

ASSOCIATION DU BARREAU CANADIEN

**Renseignements complémentaires au
CODE DE DÉONTOLOGIE PROFESSIONNELLE**

**Lignes directrices pour un exercice du droit
conforme à la déontologie dans le cadre
des nouvelles technologies de l'information**

Septembre 2008

***Comité de déontologie et de questions professionnelles
Association du Barreau canadien***

Coprésidents

David C. Day, c.r.
St. John's

Alan J. Stern, c.r.
Halifax

Membres

Inez Cardinal, c.r.
Saskatoon

Felicia S. Folk
Vancouver

Shannon Farrell
Charlottetown

Paul D. Paton
Kingston

Consultante pour le projet

Elizabeth F. Judge, Ph.D.
Faculté de droit, Université d'Ottawa, Ottawa

Conseillère en rédaction

Vicki Schmolka
Kingston

Personne-ressource

Kerri Froc
ABC, Ottawa

Lignes directrices pour un exercice du droit conforme à la déontologie dans le cadre des nouvelles technologies de l'information

Table des matières

1. Introduction
2. La compétence de l'avocat
3. La confidentialité
4. Le cryptage
5. Le secret professionnel
6. Le stockage, la conservation et la suppression électroniques
 - Le stockage
 - L'archivage
 - La suppression
7. Les métadonnées
8. La sécurité
9. La commercialisation
10. L'accessibilité
11. La prestation de service
12. La propriété intellectuelle et les logiciels
13. Les sources juridiques électroniques et la recherche documentaire
14. La participation aux discussions en ligne

Annexes

Annexe 1 : Les sources documentaires

1. Renseignements d'ordre général
2. Les sources documentaires pour effectuer des recherches juridiques en ligne sur le droit canadien
3. La déontologie juridique et les nouvelles technologies de l'information
 - i. Les « Lignes directrices sur la déontologie et la nouvelle technologie »
 - ii. Autres
4. Les sources relatives aux technologies de l'information
5. Les sources documentaires sur des sujets particuliers
 - a. Introduction
 - b. Le stockage, la conservation et l'archivage électroniques
 - c. La commercialisation
 - d. L'accessibilité
 - e. La propriété intellectuelle et les logiciels
 - f. Les sources juridiques électroniques et la recherche documentaire

Annexe 2 : Renseignements et sources documentaires sur les métadonnées

1. Les sources documentaires
2. Les pratiques de rédaction qui créent ou transfèrent des métadonnées
3. La réduction et la suppression des métadonnées
 - a. La réduction de la production de métadonnées

- b. La gestion et la suppression des métadonnées
 - i. L'utilisation de fonctions intégrées au programme
 - ii. L'installation des logiciels compagnons du fournisseur de programme
 - iii. L'utilisation de programmes de fournisseurs indépendants
- 4. Références et sources documentaires au sujet des métadonnées

Annexe 3 : Mesures à prendre pour améliorer la sécurité des technologies de l'information

- 1. Les copies de secours
- 2. Les restrictions d'accès et les protocoles d'authentification
- 3. Le cryptage
- 4. Les coupe-feu et les logiciels de détection d'intrusion
- 5. Les logiciels antivirus et les suites logicielles de sécurité
- 6. Les politiques en matière de sécurité informatique pour les employés et le personnel
- 7. La sécurité des renseignements personnels
- 8. Les réseaux sans fil
- 9. Sources documentaires en matière de sécurité

Lexique

Introduction

Lorsque l'on sait comment les utiliser, les nouvelles technologies de l'information permettent de gagner du temps, de gagner en efficacité et d'améliorer les services rendus. Elles profitent tant aux avocats qu'à leurs clients.

Les présentes lignes directrices recommandent certaines pratiques exemplaires en matière d'utilisation des technologies de l'information. Elles ne constituent pas un ensemble de règles obligatoires. Pour connaître les règles obligatoires qui vous sont applicables, veuillez consulter le code de déontologie de votre ordre professionnel.

Les lignes directrices complètent le Code de déontologie de l'ABC et servent à guider les avocats lorsqu'ils ont recours aux nouvelles technologies.

