Revue du notariat

PRATIQUE DU DROIT ET OUTILS ÉLECTRONIQUES : LES EMBÛCHES DE LA TECHNOLOGIE

Bertrand SALVAS

Volume 106, Number 3, December 2004

URI: https://id.erudit.org/iderudit/1045712ar
DOI: https://doi.org/10.7202/1045712ar

See table of contents

Publisher(s)

Éditions Yvon Blais

ISSN

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

Explore this journal

Cite this article

SALVAS, B. (2004). PRATIQUE DU DROIT ET OUTILS ÉLECTRONIQUES : LES EMBÛCHES DE LA TECHNOLOGIE. *Revue du notariat*, *106*(3), 513–556. https://doi.org/10.7202/1045712ar

THÈME 3

Droit civil et technologies de l'information

PRATIQUE DU DROIT ET OUTILS ÉLECTRONIQUES : LES EMBÛCHES DE LA TECHNOLOGIE

Bertrand SALVAS[1]

1. INTRODUCTION 517

2. QUESTIONS JURIDIQUES 518

2.1 Cadre juridique général : la *Loi concernant le cadre juridique des technologies de l'information* . . 518

2.2 Aspect déontologique 522

2.3 Protection des renseignements personnels 525

3 QUESTIONS DE SÉCURITÉ. 527

3.1 Protection des systèmes 528

3.1.1 Coupe-feu et anti-virus 528

3.1.2 Vétusté des systèmes, mise en réseau et stockage 531

1. Notaire. L'auteur souhaite remercier Me Katya Laprise, notaire, de la direction du développement de la profession, qui a contribué à la recherche ayant précédé la rédaction de ce texte.

3.2 Protection des données 533

3.2.1 Préservation des fichiers 533

3.2.1.1 Gestion des copies de sauvegarde 534

3.2.1.2 Maintien de la lisibilité 535

3.2.2 Accès aux fichiers 535

3.2.2.1 Gestion des usagers 535

3.2.2.2 Chiffrement 536

3.2.2.3 Entretien et disposition d'équipement 536

3.3 Le travail avec des documents électroniques 537

3.3.1 Dissémination d'informations cachées dans les fichiers 537

3.3.2 Archivage des dossiers informatiques et pérennité 539

3.4 Communiquer électroniquement 542

3.4.1 Protection de la confidentialité des communications 542

3.4.1.1 Un mot sur la messagerie directe . 544

4. RECOMMANDATIONS 545

4.1 Faire le bilan de sa situation technologique 545

4.2 Examiner son fonctionnement interne 546

4.2.1 Accès aux fichiers et gestion des permissions 547

4.2.2 Usage du courriel 548

4.2.3 Accès à Internet, clavardage, P2P, etc. . . . 549

4.3 Examiner ses relations avec les tiers. 550

4.3.1 Le mandat de services professionnels . . . 550

4.3.2. Situation d'assurance 550

5. CONCLUSION. 553

6. BIBLIOGRAPHIE 554

1. INTRODUCTION

[1] Au moment d'entamer la rédaction d'un texte sur la pratique du droit à l'heure technologique, nous ne pouvons nous empêcher d'avoir une pensée pour les praticiens qui, en plus de devoir rester au fait des changements législatifs et jurisprudentiels dans leurs champs de pratique de prédilection, ont à composer avec les bouleversements successifs de leurs habitudes de travail imposées par la cadence élevée de l'évolution technologique.

[2] Il semble loin le temps où les méthodes de travail des juristes pouvaient se transmettre d'une génération de notaires à l'autre. Il n'y a pas si longtemps on apprenait encore, et avec raison, aux étudiants du programme de droit notarial que tous les outils bureautiques étaient facultatifs et qu'il était toujours possible d'ouvrir leur propre cabinet et de pratiquer simplement avec une plume et une boîte de papier réglementaire.

[3] Il n'aura pourtant fallu qu'une quinzaine d'années pour faire sombrer cette affirmation dans la désuétude. Le notaire d'aujourd'hui, et son collègue avocat aussi en passant, doivent maintenant s'adapter à des registres électroniques, des modes de transmission sécurisés, des échanges de documents dématérialisés, des plates-formes technologiques et une foule de risques de sécurité dont ils ne soupçonnent souvent même pas l'ampleur. Pourtant leurs obligations, elles, n'ont pas changé.

[4] Les juristes font de plus en plus usage des technologies de l'information dans leur pratique. Autrefois relégués au rang de curiosité ou de gadget bizarre, les outils de l'univers électronique sont aujourd'hui entrés dans leur quotidien, modifiant de nombreuses pratiques établies.

[5] L'utilisation de ces outils comporte une part de risque, que les praticiens d'aujourd'hui doivent contrecarrer en développant de nouveaux réflexes. Nous tenterons ici de dresser un inventaire de ces questions pratiques, proches du quotidien des juristes de l'ère technologique.

[6] Le juriste est appelé dans son quotidien à recevoir et gérer de l'information. Il est ainsi souvent appelé à détenir des données confidentielles, qu'il s'agisse de renseignements personnels sur ses clients ou d'autres personnes, de secrets commerciaux ou d'autres données stratégiques dans le cadre d'une transaction ou d'un litige.

[7] Il a toujours été tenu à des obligations très strictes en matière de confidentialité, obligations qui ne s'amenuisent pas quant il a recours aux technologies de l'information dans leur traitement. Le simple fait d'utiliser les nouveaux médiums de communication entraînera en effet une série de nouveaux risques et responsabilités avec lesquels le juriste devra apprendre à composer.

[8] Nous aborderons ces situations sous trois chapitres. Tout d'abord en survolant les questions juridiques en jeu, puis en résumant les incontournables questions de sécurité. Nous terminerons en formulant quelques recommandations.

2. QUESTIONS JURIDIQUES

2.1 Cadre juridique général : la *Loi concernant le cadre juridique des technologies de l'information*

[9] Les principales règles québécoises en matière de gestion des documents électroniques se retrouvent dans la *Loi concernant le cadre juridique des technologies de l'information*[2] adoptée à l'automne 2000 et entrée en vigueur le 1er novembre 2001.

[10] Nous traiterons ici de façon très générale des principales dispositions de cette loi, vous référant aux textes d'autres présentateurs aux présents Entretiens qui abordent ce sujet de façon beaucoup plus précise[3].

---

2. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-11 disponible sur Internet à cette adresse : http://www.canlii.org/qc/legis/loi/c-1.1/20040323/tout.html. Une version annotée préparée par le Centre de recherche en droit public (CRDP) de l'Université de Montréal, comprenant un imposant glossaire, est en ligne sur le site de l'autoroute de l'information du Québec (http://www.autoroute.gouv.qc.ca/loi_en_ligne/index.html).
3. Nous faisons référence aux présentations des professeurs Fabien et Trudel.

[11] Cette loi est fondée sur la distinction juridique fondamentale qu'elle opère entre le document et son support.

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

[12] Aux termes de la *Loi concernant le cadre juridique des technologies de l'information*, le document s'affranchit donc du support sur lequel il est consigné.

[13] Autre élément intéressant pour nos fins, la loi impose des règles propres à assurer en tout temps l'accès aux documents. Ainsi, lorsque l'accès à un document doit être maintenu, il devra toujours rester intelligible. Cet élément revêt une certaine importance pour le juriste appelé à conserver des documents sous format électronique.

[14] Un moyen d'obtenir communication du document devra également être toujours rendu disponible. Telle communication pourra se faire soit au moyen d'une copie par impression sur support papier par exemple, ou autrement[4].

[15] Dans un autre ordre d'idées, la *Loi concernant le cadre juridique des technologies de l'information* fait en sorte de briser la règle non écrite voulant qu'un document partage le sort de l'objet

4. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-11, art. 23.

sur lequel il a été fixé lors de sa création. Le passage au numérique lui permettant en effet de lui survivre, de migrer vers un autre support, ou encore d'exister sous de multiples formes, la loi se doit de prévoir des règles qui s'adressent directement au document, ou à l'information qui le compose.

[16] C'est un peu pour cette raison que la Loi affranchit juridiquement le document de son support et introduit la notion de cycle de vie. Le cycle de vie se définissant comme étant la période de temps écoulée entre la création et la destruction d'un document, et pouvant englober une série d'opérations diverses comme un ou plusieurs transferts du document entre divers supports[5].

[17] Peu importe le support sur lequel il pourra se retrouver à un moment ou à un autre entre le jour de sa création et celui de sa destruction, le document conservera ainsi son existence propre à condition que les données qu'il renferme demeurent intègres. Les règles entourant de tels transferts d'information d'un support à un autre se retrouvent aux articles 17 et suivants de la Loi.

[18] Le but général de ces règles est d'assurer que le document demeure intelligible et accessible à la fin du processus et, surtout, qu'il conserve son intégrité :

> **6.** L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.
>
> L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction.
>
> Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie.

[19] Le critère d'intégrité sera satisfait lorsqu'il sera possible de vérifier que l'information contenue au document n'a pas été altérée et qu'elle s'est maintenue dans son intégralité. La documentation

5. Pour une définition de la notion de cycle de vie du document, se référer au site de la Loi en ligne, à l'adresse http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/cycle.html.

du processus de conversion ou de transfert de support est donc exigée afin de permettre d'établir au besoin que ces obligations ont été respectées. Cette documentation doit être conservée tout au cours du cycle de vie du document.

[20] La *Loi concernant le cadre juridique des technologies de l'information* permet également la destruction du document tel que créé sur son support d'origine, à moins que ce dernier ne comporte une valeur archivistique ou patrimoniale[6].

[21] Au niveau de la transmission du document, la *Loi concernant le cadre juridique des technologies de l'information* adapte en contexte technologique la bonne vieille théorie de l'expédition, l'assortissant pour ce faire de certaines présomptions.

[22] D'un côté, l'expédition sera présumée complète : « lorsque le geste qui marque le début de son parcours vers l'adresse active du destinataire est accompli par l'expéditeur » et ne peut plus être contremandé[7].

