tribunal a statué qu'un courrier électronique contenant l'affirmation à l'effet qu'un rapport d'expert n'est pas concluant à l'égard d'une question faisant l'objet d'un litige avec un assureur constitue une admission contraire aux intérêts de la partie qui l'a faite et donc admissible en preuve à titre d'exception à la règle du ouïe dire.

Il a été jugé à plusieurs reprises que les courriers électroniques ne constituent pas des documents, registres ou compilations confectionnés régulièrement par les entreprises dans le cours normal des affaires. En conséquence, il a été statué que l'exception à la règle du ouïe dire au titre des « Business Records » ne s'applique généralement pas aux courriers électroniques.²⁵

- o La règle de la meilleure preuve

Cette règle veut qu'à moins d'exceptions, un écrit doit être prouvé à l'aide de son original. De plus, cette règle requiert que lorsqu'une preuve de meilleure valeur existe quant à l'objet à prouver, il faille y avoir recours plutôt que de recourir à une preuve de moindre valeur. Tel que discuté plus tôt, les documents en forme électronique susceptibles d'être lus à l'aide d'un appareil ou à l'œil nu constituent des écrits admissibles en preuve.

Mentionnons certains arrêts aux fins desquels des courriers électroniques ont été admis en preuve pour prouver la conduite inappropriée d'un agent de la paix qui qualifiait les élus municipaux de « porcs, de tricheurs et de menteurs »,²⁶ ou pour démontrer qu'un employé congédié pour absentéisme avait été notifié de la politique de son employeur à cet égard.²⁷

²⁴ 72 F. Supp. 2d 441 (D. Vt. 1999)

²⁵ *United States v. Ferber*, 966 F. Supp. 90 (D. Mass. 1997).

Monotype Corp. PLC v. International Typeface Corp., 43 F.3d 443 (9th Cir. 1994)

²⁶ *Plymouth Police Broth. V. Labor Relations Com'n*, 417 Mass. 599, 630 N.E. 2d 599 (1994)

²⁷ *Jenkins v. Department of Veterans Affairs*, 132 F. 3d 54, (Fed. Cir. 1997)

En matières criminelles, un tribunal a statué que les courriers électroniques d'un individu à une dame avec laquelle il a eu une liaison amoureuse étaient admissibles pour établir un motif aux fins de son accusation du meurtre au premier degré de son épouse.²⁸

- **Documents, registres, compilations et mémorandums d'affaires en forme électronique**

Ceci réfère aux divers registres en forme électronique compilés par les entreprises. Il peut s'agir des registres comptables habituels, des divers rapports périodiques, des comptes de téléphone, des états de banque, des mémos interservices, etc.

Comme tout autre élément de preuve, les registres en forme électronique doivent satisfaire les règles de preuve à l'égard de l'authenticité, la pertinence, le ouïe dire et la règle de la meilleure preuve.

Tels les courriers électroniques, les particularités découlant de la forme électronique de ces registres ont leur plus grande incidence au niveau de la mise en preuve de leur authenticité.

- L'authenticité

Les tribunaux diffèrent quant au type et la quantité de la preuve nécessaire pour authentifier les registres d'affaires en forme électronique.

Certains tribunaux requièrent une preuve plus élaborée pour établir la fiabilité de l'ordinateur particulier utilisé pour compiler ces données, la véracité des données à l'entrée et à la sortie et quant à l'identité du témoin éligible à authentifier ces registres.

D'autres tribunaux ont statué que si les registres d'affaires en forme électroniques sous examen satisfont l'exception au titre des « *Business Records* » aux fins de la règle du ouïe dire, leur fiabilité est alors présumée et aucune preuve additionnelle à cet égard n'est nécessaire.

Face à une telle diversité de vues par les tribunaux, il est donc prudent de produire un témoin qui soit celui ou celle chargé de maintenir les registres d'affaires en forme électronique sous examen ou qui soit familier avec la façon dont ils sont compilés et maintenus pour les authentifier. À l'aide de ce témoin, il s'agira d'établir ce qui suit :

- que l'entreprise utilise des ordinateurs dans le cours normal de ses affaires;

²⁸ *Allen v. State*, 862 P.2d 487 (Okl. Cr. 1993)

- que l'ordinateur utilisé à la compilation des registres visés est fiable et qu'il est utilisé à maintenir des registres d'affaires et à produire des représentations écrites de ceux-ci (« *Printout* »);
- que les logiciels et formules utilisés à la compilation des registres visés fonctionnent correctement;
- que des mesures appropriées sont en place afin de vérifier que ces logiciels et formules fonctionnent correctement;
- que l'entreprise a mis en place des mesures servant à contrôler la fiabilité des données d'entrée servant de base à la compilation des registres visés;
- quant à la manière dont les données de base ont été entrées aux fins de la compilation des registres visés;
- que les données de base ont été entrées dans un délai raisonnable après l'occurrence des événements auxquels elles se rapportent et que l'information de base ait été fournie par des personnes ayant une connaissance personnelle de ces événements;
- que les données ont été entrées dans le cours normal des affaires;
- quant à la méthode d'entreposage des données et les précautions mises en place pour en assurer la sauvegarde;
- l'ordinateur utilisé était en état d'usage au moment où le témoin a obtenu le « *Printout* »;
- le « *Printout* » provient de l'ordinateur concerné;
- le témoin peut identifier l'élément mis en preuve comme étant le « *Printout* » produit par l'ordinateur concerné;
- le témoin peut expliquer tout symbole ou termes inusités contenu dans le « *Printout* ».

Il est facile de constater que ce processus peut devenir excessivement laborieux... C'est la raison pour laquelle les parties procèdent généralement par voie d'admission avant la tenue du procès.

o Le ouïe dire

Les registres d'affaires en forme électronique se qualifient généralement aux fins de l'exception à la règle du ouïe dire au titre des « *Business Records* » (803(6) RFP).

Ainsi, dans l'arrêt *Sea-Land Service, Inc. v. Lozen Intern, LLC.*,²⁹ le tribunal a statué comme suit :

« *for the purposes of Rule 803(6), it is immaterial that the business record is maintained in a computer rather than in company books.* »

²⁹ 285 F.3d 809, 819 (9th Cir. 2002)

Dans l'arrêt *Sears Roebuck & Co. v. Meria*,³⁰ le tribunal a statué comme suit:

“computerized bookkeeping has become commonplace. Because the business records exception is intended to bring the realities of the business world into the courtroom, a record kept on computer in the ordinary course of business qualifies as competent evidence.”

Dans la mesure où les registres d'affaires en forme électronique sont maintenus dans le cours normal des affaires, qu'il est pratique normale pour l'entreprise de maintenir de tels registres et que ceux-ci soient authentifiés par un témoin approprié, ces registres se qualifient sous l'égide de l'exception applicable aux “Business Records” aux fins de la règle du ouïe dire et sont donc admissibles en preuve devant les tribunaux.

La rationnelle sous-jacente à cette pratique veut que les entrées d'information routinières, faites avec fiabilité et sur lesquelles se base normalement les entreprises commerciales pour fonctionner sont dignes de confiance.

L'arrêt *United States v. De Georgia*,³¹ résume très bien ces règles :

« Regularly-maintained business records are admissible in evidence as an exception to the hearsay rule because the circumstance that they are regularly maintained records upon which the company relies in conducting its business assures accuracy not likely to be enhanced by introducing into evidence the original documents upon which the records are based.

In our view, this same circumstance offers a like assurance that if a business record designed to note every transaction of a particular kind contains no notation of such a transaction between specified dates, no such transaction occurred between those dates. Moreover, in our opinion, that assurance is not likely to be enhanced by the only other means of proving such a negative; that is by bringing into court all of the documents involving similar transactions during the period in question to prove that there was no record of the transaction alleged not to have occurred, and calling as witnesses all company personnel who had the duty of entering into transactions of that kind during the critical period and inquiring whether the witnesses remembered any additional transactions for which no record had been produced.”

Dans l'arrêt *Potamkin Cadillac Corp., v. B.R.I. Coverage Corp.*,³² le tribunal a refusé d'admettre en preuve un « Printout » informatique produit par un courtier d'assurance parce que celui-ci n'a pas su démontrer que ce document est préparé dans le cadre d'une pratique courante de son entreprise non plus que la fiabilité de ce document.

³⁰ 142 N.J. Super. 205, 361 A.2d 68, 69 (1976)

³¹ 420 F.2d 889, 893 (9th Cir. 1969)

³² 38 F.3d 627 (2d Cir. 1994)

- Règle de la meilleure preuve

Les mêmes considérations que celles mentionnées aux fins des courriers électroniques s'appliquent à ce titre dans le cas des registres d'affaires en forme électronique.