Elles soulignent certaines pratiques exemplaires en matière d'utilisation des technologies de l'information, en insistant sur la nécessité de préserver la sécurité des renseignements, de maintenir le secret professionnel et d'assurer le respect de la vie privée des clients.

L'un des traits saillants des technologies de l'information réside dans la rapidité avec laquelle elles sont intégrées dans notre travail et dans notre environnement ainsi que dans la rapidité avec laquelle elles deviennent obsolètes et sont remplacées.

De manière inévitable, les tribunaux sont appelés à rendre des décisions sur les responsabilités déontologiques et juridiques des avocats, en réponse à cette révolution technologique. Certaines décisions récentes ont conclu que les avocats ont, dans certaines circonstances, l'obligation déontologique d'utiliser les nouvelles technologies ou, à tout le moins, d'avoir recours à quelqu'un qui est en mesure de le faire.

Le Comité de déontologie et de questions professionnelles procèdera à une mise à jour régulière des présentes lignes directrices de sorte qu'elles demeurent pertinentes et utiles pour les avocats qui pratiquent. Votre collaboration est la bienvenue. Veuillez nous mentionner tout élément que nous aurions omis d'indiquer et nous faire des suggestions quant aux ressources ou autres renseignements qui devraient être ajoutés aux lignes directrices.

L'ABC ne cautionne aucun produit mentionné dans les présentes lignes directrices.

Les lignes directrices comprennent des renseignements concernant des ressources particulières. Certaines sources sont disponibles à la vente, d'autres sont gratuites. Dans l'un et l'autre cas, le fait qu'une ressource soit mentionnée dans les lignes directrices ne signifie pas que l'ABC cautionne ce produit. Cette mention ne vise qu'à offrir aux avocats des renseignements pratiques et faciles d'accès leur permettant de faire leur propre choix.

Les technologies de l'information comprennent :

- les logiciels bureautiques de productivité (notamment les applications telles que les traitements de texte, les feuilles de calcul électroniques et les présentations);
- la recherche juridique assistée par ordinateur;
- le courriel;
- le dépôt de documents par voie électronique;
- la messagerie vocale;
- les dispositifs sans fil, tels que les périphériques sans fil (souris, claviers, imprimantes);
- les téléavertisseurs, les téléphones cellulaires, les appareils radios émetteurs-récepteurs;
- les dispositifs de localisation par satellite;
- les assistants numériques;
- les téléphones intelligents;
- les télécopieurs;
- la voix par IP (communication téléphonique via une connexion Internet à large bande);
- la vidéoconférence (télécommunications interactives audio et vidéo);
- l'intranet (réseau informatique privé – « versions privées d'Internet » – qui utilise les protocoles d'Internet pour partager les renseignements et les ressources, mais qui se limite habituellement aux employés de l'entreprise);
- les extranets (parties de l'intranet auxquelles peuvent accéder des personnes qui ne font pas partie de l'entreprise, tels que des clients ou des fournisseurs);
- des réseaux externes, dont Internet.

1. La compétence de l'avocat

Le Code de déontologie de l'ABC : la compétence de l'avocat

La règle prescrite au chapitre II (Règle II) du Code prévoit ce qui suit :

1. L'avocat doit s'acquitter avec compétence des services juridiques qu'il donne à son client.
2. L'avocat doit accomplir sa tâche consciencieusement et fournir au client des services d'une qualité équivalente à celle que des avocats eux-mêmes attendraient, en général, d'un confrère compétent placé dans la même situation.

Le commentaire 4 sur la Règle II, ajouté au Code en 2004, traite spécifiquement de la compétence en matière de technologie :

Cette compétence dépasse la simple connaissance de principes juridiques. Elle suppose en outre une connaissance suffisante de la pratique et de la procédure nécessaires à leur mise en œuvre. Un avocat doit donc se tenir au courant de l'évolution du droit dans ses domaines d'exercice. L'avocat devrait également acquérir et entretenir son aptitude à recourir à la technologie spécifique à son domaine d'exercice afin de conserver un niveau de compétence auquel on peut raisonnablement s'attendre de la part des avocats dans le cadre de leur pratique. [non souligné dans l'original]

Au sujet du « recours à une aide extérieure », le commentaire 6 sur la Règle II souligne, entre autres, ce qui suit :

Un avocat ne doit pas hésiter à dévoiler son incompétence à traiter une affaire déterminée et reconnaître, qu'en s'en chargeant, il rendrait un mauvais service à son client.

