Septembre 2001 • Édition spéciale n° 3

BULLETIN DE PRÉVENTION

du Fonds d'assurance responsabilité professionnelle du Barreau du Québec

ÉDITION SPÉCIALE

Cette édition spéciale du *Bulletin de prévention* du Fonds d'assurance responsabilité professionnelle du Barreau du Québec est entièrement consacrée aux technologies de l'information.

Vous y trouverez un résumé des propos tenus lors de l'atelier intitulé «*Déontologie et responsabilité professionnelle: le système informatique de votre bureau est-il une passoire?*», présenté dans le cadre du congrès annuel du Barreau du Québec au mois de mai 2001. À cette occasion, les conférenciers étaient Me Louise Comeau, syndic du Barreau du Québec, l'honorable Jean-Pierre Dumais, juge à la cour du Québec, le Sergent d'état-major Normand Vallée, spécialiste en sécurité informatique à la Gendarmerie Royale du Canada et Me Marie-Chantal Thouin, coordonnateur au Service de prévention du Fonds d'assurance responsabilité professionnelle du Barreau du Québec.

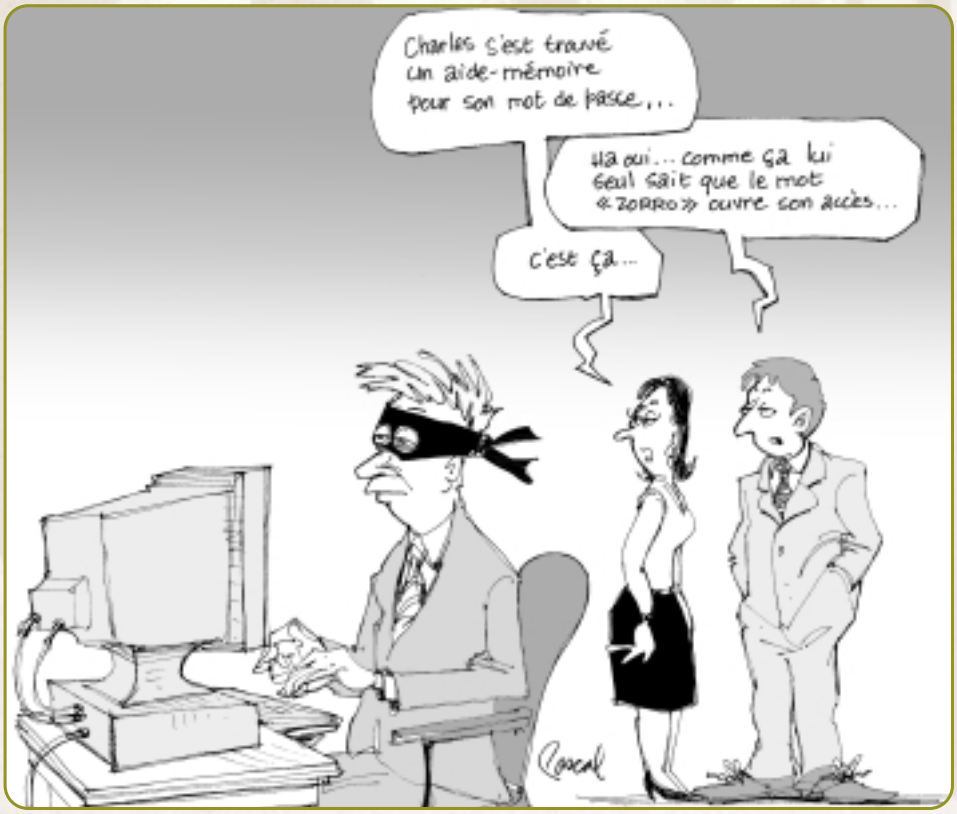
La sécurité avant tout

Soulignons d'entrée de jeu que l'expérience a démontré sans équivoque que les poursuites en responsabilité professionnelle sont le plus souvent dues aux lacunes dans l'organisation du travail dans les bureaux. Il serait bien que l'avènement des nouvelles technologies soit l'occasion de réduire les risques plutôt que de les accroître.

Voilà pourquoi nous vous proposons quelques pistes de réflexion.

Les technologies de l'information font maintenant partie intégrante de la pratique du droit. En conséquence, il importe de mieux comprendre les nombreuses possibilités qu'elles offrent, leurs limites et les risques découlant de leur utilisation. L'avocat se doit alors d'accroître ses connaissances informatiques et de développer une nouvelle compétence.[1]

Le manque de sécurité de l'Internet, les risques liés à l'utilisation du courrier électronique ont déjà défrayé les manchettes. Malheureusement, la sécurité défaillante des réseaux informatiques internes des entreprises en général, et celle des bureaux d'avocats en particulier, est trop souvent passée sous silence.