- **Chambres de clavardage (« *Chat Rooms* ») et Groupes de discussion (« *News Groups* »)**

La plupart du temps, l'information échangée entre les participants à ces services est sauvegardée, que ce soit sur l'ordinateur de chaque participant ou sur ceux des fournisseur de services.

Ces services offrent des façons d'échanger de l'information entre participants, que ce soit lors de conférences en temps réel (clavardage) ou en temps différé (groupes de discussion et listes de discussion).

Les fournisseurs de ces services sont donc susceptibles de se voir ordonner de produire l'information relative aux échanges de certains de leurs usagers par voie de subpoena.

Les chambres de clavardage et les groupes de discussion présentent des caractéristiques uniques en ce sens que les participants ne sont pas propriétaires du site où ces échanges ont lieu. De plus, les participants n'utilisent généralement pas leur nom réel pour échanger mais plutôt des pseudonymes. Ceci pose des problèmes particuliers au niveau des règles portant sur l'authenticité de la preuve soumise.

- L'authenticité

Tel que mentionné précédemment, en vertu de la règle 901(a) RFP, la règle de l'authenticité est satisfaite lorsqu'il peut être démontré à la satisfaction du tribunal que la preuve soumise est bien ce qu'elle est censée être. Dans le cas des chambres de clavardage et des groupes de discussion, cette règle nécessite de mettre l'emphase sur les points suivants:

- les caractéristiques de la procédure d'adhésion à ces services, notamment quant à l'identité des usagers et le ou les pseudonymes associés à leur identité ;
- diverses occurrences où les usagers concernés ont utilisé le ou les pseudonymes associés à leur identité alors qu'ils participaient à ces services ;
- preuve démontrant que le ou les usagers visés ont participé aux échanges sous examen ;
- tout autre élément de preuve pertinent servant à associer l'identité d'un usager avec le ou les pseudonymes reliés aux échanges sous examen ;

- lorsque possible, examen de l'ordinateur utilisé par les usagers visés pour recueillir des éléments de preuve démontrant leur participation aux échanges sous examen.

Ainsi, dans l'arrêt *Raytheon Co. v. John Does*,³³ des utilisateurs de l'Internet ont publié de l'information technique confidentielle appartenant à *Raytheon* dans des chambres de clavardage et sur des babillards électroniques. À l'aide de subpoenas auprès de *Yahoo!* et d'autres fournisseurs de tels services, *Raytheon* est parvenue à identifier les utilisateurs qui ont publié cette information malgré qu'ils ont agi ainsi sous le couvert de pseudonymes. Ces utilisateurs avaient utilisé des pseudonymes tels « Raytheonveteran », « Ditchraytheon » et « Rayman-Mass ».

Dans l'arrêt *United States v. Tank*,³⁴ le tribunal a statué que le gouvernement a fait une preuve *prima facie* (à sa face même) d'authenticité en présentant une preuve suffisante pour permettre à un juré raisonnable de croire que les comptes rendus imprimés des discussions survenues dans une chambre de clavardage qui ont été produits sont bien ce qu'ils sont censés être. Le gouvernement a aussi établi un lien entre Tank et les comptes rendus provenant de cette chambre de clavardage. Le tribunal a admis en preuve les comptes rendus de discussions qui sont survenues dans les chambres de clavardage entre des membres d'un club Internet impliqué dans la pornographie juvénile.

- **Contenu des sites Web**

Le contenu des sites Web peut changer très souvent. Le contenu de sites Web réside généralement sur le ou les disques durs d'un ordinateur. Il peut aussi arriver que ce contenu se retrouve également sur des sites miroirs disséminés à travers le monde. De plus, certains sites contiennent des pages statiques et d'autres contiennent des pages dynamiques qui sont régénérées automatiquement par des régénérateurs de pages. Finalement, il arrive souvent que le contenu de ces divers sites miroirs ne soit pas synchronisé entre les divers sites qui les reproduisent.

- L'authenticité

Les plus grosses difficultés au niveau de la mise en preuve du contenu des sites Web réside dans son authenticité et sa fiabilité. Le nerf de la guerre consiste à établir que le contenu se trouvait sur le site Web visé, que l'élément offert en preuve reflète ce contenu avec précision et démontrer l'existence d'un lien entre l'élément offert en preuve et le propriétaire du site Web en question.

³³ 164 N.J. 38, 62, 751 A.2d 538 (N.J. 2000)

³⁴ 200 F.3d 627, 630 (9th Cir. 2000)

Plusieurs facteurs peuvent aider à établir cette preuve :

- l'adresse Internet unique URL (« *Uniform Resource Locator* »);
- l'identité du propriétaire ou opérateur du site Web (recherche « *Whois* »);
- un témoin qui inscrit l'adresse du site Web et qui le fait apparaître devant le tribunal;
- des marques distinctives qui apparaissent sur le site Web, tels logos de compagnies, etc ;
- reproduction imprimée du site Web;
- témoin qui a une connaissance personnelle du site Web et de son contenu, tel un employé du propriétaire ou de l'opérateur de ce site;
- sites Web gouvernementaux qui bénéficient d'une présomption d'authenticité à titre de publications d'une autorité publique (règle 902(5) RFP).
- Sites Web d'entreprises qui pourraient contenir de l'information se qualifiant à titre de « *Business Records* ».

Dans l'arrêt *St. Clair v. Johnny's Oyster & Shrimp, Inc.*,³⁵ après que la plaignant eut été blessé sur un navire, il a tenté d'établir la propriété du dit navire à partir d'informations recueillies d'un site Web. Le tribunal a rejeté cette preuve, jugeant que son authenticité et sa fiabilité n'a pas été démontrée de façon satisfaisante et s'est prononcé comme suit:

« While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon... There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content of any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, under the most liberal interpretation of the hearsay exception rules found in Fed. R. Evid. 807. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form. »

Cet arrêt illustre très bien les défis qui attendent ceux ou celles qui veulent tenter d'établir l'authenticité et la fiabilité des informations recueillies sur des sites Web qui ne sont pas publiés par des organismes publics...

³⁵ 76 F. Supp. 2d 773, 774, 775 (S.D. Tex. 1999)

o Le ouïe dire

Il s'agit des mêmes considérations que pour les autres types de documents en forme électronique. Il faut voir si l'information sous examen puisse se qualifier aux fins des exceptions à la règle du ouïe dire lorsqu'il n'est pas possible de produire l'auteur des informations sous examen., ou un témoin qui en a une connaissance personnelle.

Dans certains cas, la mise en preuve de certaines informations apparaissant sur des sites Web ne sert pas nécessairement à prouver la véracité des assertions qu'elles contiennent, ce qui résulte inévitablement à des objections basées sur le ouïe dire, mais sert plutôt à démontrer que cette information a bel et bien été publiée sur un ou des sites Web particuliers. Ainsi, si un client achète un téléviseur d'un vendeur d'appareils électroniques sur l'Internet, il pourrait très bien chercher à mettre en preuve, par exemple, qu'il s'est fié au fait que le vendeur a inscrit sur son site Web une information à l'effet que ce téléviseur est assorti d'une garantie pour motiver sa décision de l'acheter.

Dans un tel cas, il ne s'agit pas de prouver la véracité des informations afférentes à la garantie offerte mais bien de prouver que le vendeur a indiqué sur son site Web que ce téléviseur est assorti d'une garantie et que ce fait a influencé la décision de l'acheteur.

Dans une telle situation, ces informations ne constituent pas du ouïe dire et sont donc admissibles en preuve.³⁶

³⁶ *Ries Biologicals, Inc. v. Bank of Santa Fe*, 780 F.2d 888 (10th Cir. 1986)

2. C. Le Québec

2. C. I. Cadre statutaire

« Depuis quelques années, notre société assiste à ce que d'aucuns appellent une révolution technologique. De l'avènement du micro-ordinateur dans nos foyers et sur nos bureaux à l'Internet en passant par l'arrivée de la télécopie et plus récemment, de la signature électronique, nos façons de communiquer ont été transformées. Or, c'est souvent par la communication qu'évoluent des situations juridiques. Que nous pensions aux offres de contracter, à la conclusion des contrats eux-mêmes ou encore, au libelle diffamatoire, il s'agit de communications qui entraînent des effets juridiques que nous connaissons. Or, si le droit substantif qui encadre ces situations juridiques n'a pas été affecté par l'arrivée des nouvelles technologies, les contrats se formant toujours par le consentement des parties peu importe la façon par laquelle ce consentement est exprimé, les règles du droit de la preuve ont dû être adaptées à cette nouvelle réalité. En effet, il n'est plus vrai que seuls l'écrit, le témoignage et les autres moyens de preuve permettent d'établir le consentement réciproque des parties à être liées par un contrat, car depuis quelques années et pour l'avenir, une personne peut manifester sa volonté à être liée par contrat par un simple « clic » de souris. »³⁷

Comment les règles de preuve de la Province de Québec ont-elles été adaptées pour faire face à cette nouvelle réalité ?