Les pratiques exemplaires en matière de compétence de l'avocat

Afin de s'acquitter de leur obligation déontologique de compétence au sens de la Règle II, les avocats doivent être en mesure de reconnaître quand le recours à une technologie est nécessaire à la prestation de services juridiques pour le compte de leur client et d'utiliser la technologie d'une manière responsable et conforme à l'éthique professionnelle.

Un avocat peut s'acquitter de ce devoir en ayant lui-même de bonnes connaissances au sujet de cette technologie et en utilisant celle-ci, ou en ayant recours à d'autres personnes qui maîtrisent bien cette technologie. Les avocats doivent également avoir une bonne connaissance des technologies dont se servent leurs clients, lorsque les conseils juridiques qu'ils leur donnent en dépendent.

2. La confidentialité

Le Code de déontologie de l'ABC : la confidentialité

La règle au chapitre IV (Règle IV) du Code prévoit ce qui suit :

Conserver les renseignements à titre confidentiel

1. L'avocat est tenu de garder le secret le plus absolu sur ce qu'il a appris des affaires et des occupations de son client au cours de leurs relations professionnelles. Il ne peut être relevé de ce devoir qu'avec l'autorisation soit expresse, soit tacite de son client, ou encore lorsque la loi ou le présent Code le prévoient.

Le premier principe directeur de la Règle IV se lit comme suit :

L'exercice efficace de la profession serait inconcevable en l'absence de communications franches et sans réserve entre le client et son avocat. Le client doit pouvoir compter sur l'entière discrétion de l'avocat et être assuré que, sauf en cas d'autorisation expresse de sa part, tout ce qu'il lui aura révélé ou dont il aura discuté avec lui restera complètement secret et confidentiel.

Les pratiques exemplaires en matière de confidentialité

Les principes du Code doivent être appliqués à tous les moyens de communication, y compris les communications électroniques au moyen de nouvelles technologies de l'information. Les avocats doivent exercer la même vigilance et faire preuve du même souci pour les questions de nature confidentielle quelle que soit la technologie de l'information à laquelle ils ont recours.

Les avocats doivent veiller à ce que toute communication électronique avec leurs clients ou au sujet de ceux-ci se fasse en toute sécurité et que des tiers non autorisés ne puissent y avoir accès. Lorsqu'ils transmettent des renseignements confidentiels à leurs clients ou au sujet de leurs clients, les avocats doivent utiliser toutes les mesures raisonnables qui s'imposent afin de réduire autant que possible les risques que ces renseignements ne soient dévoilés ou interceptés. Afin de déterminer s'ils doivent ou non utiliser un certain type de technologie de l'information pour transmettre des renseignements confidentiels à leurs clients ou au sujet de leurs clients, les avocats doivent évaluer la situation de différents points de vue. Quels sont les risques de divulgation ou d'interception par inadvertance liés à l'utilisation de cette technologie? Quelles seront les répercussions du choix de cette technologie à l'égard du client en termes de coûts, d'accessibilité et de facilité d'utilisation?

Les avocats doivent informer leurs clients des risques de divulgation ou d'interception non autorisée avant d'avoir recours aux technologies de l'information. Les avocats doivent s'assurer que leurs clients comprennent également qu'ils doivent protéger la confidentialité des communications qui leur sont transmises. Il peut être indiqué d'obtenir

le consentement du client préalablement à l'utilisation d'un certain type de technologie de l'information.

Les avocats doivent d'autre part être conscients que l'évolution des technologies de l'information signifie que les risques évolueront au fil du temps. Par exemple, avec le passage des répondeurs téléphoniques aux messageries vocales numériques, les messages téléphoniques posent des risques en matière de confidentialité qui sont semblables à ceux que posent les communications par courriel, à savoir qu'il est facile de les enregistrer, de les copier et de les faire suivre.