[23] La réception sera quant à elle complète au sens de la loi lorsque le document transmis deviendra accessible à l'adresse « que le destinataire indique à quelqu'un être l'emplacement où il accepte de recevoir de lui un document ou celle qu'il représente publiquement être un emplacement où il accepte de recevoir les documents qui lui sont destinés »[8].

[24] Au niveau de l'intelligibilité des communications, il faut garder à l'esprit que le document expédié par courriel sera présumé intelligible à moins que le destinataire n'avise l'expéditeur du contraire dès son ouverture. Notons aussi que l'article 31 traite bizarrement cependant de l'ouverture du « document », et non pas du message servant à le transmettre.

[25] La loi édicte également des règles entourant la gestion de renseignements confidentiels contenus dans les documents :

---

6. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-11, art. 20 *in fine*.
7. *Ibid.*, art. 31.
8. *Ibid.*, art. 31, al. 2.

> **25.** La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

[26] Ces règles s'ajoutent, faut-il le rappeler, à celles comprises dans la *Loi sur la protection des renseignements personnels dans le secteur privé*, à laquelle les professionnels du droit sont également astreints[9].

2.2 Aspect déontologique

[27] Les principaux enjeux juridiques de l'usage des technologies pour le praticien du droit sont d'ordre déontologique. Car en plus des enjeux pratiques universels qui le pousseront, à l'instar de tout utilisateur des outils informatiques, à gérer efficacement et de manière sécuritaire ses données et systèmes, le juriste pourra par surcroît voir son imprudence sanctionnée par son Ordre professionnel.

[28] Ces derniers ont en effet pris acte de la place prise par la technologie dans les cabinets. L'usage de l'informatique dans la tenue des dossiers est maintenant soumis, il ne faut pas s'en surprendre, à un certain encadrement.

[29] Du côté du *Code de déontologie des avocats*[10], nous devons nous tourner vers les dispositions générales qui trouvent toujours leur application ici. L'article 3.00.01 impose à l'avocat un devoir général de compétence, faisant en sorte que l'avocat doit être en mesure d'utiliser les outils courants de sa pratique et ne pourra se dégager de sa responsabilité en plaidant sa méconnaissance de leur fonctionnement[11].

[30] L'article 3.07.01 du *Code de déontologie des avocats* stipule quant à lui que l'avocat doit permettre au client d'avoir accès à son dossier et aux documents qu'il contient, et d'en obtenir copie.

---

9. Voir la section 2.3 ci-dessous qui traite des règles québécoises en matière de protection des renseignements personnels.
10. *Code de déontologie des avocats*, R.R.Q., c. B-1, r. 1.
11. M. TÉTRAULT, « Le praticien et les technologies de l'information : le silence est d'or », BARREAU DU QUÉBEC, Service de la formation permanente, *Développements récents en droit familial*, Cowansville, Éditions Yvon Blais, 2002, p. 67.

[31] Cet article devrait se lire en parallèle aux dispositions de la *Loi concernant le cadre juridique des technologies de l'information* imposant l'obligation de maintenir la lisibilité d'un document dont l'accès doit être maintenu[12]. Il va donc sans dire que le juriste devra faire en sorte que son système et ses archives électroniques survivent suffisamment longtemps pour lui permettre de s'acquitter de cette obligation.

[32] Du côté du notariat québécois, en plus des obligations générales de compétence et de discrétion du notaire, le *Règlement sur la tenue des dossiers et des études des notaires*[13] aborde spécifiquement à l'article 4 la question du dossier tenu sur support informatique :

> **4.** Le notaire qui utilise le support informatique pour le traitement et la conservation de tout ou partie des éléments, renseignements et documents relatifs à un dossier doit :
>
> 1º sauvegarder les données ainsi recueillies et en conserver une copie conformément à l'article 20 ;
>
> 2º utiliser une base de données distincte de toute autre pour la tenue des dossiers visés au présent règlement ;
>
> 3º protéger l'accès de ces données notamment par l'utilisation d'un mot de passe.

[33] Le *Code de déontologie des notaires*[14] ajoute quant à lui au notaire l'obligation de préserver la confidentialité de sa signature numérique ou de tout autre moyen d'agir en son nom. Les règles sont en ce cas-ci précises et impératives.

[34] En ce qui concerne le secret professionnel, nous sommes en présence d'un droit fondamental du client protégé par la *Charte des droits et libertés de la personne*[15].

> En droit civil québécois, le secret professionnel de l'avocat est une institution qui comporte deux composantes : d'abord une obligation de confidentialité qui impose à l'avocat un devoir de discrétion et créé

12. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-11, art. 19.
13. *Règlement sur la tenue des dossiers et des études des notaires*, R.Q. N-2, r. 15.3.
14. *Code de déontologie des notaires*, R.Q. N-2, r. 3.
15. L.R.Q., c. C-12, art. 9.

> un droit corrélatif à son silence en faveur de son client ; ensuite, à l'égard des tiers, une immunité de divulgation qui protège le contenu de l'information contre sa communication forcée, même dans les instances judiciaires, sous les réserves et les limites prévues par les règles et principes applicables.[16]

[35] Ce droit fondamental du client au respect de la confidentialité de son dossier reste le même, quel que soit le mode de communication ou les outils de travail choisis par son notaire ou son avocat, et l'application de toutes les règles de droit en la matière, qu'elles soient générales ou spécifiques à une profession donnée, ne fait aucun doute.

[36] Aucune limitation de responsabilité ne vient donc contrebalancer l'accroissement des risques d'intrusion ou d'erreur inhérente à l'usage des technologies de l'information. Aussi le juriste aura tout intérêt à faire preuve de prudence dans son usage de l'informatique.

[37] C'est ici que subsiste le plus grand risque d'erreur, les moyens de sécuriser les documents et les transmissions électroniques restant encore trop souvent méconnus. Les risques découlent en effet principalement d'erreurs de manipulation ou de négligence, celui découlant de possibles intrusions malveillantes ou piratage de données restant somme toute assez peu limité quand des précautions élémentaires sont mises en place.

[38] Il est donc clair que le praticien devra adopter les moyens nécessaires pour protéger les données qu'il détient qui pourraient être protégées par le secret professionnel, à moins d'obtenir une renonciation explicite du client qui dispose toujours du droit de relever le professionnel de son obligation[17].

[39] Il est aussi clair que le client devra fournir un tel consentement en toute connaissance de cause, après avoir été suffisamment informé des risques encourus et de la portée de la renonciation. La discussion et la signature du mandat de services professionnels s'avérant être le moment idéal pour ce faire[18].

---

16. *Société d'énergie Foster Wheeler Ltée* c. *Société intermunicipale de gestion et d'élimination des déchets (SIGED) Inc.*, 2004 CSC 18.
17. *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, art. 9, et *Code des professions*, L.R.Q., c. C-26, art. 60.4.
18. Voir la section 4.3.1 au chapitre des recommandations, traitant du mandat avec le client.

[40] Le but de ce texte n'est pas d'exposer en détails la question du secret professionnel, aussi nous n'entrerons pas trop dans les détails. Il faut cependant rappeler que le secret professionnel ne s'étend pas nécessairement à toute information échangée ou communiquée avec un juriste (avocat ou notaire).

[41] Dans notre contexte cependant, la prudence exigera d'étendre le plus largement possible la protection des fichiers et communications électroniques afin d'éviter le plus de problèmes issus de possibles défauts de confidentialité.

2.3 Protection des renseignements personnels

[42] Les renseignements personnels sur les clients conservés dans les dossiers du praticien sont certes protégés par le secret professionnel. Mais même s'il est déjà soumis au strict régime du secret professionnel, le juriste est-il également tenu au respect des lois régissant la collecte de renseignements personnels ?

[43] La réponse est affirmative, un cabinet professionnel constituant en effet une « entreprise » telle que cette notion est définie à l'article 1525, alinéa 3 C.c.Q.[19].

[44] Différentes lois encadrent la question de la protection des renseignements personnels en contexte québécois.

[45] Au Québec, la loi applicable au sujet qui nous intéresse est la *Loi sur la protection des renseignements personnels dans le secteur privé*[20]. La loi fédérale[21] ne s'applique en effet pas à l'égard de toute opération entreprise au sein d'une province disposant d'une législation déclarée « essentiellement similaire » à ses termes ce qui est le cas de la loi québécoise.

> Les avocats et notaires doivent donc tenir compte de la loi (sur la protection des renseignements personnels dans) le secteur privé. En quelque sorte, elle semble élargir la protection que le juriste doit

19. Voir Jacques DORAY, « Les dossiers des professionnels et les dossiers des ordres professionnels : un millefeuille de normes quasi inextricables », dans *Le respect de la vie privée dans l'entreprise*, Actes de conférence, Les Journées Maximilien Caron, 1995, Montréal, Thémis, p. 181 et s.
20. L.R.Q., c. P-39.1.
21. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

> accorder à certains renseignements qui ne seraient peut-être pas visés pas la notion traditionnelle de secret professionnel. Quoi qu'il en soit, la loi (sur la protection des renseignements personnels dans) le secteur privé astreint le juriste a des obligations spécifiques quant à la collecte, la conservation, l'utilisation et la communication des renseignements qu'elle vise, soit les « renseignements personnels ».[22]

[46] La notion de renseignement personnel se définit comme suit aux termes de la *Loi sur la protection des renseignements personnels dans le secteur privé* :

> Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.[23]

[47] Quelles obligations découlent donc de ces lois à l'égard de la gestion de tels renseignements ?