Cette adaptation a débuté dès l'adoption du Code Civil du Québec (L.Q. 1991 C. 64) qui a remplacé le Code Civil du Bas Canada en 1994. Ainsi, les chapitres VI et VII du Livre Septième du Code Civil du Québec (C.c.Q.) ont été introduits par la loi précitée spécifiquement aux fins des technologies de l'information.

En 1996, la commission des Nations Unies pour le droit commercial international a adopté une loi type sur le commerce électronique. Cette loi type avait pour but de fournir aux pays membres un modèle de législation à l'égard des nouvelles technologies, d'harmoniser autant que possible les législations nationales pour favoriser l'explosion du commerce électronique à l'échelle mondiale.³⁸

En 1998, la Conférence pour l'harmonisation des lois au Canada a publié la Loi uniforme sur le commerce électronique³⁹ dans le but d'adapter le modèle de loi de l'O.N.U. à la réalité canadienne et de fournir aux provinces canadiennes un modèle de législation à l'égard du commerce électronique.

³⁷ Me Michel Gagné, La preuve dans un contexte électronique, Service de la formation permanente, Barreau du Québec, Développements récents en Droit de l'Internet (2001) Cowansville, Les Éditions Yvon Blais Inc. page 59.

³⁸ Voir la Loi type sur le commerce électronique de l'O.N.U. à <http://www.uncitral.org/french/texts/electcom/ml-ecomm-f.htm>

³⁹ Voir la Loi uniforme sur le commerce électronique du Canada à <http://www.law.ualberta.ca/alri/ulc/acts/fueca.htm>

Le 21 juin 2001, le législateur québécois a adopté la Loi concernant le cadre juridique des technologies de l'information.⁴⁰ Celle-ci est entrée en vigueur le 1^{er} novembre 2001. Elle apporte des précisions à nos règles de preuve à l'égard des nouvelles technologies qui se sont concrétisées par des modifications importantes aux chapitres VI et VII du Livre Septième du C.c.Q. La loi précitée agit à titre de supplément aux dispositions du C.c.Q. en matières de preuve.

En conséquence, les règles de preuve en droit québécois sont prévues au Livre Septième du C.c.Q, soit aux articles 2803 à 2874 C.c.Q, et à la Loi concernant le cadre juridique des technologies de l'information, dont certaines dispositions sont à toutes fins pratiques reproduites dans leur intégralité aux articles 2837 à 2842 C.c.Q. à l'égard des documents sur support technologique.

2. C. II. Le régime de preuve

Malgré ce qu'on peut bien en croire, le régime de preuve en droit québécois a beaucoup de similarités avec celui des États-Unis ou celui du reste du Canada. Les grands principes demeurent les mêmes et les différences se retrouvent dans les modalités d'application.

Les différences les plus importantes consistent au fait qu'il n'y a pas de procès devant jury en matières civiles au Québec et dans le reste du Canada. De plus au Québec, le « *Discovery Process* » de la « *Common Law* » par lequel les parties sont tenues d'énumérer et de fournir la liste des documents pertinents au litige (« *Affidavit of Documents* ») ne retrouve pas sa contrepartie au Québec. Au Québec, une partie n'est tenue de fournir que ce que l'autre lui demande. Ceci pose une limite importante aux documents (autant sur support papier qu'en forme électronique) que les parties peuvent obtenir de leurs adversaires, surtout au niveau des documents en forme électronique qui ont fait l'objet de la fonction « Supprimer » mais qui demeurent disponibles sur les supports ayant servi à les contenir. Il en va de même pour le « *Metadata* », pourtant crucial quant à l'information qu'il peut contenir. La jurisprudence québécoise interdit à une partie de procéder par une « recherche à l'aveuglette » lorsqu'elle demande que des documents lui soient communiqués. Une demande de communication de l'ensemble des documents enregistrés sur un disque dur constituerait une « expédition de pêche » selon l'expression consacrée.

Il est à espérer qu'on réalise enfin au Québec que les normes sociales ayant guidé ces règles strictes quant à la production de documents sont devenues obsolètes et que la nouvelle réalité que nous vivons fait en sorte que la bonne foi ne peut plus se présumer d'une façon aussi naïve que ce fut peut être le cas il y a de ça bien longtemps. Cette réalité commence à se refléter à l'égard d'autres parties de notre droit civil telles la responsabilité et les obligations et il serait fort heureux que nous adoptions une approche similaire à celle des juridictions de *Common Law* à l'égard de la production des documents pertinents aux litiges.

⁴⁰ L.Q. 2001, c.32. Voir à <http://www.canlii.org/qc/legis/loi/c-1.1/20040323/tout.html>

En guise de comparaison, il a été jugé en Ontario ⁴¹ que le disque dur d'un ordinateur doit être produit aux fins du « *Discovery Process* » et non seulement les informations qu'il contient en forme de rapport imprimé (« *Printout* »), Le tribunal s'est exprimé ainsi :

« The ambit of « electronic discovery » is very broad indeed. For example, Rule 30.02 of Ontario's Rules of Civil Procedure defines the scope of discovery in civil cases; para. 30.02(1) requires disclosure of every "document"; and para. 30.1(1)(a) defines "document" to include... "and information recorded or stored by means of any device." This would allow access to metadata, residual data, « file-properties » data and other information beyond the core document at issue: this additional information would reveal who created the document, when, how many versions it went through, etc.»

On ne peut qu'applaudir une telle décision. Quant à l'approche préconisée au Québec, on ne peut plus croire, en l'an 2005, qu'une partie à un litige puisse connaître la totalité des documents pertinents au litige en possession de son adversaire pour ensuite lui demander de les produire, conformément aux règles de production de documents toujours en vigueur à ce titre. Ceci est tout simplement risible. Des solutions techniques abondent pour composer avec l'énorme quantité de documents en forme électronique et leur contenu. Il est donc à espérer que nos législateurs et la profession juridique, malheureusement deux entités à fort biais corporatiste, acceptent enfin de s'adapter aux us et coutumes qui prévalent aujourd'hui...

Par ailleurs, le droit québécois établit aussi une différence entre un acte juridique et un fait juridique. Cette différence influence la qualité de la preuve requise pour établir la recevabilité et la force probante des éléments soumis en preuve devant le tribunal.

Ainsi, l'acte juridique est défini comme toute manifestation de volonté individuelle qui est destinée à créer, modifier ou éteindre un droit. ⁴² Le meilleur exemple d'un acte juridique est le contrat. Comme nous l'aborderons plus loin dans la présente section, sauf exception, la règle de la meilleure preuve requiert que les actes juridiques soient prouvés à l'aide d'un écrit (document).

Un fait juridique constitue tout acte ou événement qui ne peut pas être qualifié d'acte juridique. Les faits juridiques se prouvent par témoin ou à l'aide d'un écrit.

La personne qui pose un acte juridique prévoit généralement ses conséquences alors que celle qui participe à un fait juridique n'avait probablement pas prévu ni voulu les conséquences qui en découlent.

⁴¹ *Reichmann v. Toronto Life Publishing Co. (1988), 66 O.R. (2d) 65 at 67.*

⁴² Jean-Louis Beaudoin, Pierre-Gabriel Jobin, *Les Obligations*, 5^e éd., Cowansville, Éditions Yvon Blais, 1998, p.40

En dernière analyse, la similitude des régimes de preuve n'a rien de bien sorcier puisque la preuve, somme toute, consiste en des écrits (documents), des témoignages et des éléments matériels (le pistolet ayant servi au crime, l'œuvre d'art assuré, par exemple) peu importe la juridiction dans laquelle on se retrouve. L'article 2811 C.c.Q. énumère en fait cinq moyens de preuve au Québec, les deux autres étant l'aveu (en somme, une variation du témoignage) et la présomption (c'est-à-dire une fiction créée par la loi). Un sixième moyen de preuve est parfois admis, soit l'affidavit détaillé, qui est lui aussi une forme dérivée de la preuve testimoniale.