3. Le cryptage

Les lignes directrices des ordres professionnels de juristes sur le cryptage

Les « Lignes directrices sur la déontologie et la nouvelle technologie » de la Fédération des ordres professionnels de juristes du Canada, qui ont été adoptées par un grand nombre d'ordres professionnels de juristes sous la forme dans laquelle elles ont été publiées ou sous une forme révisée (voir l'annexe 1, Les sources documentaires, 3 i)), conseillent aux avocats d'utiliser le cryptage lorsqu'il est question de renseignements « très délicats ». Toutefois, l'évolution des technologies et du droit permettent d'utiliser le cryptage pour protéger tous les renseignements confidentiels. Il s'agit d'une question qui est amenée à évoluer.

Dans de récentes décisions, des commissaires à la protection de la vie privée provinciaux ont statué que les renseignements personnels doivent être cryptés lorsqu'ils sont stockés sur des dispositifs vulnérables, tels que des ordinateurs portatifs ou des clés USB. Veuillez consulter à ce sujet la décision de mars 2007 du Bureau de la commission à l'information et à la protection de la vie privée de l'Ontario et la décision de septembre 2006 de la Commission à l'information et à la vie privée de l'Alberta (citées à l'annexe 1, Les sources documentaires, 5 b)).

Les pratiques exemplaires en matière de cryptage

Il est donc recommandé aux avocats de prendre les mesures suivantes :

- utiliser le cryptage pour protéger les renseignements confidentiels qui sont transmis par voie électronique (*p. ex.*, les courriels);
- restreindre l'accès aux ordinateurs (*p. ex.*, avec un mot de passe sécuritaire et en ayant recours au cryptage) pour protéger les renseignements confidentiels qui sont stockés par voie électronique, notamment sur les dispositifs de stockage portatifs (*p. ex.* les clés USB), les dispositifs informatiques portatifs (*p. ex.* les ordinateurs portatifs et les assistants numériques), ainsi que sur les ordinateurs de bureau et les ordinateurs en réseau; et
- utiliser le cryptage de disques en entier pour tout dispositif informatique portatif.

Vous pourrez trouver des renseignements complémentaires sur les mots de passe et le cryptage à l'annexe 3, « Mesures à prendre pour améliorer la sécurité des technologies de l'information ».

4. Le secret professionnel

Le Code de déontologie de l'ABC : le secret professionnel

Les renseignements confidentiels comprennent des renseignements protégés par le secret professionnel. Le troisième principe directeur de la Règle IV du Code énonce ce qui suit :

L'importance d'adopter une règle déontologique encore plus générale est illustrée par la position de la Cour suprême du Canada sur le privilège du secret professionnel. La Cour a statué que ce privilège doit être respecté de la façon la plus absolue possible si l'on veut lui conserver sa pertinence. Le privilège du secret professionnel est une règle de preuve, un droit civique et juridique primordial et un des principes de justice fondamentale au Canada. Le public a un intérêt impérieux à préserver l'intégrité des relations entre l'avocat et le client. Les communications confidentielles échangées avec un avocat constituent un exercice important du droit à la vie privée et sont essentielles pour l'administration de la justice dans un système contradictoire.

Les pratiques exemplaires en matière de secret professionnel

Les avocats doivent veiller à protéger la confidentialité et le caractère privilégié des communications par voie électronique avec la même diligence que l'on attend normalement d'eux lorsqu'ils utilisent un mode de communication traditionnel.

5. Le stockage, la conservation et la suppression électroniques

Les règles de pratique sur la conservation et la production électroniques

Dans plusieurs juridictions canadiennes, la définition des termes « document » et « dossier », dans les règles de procédure civile et les règles de pratique des tribunaux concernant la conservation et la communication préalable des documents, vise tant les formats sur papier que les formats électroniques.

Les pratiques exemplaires en matière de stockage, de conservation et de suppression électroniques

Le stockage

Afin de protéger les renseignements électroniques, il est nécessaire de prendre des mesures afin de les stocker et d'en avoir des copies de secours sur place ainsi que dans un emplacement situé à l'extérieur du cabinet.

Pour ce faire, les avocats doivent prendre les mesures suivantes :

- faire des copies de secours des renseignements stockés par voie électronique, si possible de manière quotidienne; et
- conserver une copie des données sur des supports de stockage amovibles (tels que les CD-R, les CD-RW, les DVD-R, les DVD-RW, les bandes magnétiques, les disques durs amovibles et autres supports magnétiques et optiques) dans un emplacement sûr, situé à l'extérieur du cabinet, à l'abri du feu, des dégâts d'eau, de la chaleur et des autres risques à leur intégrité.