Confidentialité, intégrité, disponibilité. Voilà les trois critères que devrait rencontrer votre système de sécurité. Il est entendu qu'aucun système, aussi performant soit-il, n'assurera la confidentialité parfaite des données. Néanmoins, différents éléments peuvent contribuer à en augmenter la résistance, c'est-à-dire diminuer le risque de voir la confidentialité brisée.

Or, les membres de la profession juridique semblent peu soucieux de la sécurité de leur réseau et les illustrations sont nombreuses à cet effet. Pensons simplement aux mots de passe, lesquels sont librement échangés, laissés bien à la vue sur le coin du bureau, rarement modifiés, ou tout simplement non remplacés au départ d'un employé.

*(Voir **Sécurité...** page 2)*

INDEX

Le site Internet

À l'heure actuelle, l'Internet est sans contredit le moyen idéal pour atteindre un vaste public et une clientèle éventuelle. Cela explique fort probablement sa popularité croissante auprès des avocats.

Le site Internet habituel de l'avocat est celui où il annonce les services qu'il peut rendre. On y trouve habituellement le nom des membres du bureau, les domaines de droit traités, et certains ajoutent également de l'information de nature juridique d'ordre général.

D'autres, par contre, poussent l'utilisation de l'Internet un peu plus loin et rendent des services juridiques en ligne: testament, mandat en cas d'inaptitude, avis de cotisation à contester, divorce avec ou sans enfants, avec ou sans pension alimentaire, etc. Dans ces cas de services en ligne, l'internaute coche la ou les rubriques désirées, remplit le formulaire et retourne le tout. Sa demande sera ultérieurement traitée. Cette façon de faire n'est pas sans risques quant à la possibilité de voir sa responsabilité professionnelle engagée. En effet, l'une des premières mesures de prévention que nous recommandons est la mise en place d'un système adéquat[1] de sélection de la clientèle, chose qu'il est impossible de faire lorsque les services sont rendus en ligne. Il est en effet difficile de savoir combien d'avocats ont été consultés, si le client a les moyens de s'offrir vos services, et ses attentes ne peuvent être identifiées. Pensons également à toutes les erreurs de programmation qui peuvent survenir et par lesquelles par exemple, l'internaute utiliserait le mauvais formulaire. Certaines précautions essentielles doivent donc être prises pour éviter toute ambiguïté et problèmes ultérieurs.

La localisation géographique de votre bureau doit être indiquée, afin de ne pas induire l'internaute en erreur, par exemple sur l'applicabilité des règles énoncées. N'oublions pas que l'internaute trouvera de l'information provenant de plusieurs juridictions et il doit pouvoir obtenir celle qui est la plus pertinente. Sur la toile, vous êtes en concurrence avec le monde.

L'adresse postale et l'adresse électronique doivent apparaître, et évidemment il importe de désigner au moins un avocat responsable de répondre aux questions ou commentaires provenant du site.

Vous devriez être en mesure de fournir en tout temps une preuve imprimée du contenu du site à un moment précis. Une copie de toute l'information contenue sur le site doit être conservée en cas de litige.

Nous vous recommandons l'inclusion d'un avertissement précisant que l'information contenue, bien qu'elle soit de nature juridique, ne constitue pas un avis juridique et qu'au surplus, l'envoi d'un courrier électronique comportant une question précise n'a pas pour effet d'établir automatiquement une relation avocat/client et ne signifie pas non plus qu'il y a acceptation du mandat de votre part.

Si le site est conçu pour rendre des services en ligne, il faut également penser aux litiges éventuels. Des moyens appropriés doivent donc être pris pour qu'un expert puisse confirmer la teneur des échanges et les dates auxquels ils ont eu lieu.

Ajoutons que si des services sont rendus en ligne, il importe que le site soit sécurisé, notamment en ce qui concerne la transmission d'informations de nature personnelle et confidentielle, tel le numéro de carte de crédit.