Tout comme aux États-Unis, la preuve en matières civiles au Québec se fait par prépondérance des probabilités. Cette règle est énoncée à l'article 2804 C.c.Q. comme suit :

« La preuve qui rend l'existence d'un fait plus probable que son inexistence est suffisante, à moins que la loi n'exige une preuve plus convaincante. »

Au Québec, comme ailleurs, la preuve devant les tribunaux doit donc respecter les grands principes suivants :

- La règle de la pertinence

L'article 2857 C.c.Q. établit la règle de la pertinence comme suit :

« La preuve de tout fait pertinent au litige est recevable et peut être faite par tous moyens. »

Cette règle est tempérée par l'article 2858 C.c.Q. qui stipule ce qui suit :

« Le tribunal doit, même d'office, rejeter tout élément de preuve obtenu dans des conditions qui portent atteinte aux droits et libertés fondamentaux et dont l'utilisation est susceptible de déconsidérer l'administration de la justice.

Il n'est pas tenu compte de ce dernier critère lorsqu'il s'agit d'une violation du droit au respect du secret professionnel. »

Les tribunaux ont été appelés à appliquer cette règle à plusieurs reprises.

Ce qui suit est tiré du volume Collection de droit 2002 – 2003: Preuve et procédure:⁴³

« Ainsi, il a été statué qu'une preuve doit être pertinente et fiable.⁴⁴ Tout ce qui est probant doit être reçu en preuve.⁴⁵ Un fait est pertinent s'il doit influencer sur la décision à rendre.⁴⁶ Ce qui n'est pas pertinent n'est pas probant; ce qui n'est

⁴³ Cowansville, les Éditions Yvon Blais Inc, 2002, page 196.

⁴⁴ R. c. Mohan (1994) 2 R.C.S. 9, 37.j. Sopinka

⁴⁵ R. c. Seaboyer, (1991) 2 R.C.S. 577

⁴⁶ Gagnon c. Ludger Harvey et Fils Ltée, (1968) B.R. 939

*aucunement probant est inutile à la solution du litige; ce qui n'a aucune valeur probante est donc irrecevable en preuve.*⁴⁷

*Une preuve pertinente peut avoir deux objets : 1° elle se rapporte aux faits en litige, qu'elle vise à établir ou à contrer; 2° elle porte sur la valeur probante d'un élément de preuve présenté par une partie.*⁴⁸ »

La règle de la pertinence s'applique à tous les éléments de preuve soumis à l'approbation du tribunal.

- L'authenticité et la fiabilité

Ces règles s'appliquent aux écrits (documents). Elles se retrouvent aux articles 2812 à 2836 C.c.Q. Le but de ces règles est d'éviter la fraude, les fausses représentations et d'induire le tribunal en erreur par l'introduction de documents qui soient des faux ou qui ne soient pas fiables.

Le code civil établit diverses classes d'écrits, dont les actes authentiques, les actes semi authentiques, les actes sous seing privé et les autres écrits (ou écrits d'entreprises).

Les articles 2813 à 2821 C.c.Q. régissent les actes authentiques. L'article 2813 C.c.Q. stipule ce qui suit :

« L'acte authentique est celui qui a été reçu ou attesté par un officier public compétent selon les lois du Québec ou du Canada, avec les formalités requises par la loi.

L'acte dont l'apparence matérielle respecte ces exigences est présumé authentique. »

L'article 2814 C.c.Q. énumère une liste d'actes authentiques:

- Les documents officiels du Parlement du Canada et du Parlement du Québec;
- Les documents officiels émanant du gouvernement du Canada ou du Québec;
- Les registres des tribunaux judiciaires ayant juridiction au Québec;
- Les registres et les documents officiels émanant des municipalités et autres personnes morales de droit public constituées par une loi du Québec;
- Les registres à caractère public dont la loi requiert la tenue par des officiers publics;

⁴⁷ Morris c. La Reine, (1983) 2 R.C.S. 190

⁴⁸ Collection de droit 2002 – 2003: Preuve et procédure, Cowansville, les Éditions Yvon Blais Inc, 2002, page 196.

- L'acte notarié;
- Le procès-verbal de bornage.

En fait, ce sont des actes sous seing public. Ils font preuve en soi de leur confection. Ils peuvent être introduits devant les tribunaux sans qu'il soit nécessaire d'en établir l'authenticité par témoin.⁴⁹ Les actes authentiques bénéficient d'une présomption d'authenticité sans qu'il soit nécessaire de présenter toute autre preuve à cet égard.

Les articles 2822 à 2825 C.c.Q. régissent les actes semi authentiques. Il s'agit en somme des actes qui émanent d'un officier public étranger compétent à l'égard d'un individu domicilié au Québec.

En vertu de l'article 2822 C.c.Q., l'acte semi authentique « *fait preuve prima facie à l'égard de tous, de son contenu, sans qu'il soit nécessaire de prouver la qualité ni la signature de cet officier.* »

Les articles 2826 à 2830 C.c.Q. régissent les écrits sous seing privé. L'article 2826 C.c.Q. les définit comme suit :

« *L'acte sous seing privé est celui qui constate un acte juridique et qui porte la signature des parties; il n'est soumis à aucune autre formalité.* »

L'article 2828 C.c.Q. ajoute ceci :

« *Celui qui invoque un acte sous seing privé doit en faire la preuve* ».

Les articles 2831 à 2836 C.c.Q. régissent les autres écrits. Il s'agit en fait des écrits non signés utilisés dans le cours des activités d'une entreprise pour constater un acte juridique et l'écrit pur et simple qui rapporte un fait matériel.⁵⁰

Tout comme les écrits sous seing privé, l'article 2835 C.c.Q. stipule que celui qui invoque un écrit non signé doit prouver que cet écrit émane de celui qu'il prétend en être l'auteur. L'article 2836 C.c.Q. ajoute que ces écrits peuvent être contredits par tous moyens.

Les écrits purs et simples consistent en des documents tels états de banque, états financiers, registres comptables, articles de journaux, divers rapports, etc.

L'article 2835 C.c.Q. précité requiert que l'écrit pur et simple qui relate un fait matériel doive être mis en preuve par témoin. L'article 2843 C.c.Q. requiert que le

⁴⁹ Tremblay c. La Reine, (1978) R.L. 55 (C.A.)

⁵⁰ Collection de droit 2002 – 2003: Preuve et procédure, Cowansville, les Éditions Yvon Blais Inc, 2002, pages 211 et 212.

témoignage soit offert par un individu qui a eu personnellement connaissance du fait ainsi relaté.

Au même titre que ce qui a déjà été discuté aux fins du régime de preuve fédéral américain, une application stricte de ces règles peut rendre pratiquement impossible ou, à tout le moins très difficile, la mise en preuve de registres générés à des fins d'affaires.

Par contre, tel qu'il est indiqué dans Collection de droit 2002 – 2003 : Preuve et procédure,⁵¹ les écrits purs et simples confectionnés dans le cours normal des affaires peuvent tout de même être admis en preuve :

« Cependant, en pratique, les circonstances où une telle preuve sera recevable sont assez nombreuses. Ainsi, l'écrit pur et simple, confectionné de façon systématique dans le cours ordinaire des activités d'une entreprise, en raison de sa présumée fiabilité, peut faire preuve des faits matériels qu'il contient, du consentement explicite ou tacite des parties, comme l'autorise l'article 2869 C.c.Q., lesquelles, à l'instar de la portée de l'article 286 C.p.c., reconnaissent que l'auteur de cet écrit, s'il était entendu, déposerait des faits y paraissant, généralement incontestables. À titre d'exemples, le contenu du dossier médical d'un centre hospitalier, le relevé d'une institution financière, le rapport météorologique seront admis en preuve pour valoir comme témoignage, sans comparution de la personne qui a constaté ou colligé les faits y paraissant et dont le témoignage ne ferait qu'en répéter le contenu. Ces documents seront généralement introduits au dossier au moyen de l'article 403 C.p.c. Les avocats, soit spontanément entre eux, soit à l'occasion d'une conférence préparatoire, conviendront de la valeur probante à attacher à ce document, pour éviter si possible la comparution autrement inutile d'un témoin. »

Ainsi, un imprimé d'ordinateur (« Printout ») peut être admis en preuve.⁵² Des reçus de dépenses peuvent être admis en preuve.⁵³ Des états financiers préparés par une banque à l'égard d'une entreprise cliente peuvent être admis en preuve.⁵⁴ Certains documents font également foi de leur contenu en raison de dispositions particulières de la Loi. En voici quelques exemples:

- Copies des livres et registres maintenus par le dépositaire désigné du conseil d'administration d'une personne morale (article 343 C.c.Q.);
- La déclaration de société ou la déclaration modificative de société (article 2195 C.c.Q.);

⁵¹ Cowansville, les Éditions Yvon Blais Inc, 2002, page 213.