Le stockage physique de renseignements informatisés dans un lieu situé à l'extérieur du cabinet protège les données contre le risque d'altération ou de perte, tout en simplifiant la récupération des données en cas de catastrophes telles les incendies, les inondations, les tremblements de terre, les pannes d'électricité et les surtensions, ou la destruction de l'emplacement physique du cabinet juridique.

Les applications technologiques deviennent parfois obsolètes (*p. ex.* les disquettes de format 5 ¼ pouces) et le support sur lequel sont stockés les renseignements peut se détériorer au fil du temps et rendre les renseignements illisibles ou irrécupérables. Les avocats doivent donc prendre les mesures suivantes de façon systématique :

- revoir les politiques concernant les méthodes de stockage et les copies de secours pour les renseignements électroniques afin de s'assurer que les méthodes choisies demeurent compatibles avec la technologie actuelle; et
- vérifier les renseignements électroniques stockés pour s'assurer que les renseignements sont récupérables et que le support et les applications sont en bon état de fonctionnement.

Il peut être indiqué pour certains clients de stocker uniquement les données par voie électronique, mais il peut être prudent pour d'autres clients de conserver à la fois des copies électroniques et des copies papier. Un bureau « sans papier » signifie un bureau dont la politique est de ne pas conserver de copies sur papier, sauf lorsque l'exemplaire original sur papier est nécessaire pour des motifs de preuve ou pour d'autres motifs juridiques. Les facteurs dont il faut tenir compte avant d'opter pour une relation « sans papier » avec un client sont les préférences du client, les ressources à sa disposition, ses connaissances de la technologie et sa familiarité avec cette dernière, ainsi que les obligations juridiques qui découlent des règles sur la conservation de documents et sur la communication préalable par voie électronique.

L'archivage

Les avocats doivent mettre en place des politiques de gestion des documents qui soient conformes aux exigences légales en matière de conservation de fichiers pour les renseignements électroniques. Lorsque ces obligations exigent la conservation d'un dossier, les renseignements doivent être préservés sans modification et doivent être à l'abri des altérations, du pillage et de la suppression. Il faut avoir recours à des méthodes d'archivage appropriées pour préserver les renseignements électroniques qui ne sont pas stockés sur le système informatique actif du cabinet juridique.

Les renseignements concernant les clients qui sont conservés sous format électronique posent des difficultés particulières en ce qui concerne la divulgation et la production de documents dans le cadre de la communication préalable de documents par voie électronique, à cause du caractère potentiellement très large et très coûteux de celle-ci, des incertitudes quant à la forme de la production, des difficultés que posent la préservation de l'intégrité des renseignements, ainsi que du problème de l'évaluation de la proportionnalité des coûts et du temps qu'il faudra consacrer à la production de renseignements électroniques susceptibles d'être pertinents par rapport à la nature, à l'objectif et à la complexité du litige en question.

Les lignes directrices et les pratiques exemplaires recommandées dans le cadre de la communication de documents par voie électronique comprennent notamment les lignes directrices de l'Ontario sur la communication de documents électroniques et les principes de Sedona Canada sur la production de documents électroniques. Ils recommandent de rencontrer les clients à intervalles réguliers pour discuter des questions relatives à la communication de documents par voie électronique et des méthodes qu'il convient le mieux d'appliquer pour préserver les données électroniques (Veuillez consulter l'annexe 1, Les sources documentaires, 5b)).

La suppression

La suppression des documents doit être faite de manière conforme aux obligations pertinentes sur la conservation de documents.

Il existe diverses façons de supprimer des documents sur un ordinateur. Il faut s'assurer que la méthode choisie convienne au degré de sensibilité des renseignements qui figurent dans le document.

La fonction classique « supprimer » consiste à supprimer le fichier, puis à vider la corbeille ou le bac de recyclage de l'ordinateur. La suppression d'un fichier supprime le nom du fichier du répertoire et indique que l'espace qu'occupait le fichier sur le disque dur est un espace disponible qui peut être recouvert pour y stocker d'autres fichiers.