1 Voir à ce sujet le *Guide de prévention en responsabilité professionnelle* publié par le Fonds d'assurance, édition Janvier 2001, p. 1

Recommandations du Sergent d'état-major Normand Vallée
Gestionnaire, Service Soutien aux opérations
Spécialiste en sécurité informatique
Gendarmerie Royale du Canada

Sites Internet à consulter:

- **Cryptographie des documents électroniques**
  http://www.WinMagic.com
  http://www.WinMagic.com/white.html
  http://www.entrust.com/solo/solo_eval.htm
  http://www.entrust.com/solo/solo_refcard.pdf

- **Logiciels pare-feu (Fire wall)**
  http://www.zonelabs.com
  http://www.zdnet.com/downloads/partners/zonealarm/download.html
  http://www.webattack.com/freeware/security/fwvirus.shtml

- **Logiciel Antivirus**
  http://securityl.norton.com/us/intro.asp?venid=sym&langid=us

Sécurité...

(Suite de la page 1)

Afin d'améliorer la sécurité des réseaux internes, il est notamment recommandé de ne pas inscrire le mot de passe au poste de travail, de choisir un mot qui contient par exemple un chiffre, une majuscule ou un caractère alphanumérique. Le mot de passe devrait être remis sous scellé à quelqu'un en autorité qui mettra cette information en sécurité. Ainsi, en cas d'oubli, d'urgence, d'accident, des tiers en autorité pourront avoir accès au système et à vos données.

Une autre mesure doit impérativement être instaurée, celle des copies de sauvegarde. Celles-ci doivent être faites quotidiennement et entreposées dans un endroit sécuritaire à l'extérieur du bureau. De cette façon, peu importe ce qui arrive à votre système informatique, vos fichiers et bases de données pourront être aisément récupérés et réinstallés; vous pourrez ainsi continuer à opérer, ce qui ne serait pas le cas sans copies de sauvegarde.

La meilleure, sinon la seule précaution à prendre, que l'on parle de la survenance d'un sinistre de type incendie ou inondation, du bris ou de la défectuosité de l'équipement survenant au moment d'une mise à niveau ou d'un virus, est la prise régulière de copies de sauvegarde.

Les virus ont suffisamment fait parler d'eux au cours des derniers mois pour que nous soyons alertés de ce danger. Votre système détruit, ou tout simplement paralysé par un virus ou parce que vous êtes victimes de piratage, pourrait vous causer bien des ennuis: nombreuses heures, voire semaines consacrées à tout rebâtir, données à jamais perdues; nous imaginons facilement les conséquences que cela pourrait avoir.

Le choix d'un antivirus adéquat et d'un garde-barrière est donc également indispensable;[2] il mérite que l'on s'y penche sérieusement. Une bonne façon d'arriver à faire un choix judicieux consiste à former un comité interne pour choisir l'équipement, rédiger la politique d'utilisation et assurer une formation adéquate du personnel.

1 Le barreau de l'Alberta va d'ailleurs dans ce sens. Voir à ce sujet «*Guidelines on Ethics and the New Technology, Part I*» sur le site www.lawsocietyalberta.com

2 Voir à ce sujet les recommandations du Sergent d'état-major Normand Vallée ci-dessus.

Le courrier électronique

La question qui se pose est de savoir si l'avocat peut utiliser le courrier électronique dans le cadre de ses relations avocat/client.

Or, nous le savons, le courrier électronique circule à ciel ouvert telle une véritable carte postale. Il est donc normal que les membres de la profession juridique s'interrogent à savoir si celui-ci peut être utilisé dans l'exercice de leur profession et, le cas échéant, si les messages ainsi transmis devraient toujours être cryptés.

L'*American Bar Association* (ABA) a émis en 1999 un avis précisant que l'envoi de messages non cryptés ne constituait pas un manquement au devoir de confidentialité. On y recommande toutefois d'utiliser la cryptographie lorsque la teneur du message le justifie.

Au Canada, à notre connaissance, seul le barreau de l'Alberta s'est prononcé officiellement sur l'opportunité d'utiliser le courrier électronique dans les relations avocat/client. On est d'avis que le seul fait de ne pas avoir crypté la communication ne constitue pas une faute.[1]

À ce jour, aucun avis n'émane officiellement du Barreau du Québec. Néanmoins, nous suggérons la mise en place de certaines mesures afin de réduire les risques de vous voir adresser quelque reproche que ce soit quant à l'utilisation de ce mode de communication:

- informer en tout premier lieu le client des risques liés à l'utilisation du courrier électronique
- ajouter une page de garde, comme c'est devenu l'habitude lors de l'utilisation du télécopieur, informant de la nature confidentielle de l'information transmise
- crypter les messages hautement confidentiels.