⁵² *N.S.K. Container Services Ltd. C. Flexi-Van Leasing Inc.*, (1992) R.D.J. 288 (C.A.)

⁵³ *Lavigne c. Marcoux*, J.E. 87-850 (C.S.)

⁵⁴ *Ferme Paul-René Courcelle et Fils Inc., c. Banque Canadienne Impériale de Commerce*, (1986) R.L. 63 (C.A.)

- Les inscriptions effectuées dans le cours ordinaire des affaires dans un livre ou registre tenu dans une institution financière (article 29 de la Loi sur la preuve au Canada);
- Le rapport d'un membre de la Sûreté du Québec peut valoir comme témoignage (article 294.1 C.p.c.).

Pour conclure quant à l'authenticité et la fiabilité des écrits (documents), des règles spécifiques prévoient la façon de contester chacun des divers types d'écrits (documents) classifiés par le code civil de même que la valeur probante qui leur est accordée.

Naturellement, les actes authentiques et semi authentiques ont une valeur probante élevée. Il est plus difficile d'en contester l'authenticité et la fiabilité.

En somme, dans le cas des actes authentiques et semi authentiques, le fardeau de preuve incombe à celui qui veut les contester alors que pour les actes sous seing privé et les autres écrits, c'est à celui qui les soumet en preuve à qui il incombe de les prouver.

- La règle de la meilleure preuve

L'article 2860 C.c.Q. consigne la règle de la meilleure preuve comme suit :

« L'acte juridique constaté dans un écrit ou le contenu d'un écrit doit être prouvé par la production de l'original ou d'une copie qui légalement en tient lieu.

Toutefois, lorsqu'une partie ne peut, malgré sa bonne foi et sa diligence, produire l'original de l'écrit ou la copie qui légalement en tient lieu, la preuve peut être faite par tous moyens. »

Mentionnons qu'en vertu des articles 2815 et 2816 C.c.Q., les copies authentifiées d'actes authentiques peuvent satisfaire la règle de la meilleure preuve.

En raison de la règle de la meilleure preuve, la preuve testimoniale ne peut généralement pas se substituer à la preuve écrite. Il existe certaines exceptions à ce principe par exemple lorsqu'une partie admet avoir signé un document écrit qui n'est pas disponible. Une telle admission constitue ce qui est appelé un commencement de preuve par écrit et permet de mettre en preuve le contenu de l'écrit manquant par témoins.

La règle du ouïe dire est une manifestation de la règle de la meilleure preuve en vertu de laquelle seuls les témoins de faits ayant eu une connaissance personnelle des faits matériels faisant l'objet du témoignage sont admissibles.

- Le ouïe dire.

Le ouïe dire est une preuve par personne interposée. Sauf exception, ce genre de preuve n'est pas recevable. La mise en preuve d'un fait matériel doit être faite par le témoignage d'une personne qui en a une connaissance personnelle.

Rapporter les paroles d'une autre personne ne constitue pas nécessairement du ouïe dire:

*« Il est établi en droit que la preuve d'une déclaration faite à un témoin par une personne qui n'est pas elle-même assignée comme témoin est une preuve par ouïe dire, qui est irrecevable lorsqu'elle cherche à établir la véracité de la déclaration; toutefois, cette preuve n'est pas du ouïe dire et est donc recevable lorsqu'elle cherche à établir, non pas la véracité de la déclaration, mais simplement que celle-ci a été faite. »*⁵⁵

*« Une déclaration extrajudiciaire qui est admise pour la véracité de son contenu est une preuve par ouïe dire. Une déclaration extrajudiciaire présentée tout simplement pour prouver que la déclaration a été faite n'est pas une preuve par ouïe dire et elle est admissible tant qu'elle a une certaine valeur probante. »*⁵⁶

Tout comme pour les fins du régime de preuve fédéral américain, il existe plusieurs exceptions à la règle du ouïe dire au Québec qu'il ne serait pas utile de décrire plus amplement dans le cadre du présent ouvrage.

2. C. III. Les documents en forme électronique

Tel que mentionné ci-devant, des modifications ont été apportées au régime de preuve du droit québécois suite à l'entrée en vigueur le 1^{er} novembre 2001 de la Loi concernant le cadre juridique des technologies de l'information. Notamment, les articles 2837 à 2842 C.c.Q. ont subi quelques aménagements pour les rendre compatibles à cette loi.

La première chose qu'il faille constater à l'examen de la loi précitée et des dispositions précitées du C.c.Q., est l'établissement du principe de la neutralité technologique et de l'équivalence et de l'interchangeabilité entre les divers types de documents. En principe, qu'ils soient sur support papier ou électronique, tous les documents sont soumis aux mêmes règles fondamentales de preuve décrites ci-devant.

Ainsi, l'article 2837 C.c.Q. établit le principe de l'équivalence des documents de divers types:

⁵⁵ R. c. O'Brien, (1978) 1 R.C.S. 591, 593, j. Dickson.

⁵⁶ R. c. Evans, (1993) 3 R.C.S. 653, 661, j. Sopinka pour la cour.

« L'écrit est un moyen de preuve quel que soit le support du document, à moins que la loi n'exige l'emploi d'un support ou d'une technologie spécifique. »

Lorsque le support de l'écrit fait appel aux technologies de l'information, l'écrit est qualifié de document technologique au sens de la Loi concernant le cadre juridique des technologies de l'information. »

À titre d'exemple de document dont la loi exige un support particulier, pensons aux actes notariés dont la Loi sur le notariat⁵⁷ exige qu'ils soient sur support papier.

L'article 2838 C.c.Q. introduit les critères d'admissibilité en preuve applicables spécifiquement aux documents technologiques, soit que leur intégrité soit assurée:

« Outre les autres exigences de la loi, il est nécessaire pour que la copie d'une loi, l'acte authentique, l'acte semi-authentique ou l'acte sous seing privé établi sur un support faisant appel aux technologies de l'information fasse preuve au même titre qu'un document de même nature établi sur support papier, que son intégrité soit assurée. »

L'article 2839 C.c.Q. indique ce qui est entendu par assurer l'intégrité des documents, soit que leur contenu ne soit pas altéré et qu'il soit maintenu dans son intégralité, que le support comme tel soit stable et qu'il assure la continuité ou la pérennité du document:

« L'intégrité d'un document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue. »

Lorsque le support ou la technologie utilisé ne permet ni d'affirmer ni de dénier que l'intégralité du document est assurée, celui-ci peut, selon les circonstances, être reçu à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve. »

Les articles 5 et 6 de la Loi concernant le cadre juridique des technologies de l'information précisent que pour que les documents technologiques aient la même valeur juridique que les documents équivalents sur support papier, leur intégrité doit être assurée tout au long de leur existence, depuis leur création, en passant par leur transfert, leur consultation et leur transmission, jusqu'à leur conservation y compris leur archivage ou leur destruction. De plus, le lien entre le ou les individus et le document technologique qui les concerne doit être maintenu en tout temps. Naturellement, les exigences de la loi pour chaque type d'écrit dont il est question doivent aussi être respectées par leurs équivalents technologiques.

⁵⁷ L.R.Q. c. C-25, art 30.

L'article 2840 C.c.Q. introduit la présomption d'intégrité des documents technologiques et impose le fardeau de preuve à celui qui veut prouver qu'ils ne sont pas intègres:

« Il n'y a pas lieu de prouver que le support du document ou que les procédés, systèmes ou technologies utilisés pour communiquer au moyen d'un document permettent d'assurer son intégrité, à moins que celui qui conteste l'admissibilité du document n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégralité du document. »

Il est utile de mentionner que l'article 89 (4) C.p.c. prévoit que celui qui veut contester l'intégrité d'un document technologique doit l'alléguer expressément et doit aussi appuyer cette contestation d'un affidavit.

L'article 2841 C.c.Q. traite de la reproduction des documents:

« La reproduction d'un document peut être faite soit par l'obtention d'une copie sur un même support ou sur un support qui ne fait pas appel à une technologie différente, soit par le transfert de l'information que porte le document vers un support faisant appel à une technologie différente.

Lorsqu'ils reproduisent un document original ou un document technologique qui remplit cette fonction aux termes de l'article 12 de la Loi concernant le cadre juridique des technologies de l'information, la copie, si elle est certifiée, et le document résultant du transfert de l'information, s'il est documenté, peuvent légalement tenir lieu du document reproduit.