Après une suppression classique, le document ou autre fichier peut toutefois encore être récupéré sur le disque dur de l'ordinateur. Il peut s'écouler beaucoup de temps avant qu'un ordinateur n'écrase cet espace ainsi libéré sur la mémoire du disque dur. Une suppression classique n'empêche pas de récupérer le contenu d'un document ou autre

fichier. De plus, le contenu de fichiers supprimés peut être récupéré, même une fois le fichier écrasé.

Il faut avoir recours à d'autres mesures pour éliminer des données critiques sur un ordinateur et s'assurer que le contenu de celles-ci ne puisse être récupéré par quiconque, y compris le propriétaire subséquent de l'ordinateur ou la personne qui l'acquiert à la suite de son vol ou de sa perte. « Nettoyer », « purger » ou « broyer » de façon sécuritaire supprime tout ce qu'il y a sur un disque dur de manière à empêcher qu'il ne soit restauré. Le broyage prend plus de temps que la suppression ordinaire de fichier, mais le temps requis pour effectuer même un « nettoyage militaire » à fond a été considérablement réduit par des programmes intégrés en 2007.

Les logiciels de nettoyage de fichiers écrasent plusieurs fois le contenu du fichier avec de nouvelles données aléatoires (« informations parasites ») et enlèvent du répertoire de l'ordinateur les renseignements sur ce fichier. On peut trouver des exemples de ces programmes en faisant des recherches sur Internet, à partir de termes tels que « nettoyage de fichiers » ou « nettoyage de données ».

Certains fabricants d'ordinateurs et entreprises de recyclage offrent des programmes permettant de retourner les ordinateurs à des fins de recyclage. Plusieurs juridictions canadiennes ont adopté des mesures ou envisagent d'en adopter, afin de réduire les déchets électroniques à l'aide d'initiatives obligatoires ou volontaires sur les déchets électroniques. Lorsque l'on se départit d'un ordinateur qui contient des renseignements confidentiels (en vertu de l'une de ces mesures ou de toute autre mesure de recyclage), la façon la plus prudente de protéger les données du disque dur contre tout accès non autorisé est de broyer le disque dur au moyen d'un programme de nettoyage de fichiers.

Une autre possibilité consiste à détruire le support sur lequel sont conservés les renseignements confidentiels. Cette méthode est généralement considérée comme étant la plus sécuritaire pour s'assurer que ces données ne seront pas récupérées. En ce qui concerne les renseignements confidentiels qui ont été copiés sur des supports de stockage portatifs, tels que des DVD ou des disques compacts, il est possible d'utiliser des déchiqueteuses de disques compacts pour détruire de façon permanente le support matériel.

(Veuillez consulter l'annexe 1 : Les sources documentaires, 5b))

6. Les métadonnées

Aperçu

On peut décrire les métadonnées de manière simple comme des renseignements sur d'autres données. De nombreux programmes informatiques intègrent des renseignements à la sortie du programme au moment où celui-ci est créé, ouvert et enregistré.

Certaines métadonnées sont stockées dans le programme et font partie des données de sortie de celui-ci. Il peut s'agir de fichiers, d'images, de diapositives de présentation, de documents, de feuilles de calcul électroniques ou d'autres données. Aux fins de la présente partie, le terme « document » renvoie à ces différents types de données de sortie.

Bien qu'elles soient masquées en vue normale, les métadonnées peuvent être affichées ou consultées par d'autres personnes lorsque le document est diffusé par voie électronique. Les renseignements contenus dans les métadonnées peuvent comprendre ce qui suit :

- le nom de l'auteur du document, ses initiales, le nom du cabinet, le nom de l'ordinateur, ou le nom du serveur de réseau ou du disque dur où le document a été enregistré;
- la date de création du document;
- l'identité des autres auteurs;
- l'identité des réviseurs;
- les révisions apportées au document, y compris les insertions et les suppressions, le suivi des modifications et les commentaires ajoutés par les auteurs des révisions;
- le nombre de révisions;
- la date du dernier enregistrement, de la dernière édition et de la dernière impression;
- le nombre de fois que le document a été imprimé;
- la distribution du document;
- des renseignements au sujet de l'imprimante sur laquelle a été imprimé le document;
- des renseignements au sujet des modèles utilisés pour créer le document;
- les versions du document;
- le temps total consacré à l'édition;
- l'emplacement du fichier stocké (*p. ex.* C://bureau/nomduclient/numerodufichier);
et
- les signets et les styles personnalisés.