> Ces lois obligeront les cabinets juridiques à ne recueillir, utiliser et divulguer les renseignements personnels d'un particulier qu'avec son consentement, lequel peut être exprès ou implicite, selon la délicatesse des renseignements visés et des attentes raisonnables de cette personne. [...] Les lois obligeront en outre les cabinets juridiques à charger un de leurs cadres à veiller au respect de la loi au sein du cabinet et à instaurer des politiques et pratiques (et à former les employées et employés afin de s'y conformer) qui mettent en œuvre les exigences des lois.[24]

[48] Sans trop s'étendre sur le sujet, le juriste devrait donc désigner une personne de son cabinet comme responsable de la gestion des informations personnelles. Cette personne devrait réviser les pratiques du cabinet ainsi que les formulaires de mandats professionnels utilisés afin de s'assurer qu'ils comportent les consentements requis.

[49] Les obligations quant à la protection des dossiers et des informations qu'ils contiennent s'appliqueront donc aux fichiers électroniques détenus et conservés par le juriste, et y trouveront potentiellement leur application.

---

22. Jean LAMBERT et Robert CASSIUS de LINVAL, « Le secret professionnel à l'ère des communications », , (1996-97) 99 *R. du N.* 84, 95.
23. *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, art. 2.
24. Jeffrey KAUFMAN, « Vie privée et pratique privée : les dix étapes essentielles à suivre », Association du Barreau canadien, Revue National, Association du Barreau Canadien, janvier-février 2004.

[50] La loi leur imposera notamment à l'article 10 l'obligation de mettre en place et de maintenir des mesures de sécurité aptes à protéger le caractère confidentiel des renseignements recueillis et conservés.

[51] Ce sujet revêt une importance particulière en contexte électronique, les données nominatives sur les individus étant particulièrement recherchées par les fraudeurs en cette époque où le vol d'identité gagne en popularité dans les cercles criminels[25].

[52] De plus, il faut souligner que la Cour suprême du Canada a intégré la notion de protection de la confidentialité des renseignements transmis dans le cadre d'une relation avocat-client au concept d'apparence de justice[26].

[53] Bref, la gestion et la conservation sécuritaire des informations recueillies par un juriste dans le cadre de l'exercice de sa profession sont plus importantes que jamais pour le juriste en pratique privée que pour toute entreprise ou organisme appelé à constituer des dossiers sur les individus. Les obligations professionnelles et la relation de confiance qu'il entretient avec ses clients augmentant d'un cran le niveau de sécurité à maintenir et l'expectative de confidentialité à l'égard des dossiers constitués.

[54] Survolons maintenant les principales embûches à contourner pour satisfaire à ces attentes et à ces obligations.

3. QUESTIONS DE SÉCURITÉ

[55] Dans le bon vieux temps, protéger son travail et l'information contenue dans ses dossiers se limitait à bien verrouiller ses classeurs et son bureau, et bien entendu à faire preuve de discernement dans la gestion de son personnel.

[56] Si le discernement est toujours de mise, les précautions pratiques pour protéger une étude faisant usage d'outils informatiques sont différentes et exigent, dans certains cas, beaucoup plus d'attention.

---

25. Le vol d'identité verra un fraudeur utiliser les informations personnelles sur un individu pour obtenir illégalement du crédit, acquérir des biens ou réaliser d'autres opérations financières dont il laissera la responsabilité à la victime.
26. *Succession Macdonald* c. *Martin*, [1990] 3 R.C.S. 1235.

[57] Les menaces sont en effet multiples. Elles peuvent se classer en deux catégories, selon qu'elles s'adressent aux réseaux ou aux systèmes en général, ou plus particulièrement aux données qu'ils renferment.

[58] Il ne faut pas non plus perdre de vue que la relative complexité pour certains de l'univers électronique rend plus probable la transmission de documents ou de données par erreur ou inadvertance que par piratage ou malveillance.

[59] Il est facile d'être alarmiste et de croire qu'une armée de *hackers* est en permanence mobilisée pour attaquer notre ordinateur ou intercepter nos communications.

[60] Ce risque est bien entendu présent mais, toutes proportions gardées, reste relativement lointain par rapport à la possibilité quotidienne de commettre soi-même une mauvaise manipulation entraînant la perte ou la dissémination de données.

3.1 Protection des systèmes

3.1.1 Coupe-feu et anti-virus

[61] Le conseil semble vieux comme le monde, mais il faut encore y revenir. Tout ordinateur, surtout lorsqu'il est raccordé à Internet comme c'est maintenant le cas la plupart du temps, devrait être protégé par un logiciel anti-virus et un coupe-feu régulièrement mis à jour.

[62] L'anti-virus cherchera à détecter la présence de codes malicieux dans un ordinateur. Alimenté par une base de données construite et actualisée par l'entreprise qui le distribue, ce logiciel pourra comparer la structure des virus connus avec toute ligne de code présente dans un ordinateur ou tentant d'y pénétrer (par courriel par exemple).

[63] Le coupe-feu a quant à lui pour but de contrôler les interactions entre un ordinateur et le réseau Internet. Il pourra dans un sens autoriser, bloquer ou demander l'intervention de l'opérateur quant à toute tentative d'un logiciel d'accéder au Web, ou dans l'autre détecter les tentatives d'intrusions menées par des pirates informatiques ou leurs logiciels. Il pourra aussi permettre d'isoler totalement un ordinateur du réseau si un quelconque risque est perçu.

[64] Bien que les mises à jour de ce type de système soient moins fréquentes, elles sont néanmoins souvent cruciales à la sécurité de l'ordinateur car elles visent habituellement à corriger des faiblesses récemment découvertes dans les systèmes.

[65] L'importance de la mise à jour fréquente d'un logiciel anti-virus, quotidienne si possible, est la principale faiblesse de ces systèmes. En effet, les distributeurs de virus comptent sur les délais de mise à jour d'un certain pourcentage d'ordinateurs pour les infiltrer.

[66] Car même si les mises à jour sont généralement disponibles la journée même de l'apparition d'un nouveau virus, la plupart des usagers ne mettent pas leur anti-virus à jour régulièrement et restent donc vulnérables pendant des semaines, parfois des mois.

[67] Une étude[27] réalisée aux États-Unis par *America Online* et la *National Cyber Security Alliance* montrait en effet que le tiers des internautes interrogés mettaient leur système anti-virus à jour à chaque semaine, et un deuxième tiers à tous les mois. Quant aux autres, une moitié n'avait pas fait de mise à jour plus fréquente qu'aux six mois, sinon plus, et l'autre ne possédait carrément aucun anti-virus.

[68] Des logiciels anti-virus de nouvelle génération tentent de contourner ce problème en cherchant à détecter l'activité des virus, y reconnaissant des actions habituellement posées par ce type de bestiole, plutôt qu'à reconnaître le code exact qui les compose par comparaison à une base de données.

[69] Ils souhaitent ainsi intervenir contre les codes malicieux sans avoir à attendre que l'usager ne mette à jour la base de données de son anti-virus. L'usage de ces logiciels relativement nouveaux n'est cependant pas encore assez étendu pour pouvoir en mesurer l'efficacité.

[70] Mais le traditionnel duo dynamique anti-virus/coupe-feu devrait se transformer en trio, la menace des logiciels espions, ou *spywares*, devant aussi être prise très au sérieux.

---

27. AOL/NCSA Online Safety Study, Conducted by America Online and the National Cyber Security Alliance, October 2004, http://www.staysafeonline.info/news/safety_study_v04.pdf, dernière verification de la page faite le 11 novembre 2004.

[71] Ce type de nuisance n'est pas un virus qui cherche à détraquer votre système, ni une tentative de prise de contrôle à distance. Plus sournois, le *spyware* cherche au contraire à rester très discret, son but étant d'espionner les internautes et de relayer des informations sur l'usage des ordinateurs. Les informations recherchées pourront constituer en l'historique des navigations sur le web, la recherche de certains types d'information sur les disques durs, comme des numéros de carte de crédit ou des mots de passe.

[72] La plupart de ces nuisances sont installées à des fins de marketing à l'occasion de l'installation de certains logiciels gratuits[28]. Mentionnons aussi dans cette catégorie les parasites qui détourneront votre page d'accueil sur Internet, vos requêtes de recherche, etc. Tout internaute devrait aussi s'inquiéter des agissements des *Webugs* qui espionnent votre système à partir de codes logés dans certaines pages Web que vous visitez.

[73] La bonne nouvelle est que ces bestioles peuvent être faciles à retracer et détruites à l'aide de logiciels spécialisés. Heureusement, car le faire manuellement est à peu près impossible parce qu'ils sont généralement conçus pour se réinstaller *ad nauseam*.

[74] La question de la qualification juridique de l'activité des créateurs de *spywares* ou de *webugs* n'est pas le propos de ce texte. D'ailleurs, malheureusement, la plupart de ces logiciels sont lancés à partir d'autres juridictions, ajoutant la territorialité et l'extradition à la liste des problèmes qu'ils engendrent.

[75] Il faut cependant relever l'étude et l'adoption aux États-Unis de certaines lois visant à interdire ces procédés, notamment le *Spy Act*[29] adopté en octobre qui exige qu'un avertissement clair et évident soit présenté aux internautes avant qu'ils ne téléchargent un module en mesure de surveiller leur comportement sur Internet[30]. La loi interdit également les détournements informatiques et

28. Les logiciels d'échange de fichiers de type *peer-to-peer*, comme Kazaa, comporte un risque très élevé d'infection de ce type.
29. Http://thomas.loc.gov/cgi-bin/query/D?c108:4:./temp/~c108wjrcZY.
30. J.-C. CONDO, *Logiciels espions : des peines de prison prévues dans une seconde loi*, Branchez-vous, 7 octobre 2004, http://www.branchez-vous.com/actu/ 04-10/08-312904.html.

l'affichage de messages publicitaires qui ne peuvent être fermés. Espérons que ces lois viennent améliorer un peu la situation[31].

[76] Quant aux *webugs*[32], notons que les dernières versions d'Internet Explorer permettent de désactiver certaines images dites « actives » sur les sites Web que vous visitez, réduisant les risques d'infection.

[77] La morale du conte ? Le maintien et la mise à jour de systèmes de protection adéquats sont essentiels pour tout propriétaire ou gestionnaire de système informatique.