La certification est faite, dans le cas d'un document en la possession de l'État, d'une personne morale, d'une société ou d'une association, par une personne en autorité ou responsable de la conservation du document. »

Finalement, l'article 2842 C.c.Q. ajoute ce qui suit :

« La copie certifiée est appuyée, au besoin, d'une déclaration établissant les circonstances et la date de la reproduction, le fait que la copie porte la même information que le document reproduit et l'indication des moyens utilisés pour assurer l'intégrité de la copie. Cette déclaration est faite par la personne responsable de la reproduction ou qui l'a effectuée.

Le document résultant du transfert de l'information est appuyé, au besoin, de la documentation visée à l'article 17 de la Loi concernant le cadre juridique des technologies de l'information. »

La Loi concernant le cadre juridique des technologies de l'information permet diverses façons d'établir un lien entre un individu et un document technologique. Il s'agit en fait de ce qui est communément appelé les signatures électroniques.

L'article 38 de la Loi concernant le cadre juridique des technologies de l'information stipule ce qui suit :

« Le lien entre une personne et un document technologique, ou le lien entre un tel document et une association, une société ou l'État, peut être établi par tout procédé ou par une combinaison de moyens dans la mesure où ceux-ci permettent:

1° de confirmer l'identité de la personne qui effectue la communication ou l'identification de l'association, de la société ou de l'État et, le cas échéant, de sa localisation, ainsi que la confirmation de leur lien avec le document;

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

L'article 39 de cette même loi ajoute :

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

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

L'article 2827 C.c.Q. stipule ce qui suit :

« La signature consiste dans l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement. »

Les dispositions de la Loi concernant le cadre juridique des technologies de l'information ne sont pas reproduites en entier au Code civil. Il faut donc y référer au besoin et cette loi sert donc de supplément aux règles de preuve autrement prévues au Code civil.

L'impact des caractéristiques propres aux documents en forme électronique quant à leur admissibilité en preuve tel que discuté dans le cadre du régime de preuve fédéral américain est tout aussi pertinent aux fins du régime de preuve québécois.

Donc, en plus de respecter les grands principes fondamentaux liés à l'admissibilité en preuve de tout élément de preuve soumis à l'appréciation du tribunal, soit la règle de la pertinence, l'authenticité et la fiabilité, la règle de la meilleure preuve et la règle du ouïe dire, il faut en plus que les documents en forme électronique (ou les documents technologiques au Québec) satisfassent aux conditions d'intégrité discutée ci-devant

quant à leur support particulier. Le lien entre le ou les individus et le document en forme technologique qui les concerne doit aussi être maintenu en tout temps.

Si on examine l'admissibilité des courriers électroniques en droit québécois, par exemple, il faut en tout premier lieu que leur contenu soit pertinent au litige, qu'ils puissent être authentifiés et introduits par un témoin qui en a une connaissance personnelle, que leur contenu respecte les règles de la meilleure preuve et du ouïe dire. Les règles de preuve usuelles applicables au type d'information qu'ils contiennent s'appliquent pour ces documents au même type que pour leur équivalent sur support papier. Ainsi, si les courriers électroniques contiennent les termes d'un acte sous seing privé constatant un acte juridique, tel un contrat, les règles de preuve applicables aux actes sous seing privé s'appliqueront. Dans un tel cas, celui qui invoque un acte sous seing privé doit en prouver le contenu (article 2828 C.c.Q.). En plus, en cas de contestation, il faut établir que ces courriers électroniques sont intègres, c'est-à-dire que leur contenu n'a pas été altéré et qu'il est maintenu dans son intégralité, et que le support qui les porte leur procure la stabilité et la pérennité voulue.

Il en va de même pour tous les autres types de documents en forme électronique. Il n'est pas nécessaire de répéter les caractéristiques propres à chaque type de document en forme électronique puisque ceci a déjà été fait dans le cadre de la discussion du régime de preuve fédéral américain. Il s'agit d'appliquer *mutatis mutandis* les règles de preuve du droit québécois.

2. D. Le Canada (règles fédérales)

2. D. I Le cadre statutaire

Les règles de preuve au Canada proviennent de la *Common Law* d'Angleterre, telle qu'adaptée à la réalité canadienne et nécessairement influencée par son évolution chez nos voisins Américains.

Au Canada, comme aux États-Unis et au Québec, les règles de preuve sont érigées sur les mêmes principes fondamentaux auxquels doivent satisfaire tout élément de preuve soumis à l'appréciation des tribunaux: la pertinence, l'authenticité et la fiabilité, la meilleure preuve et la prohibition du ouïe dire.

Quoique les modalités d'application des règles de preuve puissent différer quelque peu d'une juridiction à l'autre, les différences entre le régime de preuve du Canada et celui des États-Unis ne sont pas très grandes au niveau des quatre principes fondamentaux énumérés ci-devant, soit la règle de la pertinence, l'authenticité et la fiabilité, la règle de la meilleure preuve et la prohibition du ouïe dire. La *Common Law* n'étant pas un régime de droit codifié comme le droit civil québécois, ces principes ont évolué à travers une multitude de décisions rendues par les tribunaux canadiens à travers l'histoire du Canada. Il serait donc très fastidieux pour les fins du présent ouvrage de recenser toutes ces décisions et d'en faire la synthèse.

En conséquence, j'ai jugé préférable de ne pas m'éterniser sur une revue détaillée des modalités d'application de ces principes au droit de la preuve du Canada.

Somme toute, la règle de la pertinence parle par elle-même en ce sens que seuls les éléments de preuve pertinents au litige sont reçus en preuve. La règle de l'authenticité veut que celui qui introduit un élément de preuve puisse démontrer que celui-ci est bien ce qu'il est censé être. La règle de la meilleure preuve requiert que la meilleure preuve possible soit offerte au tribunal. Dans le cas des documents inscrits sur support papier, ceci implique que les originaux soient offerts en preuve plutôt que des copies. Dans le cas des témoins, sauf à l'égard des témoins experts qui témoignent sur leur domaine de compétence, ceci implique que les témoins de faits soient des individus qui ont une connaissance personnelle des faits à l'égard desquels ils témoignent. La prohibition du ouïe dire cherche à restreindre la présentation d'éléments de preuve par personnes interposées de sorte à permettre à la partie adverse de contre interroger ceux qui ont une connaissance personnelle des faits. Ceci dans l'optique que le contre interrogatoire par la partie adverse demeure l'outil par excellence aux yeux du tribunal pour établir la fiabilité des éléments de preuve soumis à son approbation.

Naturellement, plusieurs exceptions à ces règles ont été façonnées à travers le temps. Par exemple, les copies de documents faites conformément à des règles spécifiques peuvent satisfaire la règle de la meilleure preuve. Par ailleurs, une des premières exceptions à l'égard de la règle du ouïe dire concerne les inscriptions et copies d'inscriptions dans un livre ou registre tenu dans une institution financière (banque).

Ces inscriptions ont été jugées comme étant assez fiables pour faire preuve de leur contenu sans qu'il soit nécessaire d'ajouter aucune preuve additionnelle. Cette exception a plus tard été élargie aux inscriptions faites dans les livres et registres tenus par les entreprises dans le cours normal des affaires. Dans la même optique, puisque les inscriptions dans les livres et registres tenus par les entreprises commerciales dans le cours normal des affaires sont assez fiables pour leur permettre de bien gérer leurs affaires, elles sont aussi présumées être assez fiables pour faire la preuve de leur contenu devant les tribunaux sans preuve additionnelle.

Les règles de preuve en matières fédérales sont régies par la Loi sur la preuve au Canada.⁵⁸ Comme l'indique l'article 2 de cette loi, celle-ci s'applique à toutes les procédures pénales et civiles ainsi qu'à toutes les autres matières de compétence fédérale. Ainsi, l'exception à la règle du ouïe dire à l'égard des inscriptions et copie d'inscriptions dans les livres et registres tenus dans les institutions financières est codifiée à l'article 29 de la Loi sur la preuve au Canada. Celle plus générale à l'égard des inscriptions dans les livres et registres tenus dans le cours normal des affaires par les entreprises commerciales se retrouve à l'article 30 de cette loi.

Tel que mentionné auparavant, suite à l'adoption par l'O.N.U. en 1996 d'une loi type sur le commerce électronique, la Conférence pour l'harmonisation des lois au Canada a publié en 1998 la Loi uniforme sur le commerce électronique. Cette initiative a débouché sur le Projet de loi C-6, Chapitre 5 des Lois annuelles du Canada 2000, soit la Loi sur la protection des renseignements personnels et les documents électroniques.⁵⁹ Cette loi prévoit notamment des amendements à la Loi sur la preuve au Canada à l'égard des documents électroniques. Elle a été adoptée le 13 avril 2000 et les amendements à la Loi sur la preuve au Canada à l'égard des documents électroniques sont entrés en vigueur le 1^{er} mai 2000. La loi sur la preuve en Ontario a également fait l'objet d'amendements à l'égard des documents électroniques qui sont entrées en vigueur le 30 juin 2000.