Il peut également s'avérer important de protéger la confidentialité des documents joints au courrier électronique, notamment en n'oubliant pas d'effacer les traces des travaux qui ont pu être effectués sur le document lorsque la propriété «version antérieure» est activée. Cette fonction permet effectivement de conserver toutes les versions d'un document en une seule. Elle permet donc au destinataire d'accéder à ces différents documents en réactivant tout simplement cette fonction. Ainsi, le récepteur du document pourrait facilement reconstituer les documents antérieurs, plaçant alors l'avocat dans une situation embarrassante si ceux-ci permettent de déceler sa stratégie, ses commentaires, ou tout simplement ses impressions quant au dossier. Il est aussi recommandé de retirer le texte caché et les autres propriétés de texte.[2]

Le cryptage

Afin de protéger adéquatement l'information détenue ou transmise, il est parfois nécessaire d'avoir recours à la cryptographie. La norme actuelle habituellement reconnue est de 128 bits.[3] Au Canada, la cryptographie peut être utilisée librement. Toutefois, l'avocat traitant avec des gens à l'étranger pourrait être confronté à un problème de taille au moment de l'utiliser hors Canada. Le récepteur doit bien évidemment, pour ouvrir un message crypté, posséder le logiciel requis. Or, cela ne sera pas possible si la loi du pays où il se trouve l'interdit. Par exemple, nous savons que la Chine, l'Inde, l'Irak, le Pakistan, la Russie, la Tunisie et le Vietnam exercent un très fort contrôle quant à l'utilisation, l'importation ou encore l'exportation du matériel de cryptographie.[4]

On parle beaucoup de la protection des documents que l'on transmet par voie de courrier électronique mais n'oublions pas qu'une personne peut, à distance, s'introduire dans votre ordinateur et accéder à vos dossiers. Il peut donc être nécessaire de chiffrer les documents se trouvant dans votre ordinateur et d'utiliser un pare-feu ou garde-barrière pour limiter les risques d'intrusion.[5]

À FAIRE

- ✔ limiter les privilèges d'accès à vos documents
- ✔ établir une politique de sécurité dans votre bureau
- ✔ changer votre mot de passe souvent (aux 3 mois) et le mettre dans une enveloppe scellée sans y faire référence et garder en lieu sûr
- ✔ utiliser un mot de passe alphanumérique, avec majuscules, d'au moins 6 caractères et substitution de caractères, i.e. @ = a, $ = s, ! = 1, etc.
- ✔ activer votre écran de veille à 5 minutes avec mot de passe
- ✔ protéger les documents confidentiels avec un mot de passe, pour la lecture et la modification
- ✔ utiliser un logiciel «Antiviral» et effectuer les mises à jour régulièrement
- ✔ utiliser un pare-feu (Firewall) et effectuer les mises à jour régulièrement
- ✔ faire des copies de sauvegarde (Backup) de vos fichiers et de votre information jugée essentielle
- ✔ garder les copies de sauvegarde sous clé, dans un lieu sûr, dans une autre pièce ou site
- ✔ à la maison, la sécurité informatique est l'affaire de tous
- ✔ vérifier les logiciels, jeux, fichiers, vidéo pour vous assurer qu'ils ne contiennent pas de virus
- ✔ garder vos logiciels de sécurité Internet à jour
- ✔ faire réparer votre ordinateur par une firme dont les techniciens ont fourni un certificat de police

À NE PAS FAIRE

- ✘ partager son mot de passe ou **NIP** (**N**uméro d'**I**dentification **P**ersonnel) avec quelqu'un
- ✘ télécharger des logiciels gratuits, bandes vidéo ou jeux vidéo de sites dont vous n'avez pas confiance
- ✘ ouvrir les pièces jointes *(attachment)* de courriels dont vous ne connaissez pas la provenance
- ✘ répondre à des courriels «*junk mail*» ou à des «*spam*»
- ✘ donner vos coordonnées ou informations personnelles dans les salles de bavardage «*chat room*»
- ✘ utiliser le même mot de passe pour accéder à des sites différents
- ✘ configurer le branchement dans Internet en mode automatique, **toujours y accéder en mode manuel**

---

1 «*Guidelines on Ethics and the New Technology – Part III*»
2 Pour d'autres renseignements concernant l'usage du courrier électronique, voir le *Bulletin de prévention* publié par le Fonds d'assurance responsabilité professionnelle du Barreau du Québec de mars 2000, Vol. 1, no. 2, p.3, disponible sur le site Internet du Fonds d'assurance: www.assurance-barreau.com
3 Voir encadré pour les recommandations formulées par le Sergent d'état-major Normand Vallée.
4 Létourneau, Emmanuel «*Cryptographie: ce que vous devez savoir*» Journal du Barreau, volume 33, no. 5, 15 mars 2001.
5 note 3