[78] Ceci est particulièrement vrai dans le cas de professionnels qui accumulent dans leurs systèmes des données confidentielles sur des clients, des transactions ou des procès, et dont la négligence pourrait être sanctionnée au niveau disciplinaire.

3.1.2 Vétusté des systèmes, mise en réseau et stockage

[79] Je me souviens de certains collègues qui, au milieu des années 90, utilisaient toujours des ordinateurs achetés au cours de la décennie précédente. De telles situations se doivent aussi de passer au nombre des souvenirs pittoresques, les problèmes de sécurité devant nous pousser désormais à un renouvellement plus fréquent du matériel informatique.

[80] La rapidité d'évolution de la technologie informatique est bien connue. Elle a même fait l'objet d'une théorie baptisée loi de Moore[33] du nom de son auteur qui prédisait en 1965[34] que le nombre de transistors utilisés dans les processeurs, ainsi que leur vitesse de traitement des informations, allaient doubler à tous les deux ans environ.

---

31. Pour plus de détails, se référer à l'article suivant sur Juriscom.net : L. THOUMYRE, *Spyware wanted dead or alive ! La FTC en guerre contre les logiciels espions*, 21/10/2004 http://www.juriscom.net/actu/visu.php?ID=583 dernière vérification de la page le 10 novembre 2004.
32. Judicieusement traduit « pixel invisible » par l'Office de la langue française du Québec, http://w3.oqlf.gouv.qc.ca/terminologie/fiches/8367061.htm.
33. Http ://www.intel.com/research/silicon/mooreslaw.htm
34. G.E. MOORE, *Cramming more components onto integrated circuits*, Electronics, vol. 38, nº 8, 19 avril 1965, disponible sur Internet, ftp://download.intel.com/research/silicon/moorespaper.pdf, dernière verification de la page le 1er novembre 2004.

[81] De plus, le perpétuel jeu du chat et de la souris mené entre fabricants et pirates informatiques fait en sorte que les systèmes d'exploitation et les logiciels de protection d'aujourd'hui sont souvent difficiles à opérer pour les appareils d'hier.

[82] Le remplacement d'ordinateurs en voie de dépassement ne peut donc être différé que pendant un certain temps, leur incapacité à suivre l'évolution des logiciels de base devant les rendre vulnérables très rapidement. Qui plus est, la mise à niveau des systèmes et des logiciels s'imposera d'elle-même simplement pour préserver la lisibilité des fichiers, ce qui pourrait très bien d'ailleurs constituer une obligation[35].

[83] L'importance de ces précautions se trouve décuplée lorsque envisagée dans un contexte de mise en réseau des informations, la préservation de la confidentialité des dossiers devenant cruciale lorsque plusieurs usagers ont potentiellement la possibilité d'y avoir accès.

[84] La mise en place de normes de contrôle des usagers et d'accès à certains répertoires ou ordinateurs est capitale au maintien d'un niveau de sécurité adéquat. L'établissement d'une politique d'accès aux données, intégrées à une politique générale d'usage des ordinateurs, du courriel et de l'Internet sur les lieux de travail, permettra également d'éviter des conflits potentiels avec les employés.

[85] Une telle politique pourra impliquer l'établissement de normes d'utilisation des adresses de courriel utilisées sur le serveur du cabinet, l'interdiction d'installer des logiciels sur les postes de travail (pour éviter l'introduction de codes malicieux ou la création de conflits logiciels potentiellement désastreux) ou encore l'imposition de balises ou l'interdiction pure et simple de l'utilisation de services de clavardage au bureau.

[86] L'usage d'un réseau sans fil emporte aussi son lot de contraintes de sécurité, les caractéristiques de sécurité des équipements et logiciels installés pour ce faire devant faire l'objet d'une attention particulière pour éviter que les données ne deviennent disponibles à toute personne utilisant un système sans fil à proximité de ses bureaux.

---

35. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-11, art. 19.

[87] L'arrivée de nouveaux médiums de stockage des données emporte aussi certains risques. Par exemple les clips USB, ces petits réceptacles de mémoire vive souvent appelés aussi « lecteurs amovibles », peuvent contenir jusqu'à 1 Gigaoctet de données et sont très utiles au juriste moderne, mobile et branché qui grâce à eux aura toujours sur lui une copie récente de ses dossiers.

[88] Malgré leur utilité, les clips USB constituent aussi un risque de sécurité car quiconque aura accès pendant quelques minutes à un ordinateur pourra potentiellement y copier des quantités phénoménales de données et les emporter avec lui, ni vu ni connu. Inversement, la perte d'un clip USB farci de données confidentielles pourrait aussi constituer une catastrophe pour son propriétaire.

[89] La protection par chiffrement des fichiers contenus sur un clip USB devrait donc faire partie des précautions de base pour ses utilisateurs. Quant à la protection des réseaux contre les copies non autorisées de fichiers, le cas pourrait bien être résolu par la prochaine version de Windows qui permettrait semble-t-il de bloquer l'accès aux clips, au gré du responsable du réseau.

3.2 Protection des données

3.2.1 Préservation des fichiers

[90] Si la responsabilité pouvant découler du défaut de protéger adéquatement son système informatique semble être un peu indirecte, la négligence dans la gestion d'un fichier donné ou d'un ensemble de fichiers pourrait être invoquée avec beaucoup plus de précision.

[91] La grande mobilité des informations, résultat de la révolution technologique, impose maintenant la plus grande vigilance dans la mise en place de mesures de protection adéquates.

[92] Les notions de base entourant la protection des données sont certes mieux connues qu'elles ne l'étaient, aussi nous ne nous y attarderons pas indûment. Contentons-nous donc de les résumer à grands traits.

3.2.1.1 Gestion des copies de sauvegarde

[93] Tout d'abord, la génération régulière de copies de sauvegarde constitue la première ligne de défense à mettre en place pour s'assurer que ses fichiers survivent à un bris d'équipement ou de logiciel.

[94] La création, lorsque possible, de disques de récupération à partir du système d'opération, de son anti-virus ou autres logiciels de sécurité doit également être réalisée régulièrement. Ces disques devraient être conservés précieusement car ils pourront permettre une restauration efficace et rapide de son système après la survenance d'un problème majeur.

[95] Le défaut de générer des copies de sauvegarde relève généralement de la négligence. Ce type d'intervention étant souvent, et malheureusement, remis à plus tard faute de temps.

[96] Un des moyens d'éviter ce problème est de faire l'acquisition de systèmes automatisés qui généreront automatiquement des copies de sauvegarde sur ruban magnétique ou autre support.

[97] L'autre est de prendre des habitudes rigides en la matière en désignant un responsable de cette tâche et/ou en l'intégrant à période fixe dans son agenda par exemple. Peu importe la manière choisie pour s'en souvenir, l'important est de le faire !

[98] La prudence exige aussi de conserver des copies de sauvegarde dans un autre endroit que son bureau. Et comme ces copies contiennent des données confidentielles, leur conservation devrait être entourée des mêmes mesures de sécurité que l'ordinateur principal où elles résident, et devraient donc être mises sous clé.

[99] Le recours, dans certains cas, à un serveur miroir externe pour entreposer une copie de sauvegarde pourrait également être considéré. Solution possiblement plus coûteuse offerte par certains fournisseurs de services d'hébergement, elle permet cependant de disposer en tout temps d'un double de ses données et de pouvoir y recourir en cas de problème. Ici aussi, l'accès aux données devrait être strictement contrôlé.

3.2.1.2 Maintien de la lisibilité

[100] S'assurer que ses fichiers restent intelligibles à travers les évolutions des systèmes et des logiciels est primordial pour éviter de se retrouver dans l'impossiblité d'y avoir accès.

[101] La question de la conservation des données informatiques, particulièrement des documents signés au moyen de signatures numériques faisant usage des technologies de cryptographie asymétrique, reste non résolue. L'importance de s'assurer que ses fichiers traversent les différentes évolutions technologiques ne peut donc pas être minimisée[36].

3.2.2 Accès aux fichiers

3.2.2.1 Gestion des usagers

[102] La réseautique est aussi entrée dans les mœurs. Même au niveau résidentiel où un ménage canadien sur cinq dispose aujourd'hui d'un réseau informatique local[37], la puissance et la flexibilité permise par la mise en réseau de plusieurs ordinateurs devient un outil incontournable.

[103] La mise en réseau implique donc la théorique mise en disponibilité à plusieurs personnes des données logées sur chaque ordinateur qui y est branché. Laisser libre accès à tous les ordinateurs pour tous les membres de l'étude est cependant un jeu dangereux.

[104] Certains dossiers devront être exclus de cet accès général. Certains usagers ou catégories d'usagers devraient également être admis ou exclus de certains dossiers ou appareils, ou encore devraient disposer de droits différents quant à leur contenu (lecture seule, possibilité de modifier ou pas, etc.).

[105] La gestion des usagers est une composante de sécurité fondamentale dès que le cabinet dispose de son propre réseau. Ici

---

36. Voir la section 3.3.2, « Archivage des dossiers informatiques et pérennité », ci-dessous.
37. RBC Groupe Financier/Ipsos-Reid, *Les familles canadiennes et Internet*, Étude et sondage du 23 janvier 2002, http://www.rbc.com/nouvelles/pdf/20020123canfam_full_report-f.pdf (site visité le 29 octobre 2004).

aussi, cette responsabilité doit échoir à une seule personne qui aura notamment le pouvoir de déterminer les permissions d'accès accordées à chacun.

[106] La politique à appliquer en ce domaine devrait également être clairement identifiée et rendue disponible à toutes les personnes impliquées.

3.2.2.2 Chiffrement

[107] L'utilisation de certains logiciels permettant de bloquer l'accès à des fichiers ou à des répertoires entiers constitue une précaution simple et facile d'accès qui peut s'ajouter à d'autres mesures de contrôle.