2. D. II. Le régime de preuve à l'égard des documents en forme électronique

Avant la réforme mentionnée au paragraphe précédent qui a été introduite en l'an 2000, les documents en forme électronique étaient tout de même admis en preuve au Canada sous l'égide de l'exception à la règle du ouïe dire développée par la *Common Law* ou sous l'exception générale à l'égard des inscriptions aux livres et registres tenus dans le cours normal des affaires par les entreprises commerciales prévue à l'article 30 de la Loi sur la preuve au Canada.

⁵⁸ L.R. 1985, ch. C-5

⁵⁹ S.C. 2000, c-5, Partie 3.

Par exemple, la Cour d'Appel de la Colombie Britannique a admis en preuve un rapport imprimé (« *Printout* ») provenant du logiciel de comptabilité d'une entreprise sous l'égide de l'article 30 de la Loi sur la preuve au Canada.⁶⁰ Cette même cour a confirmé sa position à ce titre une douzaine d'années plus tard.⁶¹

Dans les cas où une loi particulière portant sur les règles de preuve ne pouvait permettre l'admission en preuve de documents en forme électronique parce que l'une quelconque des conditions qui y sont stipulées n'était pas satisfaite, l'exception à la règle du ouïe dire développée par la *Common Law* à l'égard des registres à fins d'affaires a alors été utilisée pour ce faire.⁶² L'arrêt *Kinsella v. Logan* de la Cour d'Appel du Nouveau Brunswick en constitue un excellent exemple.⁶³

Un autre arrêt⁶⁴ s'est penché sur des éléments de preuve accumulés sans intervention humaine. Puisque l'article 30 précité de la Loi sur la preuve au Canada nécessite l'intervention d'un être humain comme condition préalable à l'admission en preuve des inscriptions aux livres et registres dans le cours normal des affaires des entreprises commerciales, cet article ne pouvait pas être utilisé pour admettre en preuve l'information accumulée automatiquement par un ordinateur concernant le moment et la durée des appels téléphoniques faits par le prévenu dans cette affaire. La cour a décrété que cette information ne constitue pas du ouïe dire mais bien de la preuve directe qui est admissible. Le tribunal s'est exprimé comme suit:

« Where evidence is automatically recorded by any means, other than by human labour, and the evidence so recorded can be reproduced in any form, intelligible to the human mind, the reproduction is admissible as real evidence. The recording may be mechanical, chemical, electronic, photographic, or auditory, to name a few examples, and the reproduction may be by computer printout, audiovisual playback, photographs, or other means. The weight to be attached to such evidence will depend on the accuracy and integrity of the process employed. »

Naturellement, plusieurs décisions, parfois contradictoires, ont été rendues par les tribunaux canadiens sur cette question avec pour résultat que les documents en forme électronique constitués dans le cours normal des affaires par les entreprises et sur la base desquels celles-ci gèrent leurs affaires sont présumés fiables par nos tribunaux et admissibles en preuve. Cette présomption de fiabilité peut être renversée s'il est démontré à la satisfaction du tribunal que le processus par lequel ces documents sont confectionnés et maintenus n'est pas fiable ou intègre, que ces documents ne sont pas confectionnés dans le cours normal des affaires ou que les entreprises concernés ne s'y fient pas pour gérer leur affaires.

⁶⁰ *R. v. Vanlerberghe* (1976), 6 C.R. (3d) 222 (B.C.C.A.)

⁶¹ *R. v. Bicknell* (1988), 41 C.C.C. (3d) 545 (B.C.C.A.)

⁶² Concernant les exceptions à la règle du ouïe dire développées par la *Common Law*, voir les arrêts *R. v. Khan*, (1990) 2 S.C.R. 531 et *R. v. Seaboyer*, (1991) 2 S.C.R. 577.

⁶³ (1995), 163 N.B.R. 1 (N.B.Q.B.)

⁶⁴ *R. v. McCulloch*, (1992) B.C.J. No. 2282 (B.C. Prov. Ct.)

Un autre point intéressant digne de mention porte sur la quasi-disparition de la vieille distinction entre l'original d'un document et sa copie. Cette distinction découlait de la règle de la meilleure preuve durant l'ère des documents sur support papier et des copies transcrites à la main par un individu autorisé à ce faire. Depuis l'avènement de l'ère électronique, où l'information existe en forme de bit et de bytes, il est bien moins utile de tenter de distinguer entre un original et une copie que de s'assurer de l'intégrité et de la fiabilité des systèmes utilisés à accumuler l'information sous examen.

la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) a donné lieu à des amendements aux articles 31.1 à 31.8 de la Loi sur la preuve au Canada (LPC) à l'égard des documents en forme électronique.

L'article 31.8 LPC définit « document électronique » comme suit:

« Ensemble de données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable et qui peuvent être lues ou perçues par une personne ou par un tel système ou dispositif. Sont également visés tout affichage ou toute sortie imprimée ou autre de ces données. »

L'article 31.8 LPC définit « données » comme suit:

« Toute forme de représentation d'informations ou de notions. »

L'article 31.8 LPC définit « système informatique » comme suit:

« Dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs :

- a) contiennent des programmes d'ordinateur ou d'autres données ;*
- b) conformément à des programmes d'ordinateur, exécutent des fonctions logiques et de commande et peuvent exécuter toute autre fonction. »*

L'article 31.8 LPC définit « signature électronique sécurisée » comme suit:

« Signature électronique sécurisée au sens du paragraphe 31(1) de la Loi sur la protection des renseignements personnels et les documents électroniques. »

L'article 31 (1) LPRPDE définit « signature électronique sécurisée » comme suit:

« Signature électronique qui résulte de l'application de toute technologie ou de tout procédé prévu par règlement pris en vertu du paragraphe 48 (1). »

L'article 31 (1) LPRPDE définit « signature électronique » comme suit:

« Signature constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres symboles sous forme numérique incorporée, jointe ou associée à un document électronique. »

L'article 31.8 LPC définit « système d'archivage électronique » comme suit:

« Sont assimilés au système d'archivage électronique le système informatique et tout dispositif semblable qui enregistre ou met en mémoire des données ainsi que les procédés relatifs à l'enregistrement ou à la mise en mémoire de documents électroniques. »

L'article 31.1 LPC établit ce qui suit à l'égard de la règle de l'authenticité:

« Il incombe à la personne qui cherche à faire admettre en preuve un document électronique d'établir son authenticité au moyen d'éléments de preuve permettant de conclure que le document est bien ce qu'il paraît être. »

Le paragraphe 31.2 (1) LPC établit ce qui suit à l'égard de la règle de la meilleure preuve:

« 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.*

Le paragraphe 31.2 (2) LPC ajoute ce qui suit:

« Malgré le paragraphe (1), sauf preuve contraire, 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. »

L'article 31.3 LPC prévoit ce qui suit à l'égard des systèmes d'archivage électroniques:

« 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 autre 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.*

L'article 31.4 LPC permet d'établir des présomptions comme suit:

« 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.*

L'article 31.5 LPC ajoute ce qui suit quant à l'admissibilité en preuve de documents électroniques:

« 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. »

L'article 31.6 (1) LPC permet une preuve par affidavit comme suit:

« La preuve des questions visées au paragraphe 31.2 (2) et aux articles 31.3 et 31.5 ainsi que dans les règlements pris en vertu de l'article 31.4 peut être faite par affidavit. »

L'article 31.6 (2) LPC permet le contre interrogatoire comme suit:

« Toute partie peut contre interroger l'auteur d'un affidavit visé au paragraphe (1) et déposé en preuve:

- a) *de plein droit, dans le cas où l'auteur de l'affidavit est une partie adverse ou est sous l'autorité d'une telle partie;*
- b) *avec l'autorisation du tribunal, dans les autres cas.*

Enfin, l'article 31.7 LPC clarifie ce qui suit:

« Les articles 31.1 à 31.4 n'ont pas pour effet de restreindre l'application des règles de droit relatives à l'admissibilité de la preuve, à l'exception des règles de droit régissant l'authentification et la meilleure preuve. »

Ces nouvelles dispositions de la LPC confirment l'admissibilité en preuve des documents en forme électronique au Canada et font disparaître les difficultés qui surgissaient à ce titre en raison de dispositions qui ont été adoptées alors que les technologies de l'information modernes n'existaient pas encore.