Une politique d'utilisation pour tous

Une politique d'utilisation de l'équipement informatique devrait être établie et s'appliquer à tous ceux ayant accès aux ressources. Cette politique devrait englober tant l'utilisation de l'équipement liée aux fonctions professionnelles que celle visant des fins personnelles. En effet, inutile de se le cacher, le courrier électronique, et l'Internet de façon plus générale, servent à des fins personnelles tant sur les heures de bureau qu'à l'extérieur de celles-ci.

Pour être efficace, la politique devrait être expliquée et rappelée de façon régulière, par exemple, en faisant signer un engagement à cet égard annuellement.

Voici un exemple de ce que l'on devrait trouver dans une telle politique d'utilisation:

- un avis à l'effet que le système de sécurité informatique de l'entreprise enregistre les sites Internet visités et le temps d'utilisation
- l'interdiction de naviguer sur certains sites racistes, de pornographie juvénile, etc.
- l'interdiction d'enregistrer du matériel ou des logiciels sans avoir obtenu une autorisation au préalable des autorités compétentes
- l'utilisation des courriels doit être limitée aux besoins des fonctions exercées
- le courriel ne doit pas être utilisé pour transmettre de l'information confidentielle
- les mots de passe doivent demeurer confidentiels
- la sanction applicable en cas de non-respect de l'ensemble de la politique devrait également être prévue.[1]

1 Source: David J. Bilinsky, Law Society of British Columbia, «*Sample Internet and E-mail Use Policy*»

L'assurance d'être bien protégé

Victime de piratage, données détruites par un virus, bris de l'équipement entraînant la perte de son contenu, virus se transmettant à votre insu à tous vos correspondants endommageant leur système et paralysant leurs opérations, courriels confidentiels transmis au mauvais destinataire, etc. autant de scénarios cauchemardesques susceptibles de se produire et qui pourraient vous laisser dans l'embarras, et pour lesquels on pourrait tenter de vous tenir responsable.

Si cela se produisait malgré toutes les précautions prises, êtes-vous adéquatement protégé?

La police du Fonds d'assurance responsabilité professionnelle du Barreau du Québec vous protège pour les erreurs et omissions commises à l'occasion de services professionnels. La notion de services professionnels est définie au contrat:

> «**1.04 – SERVICES PROFESSIONNELS**: Tous les services qui ont été rendus ou qui auraient dû être rendus par l'**Assuré**, directement ou indirectement, dans le seul exercice de la profession d'avocat et en tant que membre en règle du Barreau du Québec […]»

En conséquence, pour que la garantie puisse trouver application, les dommages devront avoir été causés dans le cadre de la relation avocat/client. Cela signifie par exemple, que le coût occasionné par la perte de données et la reconstitution du système ne saurait être couvert. Par contre, si une prescription était omise de ce fait, entraînant des dommages à votre client, cette perte serait susceptible de l'être.

Il y aurait donc lieu de vérifier auprès de votre assureur excédentaire ou auprès de celui vous octroyant une police multirisques commerciale, l'étendue de la protection dont vous bénéficiez et si celle-ci couvre également les dommages qui pourraient être causés à des tiers, par exemple lors de la propagation d'un virus. Notons par ailleurs qu'il existe des assurances offrant une couverture Internet ciblant plus particulièrement le commerce électronique, c'est-à-dire l'interruption du commerce causant une perte de revenus, la diffamation présente sur un site Web, le droit à la vie privée – par exemple, le piratage ayant permis à des tiers de retracer les numéros de cartes de crédit de vos clients – la transmission d'un virus à des tiers, etc.

Ce **Bulletin de prévention** est publié par le Fonds d'assurance responsabilité professionnelle du Barreau du Québec

Service de prévention
Me Marie-Chantal Thouin, Coordonnateur
445, boul. Saint-Laurent, bureau 550
Montréal, QC H2Y 3T8
Téléphone: (514) 954-3452, ou 1-800-361-8495, poste 3282
Télécopieur: (514) 954-3454
Courrier électronique: info@assurance-barreau.com
Visitez notre site Internet: www.assurance-barreau.com

Une version anglaise est aussi disponible sur demande.
An English version is available upon request.