[108] Mais la préservation du caractère confidentiel de certains fichiers devrait justifier à elle seule l'implantation d'outils de chiffrement.

[109] Surtout connus pour leur aptitude à chiffrer les communications électroniques, les logiciels de chiffrement[38] peuvent également servir à chiffrer un ou plusieurs fichiers. D'autres logiciels permettent de systématiquement chiffrer tout fichier placé dans un ou plusieurs dossiers donnés.

[110] Ces technologies sont au point et disponibles à peu de coût.

3.2.2.3 Entretien et disposition d'équipement

[111] Le rythme effréné de renouvellement du parc informatique et les habitudes de consommation de nos sociétés modernes réduisent la durée de vie utile des ordinateurs à quelques années à peine.

[112] Dépense fiscale amortie sur trois ans, l'ordinateur sera souvent remplacé peu de temps après cette échéance. Mesure de sécurité souvent négligée, jeter un ordinateur, des disques ou autres médiums de stockage est un geste à première vue anodin, mais souvent porteur de conséquences.

38. Le plus connu étant PGP (http://www.pgp.com/).

[113] Les pirates informatiques le savent bien puisqu'ils visitent souvent les conteneurs à déchets des centres-villes à la recherche de matériel informatique usagé afin d'y trouver des informations confidentielles comme des données nominatives, fort prisées en cette ère du vol d'identité, ou encore des mots de passe permettant d'accéder à différents sites, réseaux ou services sécurisés sur Internet.

[114] Mis à part ce scénario plausible mais quelque peu hollywoodien, il ne faut pas non plus négliger le risque d'indiscrétion découlant du don ou de la revente d'un système informatique qui n'aurait pas été préalablement purgé de ses données.

[115] Le formatage d'un disque dur n'étant pas toujours suffisant pour tout effacer, l'utilisation de logiciels d'effacement de la surface des disques ou le recours à un expert serait donc à conseiller en pareil cas.

[116] Il faut ici rappeler les devoirs des professionnels du droit en matière de secret professionnel, et la possible responsabilité en cas de dissémination ou réutilisation frauduleuse de données nominatives.

[117] De la même façon, jeter un vieux disque de récupération, ou tout autre médium de stockage comme CD ou disquettes sans les détruire physiquement au préalable est désormais impensable.

3.3 Le travail avec des documents électroniques

3.3.1 Dissémination d'informations cachées dans les fichiers

[118] En plus d'offrir des outils de plus en plus puissants pour les préparer, l'informatique permet aussi de créer des documents aux facultés inédites.

[119] Intégrer images, sons ou vidéo à un texte, combiner tableurs, graphiques et bases de données, travailler en collaboration avec des collègues installés à l'autre bout du monde, l'informatique repousse les limites de la créativité un peu plus à chaque jour.

[120] Le résultat de ces efforts, qu'il s'agisse d'un texte, d'une présentation graphique ou d'une feuille de calcul, est donc souvent porteur d'une quantité parfois étonnante de méta données[39].

[121] Si plusieurs de ces méta données sont inoffensives, comme celles fournissant des statistiques sur le document ou certaines de ses caractéristiques de formatage, d'autres peuvent s'avérer être beaucoup plus éloquentes et indiscrètes.

[122] Par exemple le nom et les initiales du créateur du document (l'utilisateur du logiciel) ou de ceux qui l'auront révisé, le sommaire et la description du document, le nom du modèle utilisé pour le préparer, les dates de création, de modification et de consultation du fichier, le texte des versions antérieures, des fragments de texte supprimé ou ajouté, des marques et annotations de révision, l'historique annuler/refaire, certains commentaires apportés en cours de révision, etc. sont autant d'informations qui peuvent se retrouver en méta données.

[123] Peu d'utilisateurs des outils informatiques soupçonnent la présence de tels types d'information en arrière-plan des fichiers, et ne portent donc aucune attention lors de la transmission de projets ou de documents sous format électronique. De nombreuses informations pourraient ainsi être indûment transmises.

> Par exemple, un avocat a pour mandat de rédiger un contrat pour un client. Un confrère qui a récemment complété un mandat analogue lui propose alors de prendre comme modèle le contrat qu'il a alors rédigé pour un autre client. Il lui en transmet une version électronique afin d'accélérer le travail de préparation du document. Notre avocat ouvre le document et l'adapte aux besoins particuliers de son client en modifiant plusieurs clauses. Il rédige ainsi un nouveau contrat, qu'il transmet à son client par courriel pour approbation. Ce client le révise, y effectue quelques modifications et y ajoute des commentaires de nature stratégique afin d'orienter l'avocat dans la préparation de la version finale. Il y ajoute aussi un tableau en le copiant à partir d'une feuille de calcul ouverte dans un tableur. Après

39. Nous ne traitons ici que sommairement de cette question, mais nous vous référons au texte suivant : F. PELLETIER et D. POULIN, *La préparation des documents pour distribution électronique*, Comité canadien de la référence, septembre 2002, http://www.lexum.umontreal.ca/ccc-ccr/guide/docs/distribution_fr.html#_ftn1 dernière vérification de la page Web faite le 2 novembre 2004.

> quelques échanges du document entre l'avocat et son client, sa version finale est envoyée par courriel à l'avocat de la partie co-contractante.[40]

[124] Les techniques sécuritaires de minimisation ou d'élimination des méta données ou encore d'insertion d'objets dans les documents produits en cours de pratique devraient donc être mises en place afin d'éviter de ne pas en donner plus que le client n'en demande.

3.3.2 Archivage des dossiers informatiques et pérennité

[125] Nous avons traité un peu plus tôt de l'obligation factuelle de maintenir son système à niveau. Ceci est particulièrement vrai dans le cas de l'archivage de documents informatiques.

[126] La conservation à long terme des octets composant un fichier ne pose guère problème. Les appareils et médiums de stockage sont facilement accessibles et permettent la conservation sécuritaire des données. L'adoption de bonnes pratiques de gestion des copies de sauvegarde permet d'assurer la disponibilité presque éternelle des fichiers en tant que tels.

[127] Le problème de la pérennité des données se situe plutôt au niveau de la lisibilité des fichiers sauvegardés, la question étant en effet de s'assurer que les logiciels de demain puissent toujours décoder et comprendre les fichiers d'hier.

[128] Le choix du format de sauvegarde est donc important, tout comme les précautions à prendre lorsque s'effectue un changement de technologie.

[129] Une telle affirmation semble surprenante à première vue, mais n'oublions pas que les plus récentes versions de Microsoft Word n'arrivent pas toujours à ouvrir efficacement les fichiers créés avec certaines versions plus anciennes de ce même logiciel ou d'autres provenant de versions plus anciennes de logiciels couramment utilisés comme *Word Perfect 4.0* par exemple.

---

40. F. PELLETIER et D. POULIN, *La préparation des documents pour distribution électronique*, *ibid*, par. 10.

[130] On pourrait en tel contexte penser que la sauvegarde parallèle de certains documents importants dans un autre format plus universel que celui du logiciel d'origine pourrait leur apporter un peu plus de stabilité.

[131] Le choix d'un format universel de sauvegarde pour ses documents, comme le format RTF[41] par exemple, plutôt que le format maison du logiciel utilisé peut offrir de meilleures chances de maintenir ou d'élargir l'accessibilité au document puisque ce format est supporté par un grand nombre de logiciels de traitement de texte et même différentes plates-formes.

[132] Il faut cependant être conscient que certaines fonctions particulières du logiciel peuvent être perdues si on opte pour un format de sauvegarde autre que le format propre à ce logiciel. Mais généralement, pour des fichiers ne faisant usage que des fonctions de base, l'usage du RTF ne limite pas vraiment l'utilisateur tout en le sécurisant un peu mieux sur la survie de ses documents[42].

[133] Conserver les disques d'installation des anciennes versions des logiciels de traitement de texte, applications de productivité et systèmes d'opération utilisés au fil des ans est également une bonne précaution à prendre. En certains cas extrêmes, il pourrait s'agir de la seule façon d'accéder à des documents plus anciens.

[134] D'ailleurs, lors d'une mise à niveau d'un logiciel, l'usager prudent prendra la peine de vérifier dans la documentation si tous les types de fichiers qu'il utilise, ou qu'il a utilisé par le passé, sont toujours pris en charge dans la nouvelle version.

[135] Quelques essais viendront confirmer s'il y a effectivement un problème ou pas, et si des mesures de conversion immédiates sont nécessaires pour maintenir la lisibilité de tous les fichiers archivés. En pareil cas, la conversion des fichiers plus âgés au nouveau format sera de mise pour s'assurer de toujours pouvoir leur accéder.

---

41. Rich Text Format.
42. L'auteur tient à souligner qu'il n'a personnellement utilisé que le format RTF avec Microsoft Word pendant de nombreuses années, sans limiter son usage du logiciel ni modifier ses habitudes.

[136] Il faut souligner finalement les problèmes majeurs que de telles opérations peuvent causer dans le cas de documents signés électroniquement, car ce type de signature perdra en effet toute validité lors de la migration des données.

[137] L'application d'une signature numérique à un fichier se fait au moyen de procédés de cryptographie. La cryptographie consiste, on le sait, à brouiller le code numérique d'un fichier au moyen d'une formule mathématique complexe. Le fichier en résultant ne peut donc être décodé que par un système disposant de la clé inverse correspondant à celle utilisée pour le brouiller.

[138] Dans un système de signature numérique l'apposition d'une clé dite « privée » permettra donc d'assurer que le consentement a été apposé par le titulaire de ladite clé. Comme elle est théoriquement la seule personne qui puisse l'utiliser, le décodage du fichier au moyen de la clé correspondante publique viendra confirmer irrémédiablement l'identité du titulaire de la clé de chiffrement[43].