Ces documents bénéficient d'une présomption de fiabilité qu'il est toujours possible de renverser, L'histoire démontre que rares sont les avocats qui se lancent dans des batailles futiles pour établir que des documents en forme électronique confectionnés par les entreprises dans le cours normal des affaires ne sont pas fiables et ne devraient pas être admis en preuve. Ceci demeure toutefois dans le domaine du possible dans les rares cas où il peut être démontré que ces documents ont pu être altérés ou que les systèmes utilisés sont déficients et ne sont vraiment pas fiables.

Tel que mentionnée précédemment, tout élément de preuve soumis à l'appréciation du tribunal doit d'abord satisfaire aux quatre principes fondamentaux des règles de preuve, soit la règle de la pertinence, l'authenticité et la fiabilité, la règle de la meilleure preuve et la prohibition du ouïe dire. Ensuite, dans le cas des documents en forme électronique, il peut arriver des situations où la présomption de fiabilité qui leur est attribuée soit remise en question. Dans de tels cas, il faut alors établir que les systèmes utilisés à leur confection sont fiables, stables et intègres.

Partie 3 Survol de quelques solutions technologiques

3. A. Acquisition, analyse et préservation de la preuve électronique

3.A.I. *EnCase* ®*Forensic* et *EnCase* ® *Forensic Edition Professional Suites* ⁶⁵

L'ensemble logiciel *EnCase* ® *Forensic* est sans aucun doute le chef de file dans son domaine. Il est utilisé par la plupart des services d'enquête policiers aux États-Unis. Cet ensemble se vend 2 495\$ USD par licence. Les utilitaires de l'édition professionnelle sont en supplément et se vendent 895\$ USD.

Cet ensemble logiciel offre tous les outils nécessaires pour mener à terme toute enquête portant sur des documents en forme électronique:

- Il permet de procéder à l'acquisition de la preuve de façon non invasive en créant des images de l'information tout en préservant son intégrité et en ne l'altérant d'aucune façon.
- Il permet de créer des images constituant des reproductions exactes, bit par bit, de l'information ce qui permet ensuite de travailler avec celles-ci tout en préservant l'original.
- Il permet d'analyser et de trier l'information par voie de recherche par mots clés, recherches complexes, filtres et scripts spécialisés. Il permet aussi toutes sortes d'analyses, dont celle des caractéristiques particulières des divers fichiers, la signature des fichiers, etc.
- Il contient des outils permettant d'émettre des rapports complets visant à présenter l'information et la preuve recueillie de façon efficace.
- Il contient des outils de gestion permettant de documenter et la chaîne d'acquisition et de préservation de la preuve.

3.A. II *New Technologies Inc. (Ni)* ⁶⁶

Cette entreprise offre l'ensemble *Computer Response Tool Suite* qui contient une suite d'utilitaires destinée aux agents chargés de l'application de la loi (« *Law Enforcement* »).

Cet ensemble comprend la plupart des utilitaires nécessaires pour procéder à des enquêtes électroniques complètes, quoique non intégrés dans un tout comme l'ensemble *EnCase* ® *Forensic*, par exemple.

⁶⁵ <http://www.encase.com/>

⁶⁶ <http://www.forensics-intl.com/intro.html>

Cet ensemble logiciel vise les départements spécialisés en enquête électronique des divers services policiers, les spécialistes en informatique et les experts en développement de logiciels. Le prix de cet ensemble logiciel n'est pas publié sur le site Web de l'entreprise.

Cette entreprise offre aussi des services conseil en support au litige pour les firmes d'avocats aux prises avec la nécessité d'acquérir, analyser et préserver de l'information électronique dans le cadre de leurs dossiers. Des services de formation sont aussi offerts.

3.B. Support au litige

3.B.I. *Summation*® *IBlaze*⁶⁷

Ce logiciel est sans contredit l'un des chefs de file dans son domaine. Il se vend 2 495\$ USD en version singulière, 6 895\$ USD pour 5 postes de travail en réseau et 11 495\$ USD pour 10 postes de travail en réseau. Des options additionnelles sont disponibles moyennant des frais supplémentaires. Il couvre toutes les facettes de la gestion des litiges :

- Gestion complète des documents, permettant la recherche textuelle et par image. Bases de données. Révision de documents (information confidentielle).
- Production électronique de documents.
- Gestion des procédures, gestion du calendrier, gestion du temps, comptabilité.
- Permet l'accès sécurisé et la collaboration avec plusieurs collègues et assistants.
- Gestion de la recherche doctrinale et jurisprudentielle.

3.B.II *Dataflight Software Inc.*⁶⁸

Cette firme offre une suite de logiciels voués à la gestion des litiges, *Concordance*® 8, *Opticon*™ 3.0 et *FYI Internet Server*™. Cette suite de logiciels fait aussi partie des chefs de file dans ce domaine. Le prix de ces logiciels n'est pas publié sur le site Web de l'entreprise. La combinaison de ces trois solutions constitue un outil de travail très puissant pour les firmes d'avocats aux prises avec d'énormes quantités d'information à gérer autant sur support papier et que sur support électronique.

⁶⁷ <http://www.summation.com/>

⁶⁸ <http://www.dataflight.com/>

3.B.III. CaseSoft⁶⁹

Il s'agit d'une autre firme qui offre une suite de logiciels destinés à supporter les litiges et enquêtes: CaseMap, TimeMap, TextMap, NoteMap, DepPrep. Le prix de ces logiciels n'est pas publié sur le site Web de l'entreprise.

Plusieurs autres solutions technologiques voués à ces fins existent au Canada, aux États-Unis et ailleurs. Le but de la présente partie n'est pas de présenter une liste exhaustive de celles-ci mais simplement d'en présenter quelques unes pour illustrer ce qui existe à l'heure actuelle dans ce domaine et inciter le lecteur à faire de plus amples recherches à ce titre. La façon la plus facile pour ce faire consiste à utiliser un moteur de recherche comme *Google* sur Internet et de faire une recherche avec des mots clés comme « *Litigation Support Software* », « *Litigation Support Services* », « *Computer Forensic Software* », *Computer Forensic Services* », etc.

3.C. Formation professionnelle

Pour ceux qui sont intéressés par les enquêtes de nature électronique sur ordinateur et qui désirent obtenir une certification à ce titre, le « *International Society of Forensic Computer Examiners* ®»⁷⁰ offre une certification reconnue mondialement et qui s'appelle le « *Certified Computer Examiner* ® ».

Tel que décrit sur le site Web de cette association, cette certification requiert les connaissances particulières suivantes:

"The initial CCE certification process will encompass:

- *Acquisition, marking, handing and storage of evidence procedures*
- *Chain of custody*
- *Essential "core" forensic computer examination procedures*
- *The "Rules of Evidence" as they relate to computer examinations*
- *Basic PC hardware construction and theory*
- *Very basic networking theory*
- *Basic data recovery techniques*
- *Authenticating MS Word documents and accessing and interpreting metadata*
- *Basic CDR recording processes and accessing data on CDR media*
- *Basic password recovery techniques*
- *Basic Internet issues*

Various operating system specific endorsements are/will be available. Endorsements include:

The Microsoft FAT (Windows 95/98) operating systems and forensic issues related to those operating systems.

⁶⁹ <http://www.casesoft.com/>

⁷⁰ <http://www.certified-computer-examiner.com/>

The Microsoft NTFS (Windows NT/2000/XP) operating systems and forensic issues related to those operating systems.

The Unix/Linux operating systems and forensic issues related to those operating systems.

The MAC/Apple operating systems and forensic issues related to those operating systems.

Those CCEs who obtain three or more operating system endorsements will become Master Certified Computer Examiners (MCCE) ».

Intense School ⁷¹offre un programme de formation menant à l'obtention de la certification « Certified Computer Examiner ® » (CCE).

⁷¹ <http://www.intenseschool.com/>

Bibliographie

Michael R. Arkfeld, *Electronic Discovery and Evidence*, 2003, Law Partner Publishing LLC, Phoenix, Arizona.

Michael R. Arkfeld, *The Digital Practice of Law, 5th Edition*, 2001, Law Partner Publishing LLC, Phoenix, Arizona.

Me Michel Gagné, *La preuve dans un contexte électronique*, Service de la formation permanente, Barreau du Québec, *Développements récents en Droit de l'Internet*, 2001, Les Éditions Yvon Blais Inc.

Léo Ducharme, *L'administration de la preuve*, 3^e édition, 2001, Wilson Lafleur Ltée.

Claude Marseille, *La règle de la pertinence en droit de la preuve civile québécois*, 2004, Les éditions Yvon Blais Inc.

George S. Takach, *Computer Law, 2nd Edition*, 2003, Irwin Law