[139] Tout ce processus de chiffrement repose ainsi sur des manipulations mathématiques opérées sur le code numérique du fichier, ou document, visé. Il est donc clair que la modification d'un seul octet d'un document signé électroniquement aux fins de le faire migrer d'un format à un autre, viendra du coup invalider les signatures qui lui ont été apposées. L'empreinte numérique du fichier étant perdue, la validité des signatures sera irrémédiablement compromise.

[140] La solution définitive de cette énigme technique n'a pas encore été trouvée. La seule piste de solution avancée jusqu'à ce jour implique la resignature des documents au moment de leur migration. Aussi importe-t-il d'agir prudemment avant de procéder à la migration de fichiers assortis de signatures numériques fondées sur des procédés cryptographiques[44]. La conservation jalouse des logiciels servant à les utiliser dans leur forme originale prenant une importance capitale jusqu'à nouvel ordre.

---

43. Sans pouvoir confirmer cependant que c'est cette personne qui a effectivement apposé la signature numérique.
44. Le lecteur intéressé par cette question trouvera plus de détails dans le texte de Me Eric Dunberry, « L'archivage des documents électroniques », contenu dans l'ouvrage *Droit du commerce électronique*, collectif, sous la direction de Vincent GAUTRAIS, Montréal, Éditions Thémis, 2002, p. 87.

3.4 Communiquer électroniquement

[141] L'usage du courrier électronique fait maintenant partie du quotidien de millions de gens. Il est par conséquent facile de baisser la garde, de se laisser prendre au jeu, et de tomber dans un des pièges que présente son utilisation.

[142] Les juristes ne font pas exception, loin de là. Par exemple, une étude réalisée en 2002 pour l'American Bar Association nous apprend que 97 % des avocats américains sondés utilisent le courrier électronique dans leur travail quotidien. Autre donnée intéressante, 92 % des avocats américains échangent des pièces jointes par courrier électronique, 63 % discutent par ce moyen de l'évolution de leurs causes et 64 % s'en servent pour échanger des procédures et autres documents reliés au dossier. Le courriel est par ailleurs choisi comme mode d'échange de consentements dans la conclusion de contrats par 20 % des avocats interrogés[45].

[143] Sans vouloir, ni pouvoir se priver des avantages de la communication électronique, certains conseils de prudence doivent être gardés à l'esprit.

3.4.1 Protection de la confidentialité des communications

[144] Tout d'abord il faut rester conscient que toute communication électronique peut tomber entre de mauvaises mains. Qu'il s'agisse des risques d'interception par des logiciels espions programmés pour détecter certains types de renseignements (des numéros de cartes de crédit par exemple), ou de problèmes de discrétion liés à l'accès de collègues ou de tiers à un certain poste de travail, les dangers sont variés.

[145] La prudence nous dictera donc un peu de retenue dans la rédaction de nos courriels. Vérifier si tout ce qui se trouve dans un message mérite d'être largement diffusé nous emmènera souvent à modérer nos transports dans nos envolées épistolaires. Les paroles s'envolent et les écrits restent, c'est bien connu. Et en matière de communication électronique ils ont par-dessus le marché la vie plutôt dure et une grande liberté de mouvement.

---

45. American Bar Association, Legal technology resource center survey report, 2002, http://www.lawtechnology.org/surveys/2002survey/2002survey_exec.pdf site visité le 1er novembre 2004.

[146] Pensez par exemple à la facilité avec laquelle un message peut être transmis à d'autres personnes. Nombre d'internautes ont pris l'habitude de communiquer en utilisant la fonction de réponse à un message, en incluant parfois sans vraiment trop y penser tous les destinataires de l'envoi d'origine, en en ajoutant parfois d'autres, et en laissant dans le message tout le fil de la conversation qui a précédé.

[147] Imaginez par exemple que vous écrivez à une partie à une transaction pour lui fixer un rendez-vous pour la séance de fermeture. Vous ajoutez innocemment de ne pas oublier que l'autre partie n'est pas au courant de l'existence d'une offre sur une autre propriété de votre client. La présence de cette remarque inutile au but véritable du message pourrait devenir explosive si le courriel se met à circuler, aux fins de confirmer le rendez-vous, entre toutes les personnes qui doivent être présentes [...] Vous pourrez ajouter au message les mises en garde que vous voudrez sur le caractère confidentiel de la communication, le mal sera fait.

[148] De telles mises en garde ne permettent en effet que d'éviter que des informations protégées par le secret professionnel, une fois interceptées ou reçues par un tiers, ne soient réutilisées en preuve dans le cadre d'une procédure judiciaire.

> Sans nier l'importance de [...] la protection (conférée) aux informations confidentielles dans certains contextes (par la présence d'un avertissement de confidentialité), force est de conclure que son utilité est limitée : dans les faits, la notice n'empêchera pas le pirate de prendre connaissance de l'information confidentielle. De plus, le tort sera le plus souvent causé non pas à l'occasion d'une éventuelle utilisation de l'information devant les tribunaux, mais par l'usage non judiciaire qu'en feront des personnes qui en tireront quelque avantage. [...] Enfin, cet article ne sera pas d'une grande utilité lorsque nous serons en présence d'une communication transfrontalière.[46]

[149] Bref, la mise en garde n'enlève rien et n'apporte pas grand-chose. Il peut être utile de l'insérer pour éviter au moins le risque d'une réutilisation judiciaire d'informations confidentielles tombées en de mauvaises mains, mais il ne faut pas y voir une panacée.

---

46. Jean LAMBERT et Robert CASSIUS de LINVAL, « Le secret professionnel à l'ère des communications », (1996-97) 99 *R. du N.* 84, 124.

[150] À ce titre, il faut réaliser qu'une fois qu'un message est envoyé rien ne peut nous le ramener[47]. Aussi le recours au chiffrement pour protéger la confidentialité de communications importantes devrait être envisagé, ou systématisé si possible.

[151] Un courriel n'est pas nécessairement non plus très fiable, car il est relativement facile de faire croire à notre correspondant que le message provient d'une autre personne que soi.

[152] Plusieurs logiciels de courrier électronique permettent étonnamment d'inscrire ce que l'on veut dans le champ « expéditeur », comme l'adresse électronique d'une tierce personne. L'usager averti, en cas de doute, ira vérifier dans le code interne du message pour retrouver le compte courriel effectivement utilisé pour la transmission. Nous trouvons ici aussi une justification à l'adoption d'outils sécurisés de communication électronique.

[153] Mais la prise de telles précautions n'est pas monnaie courante, ni à la portée de l'usager moyen. Il faudrait peut-être néanmoins garder à l'esprit cette curiosité du protocole du courrier électronique lors de la réception de messages qui semblent étonnants de la part de certains expéditeurs.

[154] Malgré le fait que le courriel soit maintenant utilisé de façon courante à tous les niveaux de la société, il faut malgré tout rester prudent et vigilant dans son usage de ce médium, surtout dans un contexte professionnel, et être conscient des risques inhérents à ce mode de communication.

3.4.1.1 Un mot sur la messagerie directe

[155] La messagerie directe, ou *tchat* est très en vogue sur le Web. Lancée par la compagnie ICQ au milieu des années 80 puis repris par le système MSN Messenger de Microsoft, ce mode de communication en temps réel compte des dizaines de millions d'adeptes sur la planète.

[156] Utilisée principalement à des fins récréatives, la messagerie directe compte aussi de nombreux adeptes qui l'utilisent pour collaborer dans un contexte commercial ou professionnel.

---

47. Un correspondant a un jour demandé à l'auteur de lui retourner un courriel envoyé par erreur… Malheureusement, pas plus que l'envoi d'un fax à un mauvais numéro, rien ne peut permettre de renverser la vapeur.

[157] L'usage de tels systèmes n'est pourtant pas sans risques. Certains ouvrent la porte aux intrusions, permettent la transmission de fichiers infectés de virus ou même, dans les pires cas, facilitent la prise de contrôle à distance des ordinateurs à l'insu de leur propriétaire.

[158] Ces risques de sécurité, ajoutés aux problèmes de productivité du personnel pouvant découler de leur usage, poussent de nombreuses entreprises à interdire l'utilisation du *tchat* au travail ou à limiter les fonctionnalités de ces systèmes pour empêcher l'échange de fichiers avec des correspondants externes au réseau.

[159] On se rappelle notamment de l'affaire *CAE Électronique* où un tribunal d'arbitrage rejetait le grief d'un employé congédié pour abus de l'usage d'Internet sur le lieu de travail[48].

[160] Les règles entourant l'usage de la messagerie directe ou l'interdiction formelle d'en faire usage, devrait être clairement établies et affichées autant pour éviter que des problèmes ne surgissent, que pour montrer patte blanche en matière de protection de la vie privée des employés[49].

4. RECOMMANDATIONS

[161] Alors que faire pour se protéger ? Installer un anti-virus, faire des copies de sécurité, surveiller ses employés mais pas trop… Chacun y va de son propre conseil.

[162] Pour résumer un peu les différentes propositions essaimées dans le présent texte, nous pourrions classer les principales recommandations sous trois catégories.

4.1 Faire le bilan de sa situation technologique

[163] L'atteinte de tout résultat efficace passe par l'établissement d'un bilan technologique de son cabinet. Dresser l'inventaire

48. M.A. AMIOT, *Un arbitre confirme le renvoi d'un employé ayant abusé d'Internet*, La Presse, 2 février 2000, p. A1.
49. Pour plus de détails sur la question de la protection de la vie privée des employés en milieu de travail, nous vous conseillons le texte de Mme Juliette Lenfant, *Le droit à la vie privée s'étend-il à l'utilisation du courriel par un employé dans le cadre de ses fonctions ?*, mai 2000, publié sur Juriscom à l'adresse suivante http://www.juriscom.net/uni/etd/04/priv01.pdf.

de ses appareils et de leur interconnexion, des logiciels de sécurité (anti-virus, coupe-feu, anti-*spyware*) et de leur actualisation (situation et fréquence), de ses pratiques en matière de génération de copies de sauvegarde, de communication, d'accès et d'utilisation des données, constitue donc la première phase de toute intervention.

[164] Il faut ici bien entendu tenir compte de l'utilisation au cabinet de toute plate-forme technologique, car elle pourrait elle-même intégrer des mesures de protection et régler plusieurs problèmes potentiels, notamment au niveau de la communication électronique.

[165] Notez à cet égard qu'il ne faut pas hésiter à faire appel à des ressources externes et d'obtenir des conseils. Par exemple Notarius, la filiale technologique de la Chambre des notaires du Québec, offre aux notaires un service d'audit technologique qui cadrerait très bien dans la poursuite des objectifs présentés ici. D'autres firmes ou consultants en informatique pourraient être mis à contribution à de telles fins.

[166] De ce bilan de santé informatique découle deux autres séries de recommandations, visant respectivement le fonctionnement interne du cabinet et la gestion de ses relations avec les tiers.

4.2 Examiner son fonctionnement interne

[167] Tout d'abord, il importe de désigner un responsable informatique. Selon la taille du cabinet, il pourra évidemment s'agir d'un professionnel de l'informatique qui s'occupera de la gestion du réseau, de la mise à jour des différents systèmes, de régler les problèmes qui surgiront, etc.

[168] Mais toutes les études ne peuvent se permettre un tel luxe. La désignation d'un responsable parmi le personnel régulier, plutôt que de laisser le soin à chacun de s'occuper de son poste ou les associés peut malgré tout s'avérer un choix intéressant au niveau de la coordination des interventions. Les chances d'oublier une tâche ou de croire, de bonne foi, qu'elle a été accomplie par une autre personne, s'en trouveront minimisées.

[169] Un tel responsable, en plus d'accomplir certaines tâches techniques à sa portée, pourra s'assurer que chacun met à jour régulièrement ses logiciels de sécurité ou ses applications importantes, coordonner la génération des copies de sécurité à intervalles réguliers et leur lieu de conservation (rotation des copies entre les lieux internes et externes de conservation, etc.), faire le suivi sur l'entretien de l'équipement, voir au respect des politiques technologiques internes, s'assurer de retirer les permissions d'accès à tout employé quittant la firme, etc.

[170] L'établissement de politiques internes claires quant à l'usage des outils informatiques peut ensuite s'avérer extrêmement utile, voire crucial, pour augmenter le niveau de sécurité en vigueur et contribuer à maintenir une saine atmosphère de travail.

[171] Ces politiques devraient bien entendu être affichées ou distribuées au personnel, et surtout réellement mises en pratique afin d'assurer tant leur application que leur opposabilité. Ne pas appliquer de telles règles de conduite équivaut presque en effet à admettre qu'elles n'ont aucun effet.

[172] Quant à leur contenu, ces règles devraient notamment aborder les sujets suivants.

4.2.1 Accès aux fichiers et gestion des permissions

[173] Toute bonne gestion d'un réseau informatique implique la catégorisation des usagers selon leur position dans l'entreprise et/ou leur ancienneté. Nous l'avons vu, les risques d'accès non-autorisés à certaines données confidentielles, de modifications ou destructions accidentelles des fichiers ou encore leur détournement seront grandement réduits en limitant l'accès aux fichiers aux seules personnes qui en ont besoin dans l'accomplissement de leurs tâches.

[174] Chaque compte d'usager peut être assorti de différentes conditions limitant leur ouverture, leur modification ou leur effacement. Des droits différents peuvent être accordés de façon individuelle, ou encore plus généralement par catégories d'usagers (groupes de travail, ancienneté, etc.).

[175] La mise en œuvre de certains niveaux de droits d'accès devrait notamment permettre d'appliquer de façon efficace les règles du secret professionnel.

[176] Si de telles solutions sont envisagées, il est à conseiller d'établir clairement les règles entourant la gestion des comptes d'usagers et des permissions afférentes, et de les rendre disponibles à tous au sein du cabinet.

[177] Des règles régissant l'archivage des fichiers pourraient aussi être établies à ce chapitre, qu'il s'agisse de déterminer le format et le support de tels archivages.

4.2.2 Usage du courriel

[178] La plupart des entreprises fournissent à leurs employés des adresses de courriel dites corporatives, sous leur propre nom de domaine.

[179] Une première politique d'usage du courriel pourrait consister à établir les règles selon lesquelles le personnel pourra utiliser une telle adresse. Généralement, cet usage devrait être limité à l'accomplissement des fonctions de chacun au sein du cabinet et exclura tout usage personnel.

[180] L'utilisation d'une adresse corporative pour participer personnellement à certains forums de discussion ou comme identificateur sur des sites Internet devrait être formellement exclue pour éviter toute responsabilité éventuelle du cabinet ou toute mauvaise publicité. On verrait mal par exemple un employé utiliser une adresse courriel d'un bureau de notaires ou d'avocats dans le cadre d'un système d'échange de fichiers illicites, qu'il s'agisse de contravention au droit d'auteur ou carrément de fichiers pornographiques.

[181] D'autres politiques relatives à l'usage du courriel devraient aussi être considérées. Par exemple, le cabinet exigera-t-il que tout courrier électronique échangé dans le cadre d'un dossier, ou d'un type particulier de dossier, soit l'objet d'un chiffrement ? Exigera-t-on plutôt que cette précaution soit limitée aux courriels contenant des pièces jointes, laissera-t-on toujours la décision au soin du client[50] ?

---

50. Voir section **Erreur ! Source du renvoi introuvable.** ci-dessous sur le mandat professionnel.

[182] Le cabinet pourrait également décider à ce niveau de l'usage ou non d'un message d'avertissement à insérer aux communications électroniques, avisant que les informations incluses sont protégées par le secret professionnel.

[183] Il est certain que de telles décisions peuvent être prises à la pièce et que des dérogations resteront possibles en certaines circonstances particulières. L'avantage de leur insertion à une politique générale tient cependant à l'uniformisation des règles, ce qui permettra généralement d'assurer leur application et de mieux se conformer aux différentes obligations applicables en la matière.

[184] La démonstration de bonne foi face à la gestion des informations confidentielles et au maintien d'un environnement technique sécuritaire n'est pas non plus à dédaigner.

4.2.3 Accès à Internet, clavardage, P2P, etc.

[185] Finalement, un dernier exemple de politiques internes vise l'usage à des fins personnelles des outils technologiques.

[186] Le personnel sera-t-il autorisé à utiliser Internet sur les lieux de travail et à quelles conditions ? Pourra-t-il utiliser un service de clavardage pour communiquer avec des tiers à l'extérieur du réseau, ou encore installer et utiliser des applications d'échanges de fichiers (*peer-to-peer*, ou P2P).

[187] Si l'installation de tout logiciel implique un danger potentiel à la stabilité et à la sécurité d'un système informatique, les logiciels de type P2P présentent un risque documenté d'infection d'un système par des logiciels espions ou les virus tant à l'installation qu'à l'usage.

[188] Leur utilisation au bureau devrait donc être formellement interdite. De toute façon, la permission d'installer un logiciel sur tout poste de travail devrait être réservée aux quelques individus détenant un pouvoir d'administration sur les appareils afin d'éviter tout problème technique potentiel ou l'implication du cabinet dans des problèmes juridiques tenant au non-respect des licences de logiciels.

4.3 Examiner ses relations avec les tiers

4.3.1 Le mandat de services professionnels

[189] Du point de vue du praticien, l'usage des outils informatiques comporte des avantages certains. Meilleure productivité, meilleur accès à l'information, possibilités d'inscrire certains actes et procédures à distance, etc.

[190] Nous avons cependant vu que l'usage de ces outils comporte des risques, certains d'entre eux impliquant directement le client. Il est donc logique que le praticien aborde certaines de ces questions avec le client concerné, et laisse certaines décisions à sa discrétion. Le *mandat de services professionnels* pourrait donc être l'outil de choix pour éclaircir certains points.

[191] On pourrait par exemple autoriser ou interdire l'usage de certaines plate-formes électroniques, interdire ou permettre l'échange de certains types de fichiers (des états financiers par exemple) par courrier électronique ou convenir d'un processus de chiffrement.

[192] Le client pourrait autoriser les modes de communications à mettre en place dans la gestion de son dossier, courrier électronique, clavardage, etc.

[193] L'idée étant ici d'agir de façon transparente et d'éviter que les clients ne tiennent certaines situations pour acquis.

4.3.2 Situation d'assurance

[194] Une conclusion s'impose d'elle-même : la façon dont un juriste gère l'environnement technologique de son cabinet et les données qui y circulent entraine différents risques.

[195] Il s'agira principalement de risques de perte, qu'il s'agisse du matériel ou des fichiers, ou de risques de transmission inapropriée de certaines données conservées dans son système ou confiées à sa garde, que telle indiscrétion résulte d'un piratage (menace externe) ou de négligence (menace interne).

[196] Dans nos sociétés occidentales qui dit « risque » et « perte » sous-entend « assurance ». On peut donc se demander si les risques découlant de la gestion d'un environnement de bureau de l'ère technologique, plus particulièrement pour un professionnel du droit, sont assurables que ce soit au niveau de l'assurance responsabilité professionnelle ou carrément sous les assurances générales du cabinet.

[197] La gestion du risque informatique, pris dans une optique d'assurance, fait appel à une série d'étapes prédéfinies dont certaines correspondent à celles déjà proposées ci-dessus[51].

[198] Tout d'abord, les risques découlant d'une situation en particulier doivent être identifiés et hiérarchisés dans le but d'isoler ceux qui ont le plus de chances de se réaliser tout en présentant les conséquences potentielles les plus graves.

[199] L'adoption de politiques internes s'ensuit afin de modifier certains comportements pouvant entraîner leur concrétisation, ainsi que l'application préventive de solutions techniques requises (coupe-feu, anti-virus, etc.)

[200] L'application des politiques internes par le personnel devrait être encouragée de deux façons, d'un côté des récompenses et de l'autre des mesures dissuasives.

[201] Finalement, l'adoption d'un plan d'urgence précisant les mesures à adopter advenant la réalisation de certains risques pourrait être envisagée, seuls les risques résiduels devant être soumis à l'assurance[52].

[202] Ces propositions correspondent aux mesures que l'on serait tenté d'appliquer instinctivement, l'assurance ne devenant une solution que dans les cas extrêmes où les appareils ou les données sont irrémédiablement perdus, ou après qu'une fuite irréparable d'informations se soit produite.

---

51. L. TOUSIGNANT, diapositives d'un exposé intitulé *Les risques en émergence des affaires électroniques*, recueil préparé par Insight Information inc., Les aspects juridiques du commerce électronique, 2001.
52. Les suggestions faites dans les derniers paragraphes étant formulées par M. Tousignant dans sa présentation relatée en note 51 ci-dessus.

[203] Première question à se poser, les assurances responsabilités professionnelles couvrent-elles certains de ces risques ?

[204] Il nous faut constater que ces questions n'ont jusqu'à tout récemment pas été l'objet de règles très étendues. La police d'assurance responsabilité émise par le Fonds d'assurance responsabilité des notaires ne contenait aucune disposition à cet effet.

[205] On y insérait en octobre 2004 une exclusion de toute conséquence liée à une perte de données :

> 2.04 EXCLUSIONS : Le présent contrat ne s'applique pas à une Réclamation ou partie d'une Réclamation :
>
> [...]
>
> q) découlant de Dommages causés aux biens matériels ou immatériels ou de la perte de leur utilisation, de la perte de données, de la divulgation de renseignements personnels ou de toute autre perte directement ou indirectement liée à la réception ou à la transmission d'un virus informatique ou autre programme destructeur par Internet ou par toute autre voie électronique ou par tout accès non autorisé à une connexion Internet, à un réseau, à un ordinateur ou à un appareil de télécommunication.

[206] L'insertion de cette clause dans le contrat d'assurance responsabilité des notaires était expliquée de cette façon par la présidente du Fonds d'assurance :

> Le dommage causé par un virus informatique ne peut être couvert par le Fonds puisqu'il ne s'agit pas d'une réclamation à titre de dommages en raison d'un manquement dans la prestation d'un service professionnel rendu par le notaire à l'égard d'un tiers. Cette exclusion s'ajoute aux exclusions existantes portant sur l'utilisation d'un environnement informatique. D'ailleurs, la plupart des assureurs en responsabilité professionnelle canadiens ont déjà intégré à leur police une exclusion à ce sujet.[53]

[207] Peut-on alors se tourner vers les assurances de risques commerciales ou générales ? Celles-ci couvrent habituellement, et depuis longtemps, les risques généraux de perte de matériel advenant un sinistre classique.

---

53. M. OUELLET, *Faits saillants du programme 2005* (d'assurance responsabilité professionnelle), Chambre des notaires du Québec, Entracte, 15 novembre 2004.

[208] Les assurances commerciales du cabinet permettraient donc de remplacer du matériel informatique volé ou détruit lors d'un incendie par exemple. Certaines polices contiennent des couvertures spécifiques permettant la reconstitution de dossiers, mais ces garanties sont généralement limitées.

[209] À l'opposé, la plupart des contrats d'assurance contiennent des exclusions ou des limitations spécifiques quant aux risques virtuels ou les pertes de données informatiques. Quant à la couverture protégeant les assurés des conséquences d'actes criminels, elle exclut habituellement de façon spécifique la fraude informatique ou les détournements de données par le personnel.

[210] Il est donc loin d'être certain que les assurances générales du cabinet permettront de le dédommager en cas de problèmes liés à l'usage de l'informatique. Mais certains assureurs commencent à réagir et à offrir des produits spécifiques dans ce domaine.

[211] La conclusion prudente à en tirer est que les juristes devraient faire le bilan de leur situation d'assurance dans ce domaine, s'enquérir auprès de leur courtier d'assurance de la teneur de leur police quant au risque informatique, et chercher à obtenir des couvertures additionnelles, si nécessaire, pour se prémunir des conséquences de toute situation irréparable.

5. CONCLUSION

[212] L'informatique est un outil puissant. Si nous nous sommes émerveillés à son arrivée des miracles qu'elle permettait d'accomplir, aujourd'hui l'effet de nouveauté est passé et il faut constater sa quasi-banalité. Ce qui ne veut pas dire qu'elle doive être tenue pour acquis et que ses risques doivent être banalisés.

[213] Il importe donc que les règles de base balisant son usage soient appliquées et maintenues, et soient à ce point intégrées à notre travail qu'elles deviennent carrément des réflexes.

[214] C'est de cette façon que les juristes pourront espérer continuer à se conformer à leurs obligations fondamentales de respect du secret professionnel, de confidentialité et de préservation des données dans le nouveau et formidable contexte que leur offre l'informatisation.

6. BIBLIOGRAPHIE

A. Monographies

BARREAU DU QUÉBEC, *Développements récents en déontologie, droit professionnel et disciplinaire*, Service de la formation permanente, Cowansville, Éditions Yvon Blais, 2001.

BARREAU DU QUÉBEC, *Développements récents en droit familial*, Service de la formation permanente, Cowansville, Éditions Yvon Blais, 2002.

LES JOURNÉES MAXIMILIEN-CARON 1995, *Le respect de la vie privée dans l'entreprise : de l'affirmation à l'exercice d'un droit*, textes réunis par André Poupart, Montréal, Thémis, 1996.

MARQUIS, P-Y., *La responsabilité civile du notaire*, Cowansville, Éditions Yvon Blais, 1999.

PALLARD, H., *Déontologie juridique*, Moncton, Centre international de la common law en français, 2002.

ROY, A., *Déontologie et procédure notariales*, Montréal, Thémis, 2002.

B. Articles

CONDO, J.-C., « Logiciels espions : des peines de prison prévues dans une seconde loi, Branchez-vous », 7 octobre 2004, http://www.branchez-vous.com/actu/04-10/08-312904.html.

LAMBERT, J. et R. CASSIUS DE LINVAL, « Le secret professionnel à l'ère des communications, (1996-97) 99 *R. du N.* 84.

TÉTRAULT, M., « Le praticien et les technologies de l'information : le silence est d'or », BARREAU DU QUÉBEC, Service de la formation permanente, *Développements récents en droit familial*, Cowansville, Éditions Yvon Blais, 2002, p. 67.

DORAY, J., « Les dossiers des professionnels et les dossiers des ordres professionnels : un millefeuille de normes quasi inextricables », dans *Le respect de la vie privée dans l'entreprise* , actes de conférence, Les Journées Maximilien Caron 1995, Montréal, Thémis, p. 181 et s.

KAUFMAN, J., *Vie privée et pratique privée : les dix étapes essentielles à suivre*, Association du Barreau Canadien, Revue National, Association du Barreau Canadien, janvier-février 2004.

MOORE, G.E., « Cramming more components onto integrated circuits », Electronics, vol. 38, nº 8, 19 avril 1965, disponible sur Internet, ftp://download.intel.com/research/silicon/moorespaper.pdf.

THOUMYRE, L., « Spyware wanted dead or alive ! La FTC en guerre contre les logiciels espions », Juriscom.net, 21/10/2004 http://www.juriscom.net/actu/visu.php ?ID=583.

DUNBERRY, E., « L'archivage des documents électroniques », contenu dans l'ouvrage *Droit du commerce électronique*, collectif, sous la direction de Vincent GAUTRAIS, Montréal, Éd. Thémis, 2002, p. 87.

OUELLET, M., *Faits saillants du programme 2005 (d'assurance responsabilité professionnelle)*, Chambre des notaires du Québec, Entracte, 15 novembre 2004.

PELLETIER, F. et D. POULIN, « La préparation des documents pour distribution électronique », Comité canadien de la référence, septembre 2002, http://www.lexum.umontreal.ca/ccc-ccr/guide/docs/distribution_fr.html#_ftn1.

AMIOT, M.A, « Un arbitre confirme le renvoi d'un employé ayant abusé d'Internet », *La Presse*, 2 février 2000, p. A1.

LENFANT, J., « Le droit à la vie privée s'étend-il à l'utilisation du courriel par un employé dans le cadre de ses fonctions ? », mai 2000, travail universitaire publié sur Juriscom à l'adresse http://www.juriscom.net/uni/etd/04/priv01.pdf.

C. Études et sondages

AOL/NCSA Online Safety Study, Conducted by America Online and the National Cyber Security Alliance, October 2004, http://www.staysafeonline.info/news/safety_study_v04.pdf.

RBC Groupe Financier/Ipsos-Reid, *Les familles canadiennes et Internet*, Étude et sondage du 23 janvier 2002, http://www.rbc.com/nouvelles/pdf/20020123canfam_full_report-f.

AMERICAN BAR ASSOCIATION, Legal technology resource center survey report, 2002, http://www.lawtechnology.org/surveys/2002survey/ 2002survey_exec.pdf.

TOUSIGNANT, Luc, diapositives d'un exposé intitulé « Les risques en émergence des affaires électroniques », recueil préparé par Insight Information inc., *Les aspects juridiques du commerce électronique*, 2001.

D. Législation et réglementation

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5.

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

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-11.

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1.

Code de déontologie des avocats, R.Q. B-1, r. 1.

Code de déontologie des notaires, R.Q. N-2, r. 3.

Règlement sur la tenue des dossiers et des études des notaires, R.Q. N-2, r. 15.3.

Internet Spyware (I-SPY) Prevention Act of 2004, http://thomas.loc.gov/cgi-bin/query/D?c108:4:./temp/~c10823nLq6.

E. Jurisprudence

Société d'énergie Foster Wheeler Ltée c. *Société intermunicipale de gestion et d'élimination des déchets (SIGED) Inc.*, 2004 CSC 18.

Succession Macdonald c. *Martin*, [1990] 3 R.C.S. 1235.