Les métadonnées figurant dans les documents électroniques peuvent être utiles durant les étapes de rédaction d'un document, en facilitant la collaboration au moyen de l'ajout de commentaires, du suivi des révisions et de l'enregistrement de renseignements sur les versions du document. Les métadonnées peuvent cependant entraîner des problèmes lorsque le document est diffusé par voie électronique à d'autres, par exemple lors de la transmission d'un document par voie électronique au tribunal, lors de la transmission à l'avocat de la partie adverse d'un projet au cours de négociations ou encore lors de la diffusion de documents aux parties adverses. Les métadonnées du document peuvent contenir des renseignements masqués que l'auteur du document ne veut pas partager avec les destinataires, tels que les commentaires formulés à l'égard de révisions ou l'heure à laquelle ces commentaires ont été faits et l'identité de leur auteur.

Si l'on ne prend aucune mesure afin de les éliminer, les métadonnées feront partie du document, quel que soit le support utilisé pour diffuser le document – en tant que pièce jointe à un courriel, en le copiant sur une clé de mémoire, un DVD, un disque compact ou une disquette, ou encore en le téléchargeant sur un réseau ou sur l'extranet. Même s'ils ne sont pas visibles en vue normale, les renseignements intégrés sont facilement accessibles en langage clair en cliquant simplement sur le bouton droit de la souris pour visualiser les propriétés du document ou en utilisant un éditeur de texte.

Le quatrième commentaire sur la Règle IV prévoit qu'en règle générale l'avocat ne doit pas révéler qu'une personne l'a consulté ou a retenu ses services, à moins que la nature de l'affaire ne l'exige. Les métadonnées peuvent divulguer, par exemple, des renseignements confidentiels sur un client ou le fait que l'avocat a été consulté par celui-ci, et ainsi violer le secret professionnel.

Les pratiques exemplaires en matière de métadonnées

Lorsqu'ils transmettent des documents par voie électronique, la déontologie exige des avocats qu'ils fassent preuve d'une diligence raisonnable pour s'assurer que les renseignements confidentiels de leurs clients ne soient pas divulgués par les métadonnées.

Il existe des moyens permettant de réduire la création de métadonnées et de supprimer les données masquées avant leur diffusion ou leur publication, de façon à ce que ces renseignements ne puissent pas être consultés par d'autres personnes que leur destinataire. Avant de supprimer les métadonnées, les avocats doivent s'assurer qu'ils n'ont aucune obligation juridique de les conserver (*p. ex.* des obligations en matière de communication préalable).

L'« exploration » décrit les actions entreprises pour trouver et afficher les métadonnées masquées que le créateur ou l'expéditeur du document n'avait pas l'intention d'afficher. Les avocats voudront peut-être se prémunir contre l'exploration de métadonnées en négociant des accords de confidentialité ou en obtenant des ordonnances conservatoires visant à prévenir que les renseignements contenus dans les métadonnées puissent ensuite être utilisés par le destinataire contre l'expéditeur ou présentés en preuve dans le cadre d'un litige.

À l'annexe 2, Renseignements et sources documentaires concernant les métadonnées, vous trouverez des suggestions particulières pour vous aider à limiter la création de métadonnées et à supprimer celles-ci.

7. La sécurité

Aperçu

Lorsqu'ils utilisent des technologies de l'information, telles que les télécopieurs, les téléphones cellulaires, le courrier électronique et le courriel Web, ainsi que les appareils sans fil, pour communiquer au sujet d'un client ou avec celui-ci, les avocats doivent prendre les précautions nécessaires pour réduire le risque de divulgation par inadvertance ou l'interception des communications en question, ainsi que l'accès non autorisé aux renseignements.

La vulnérabilité en matière de sécurité informatique peut revêtir diverses formes :

- les « maliciels » – un terme qui désigne les logiciels malicieux et indésirables qui sont conçus pour pénétrer sans consentement dans un système informatique et pour endommager le matériel informatique, les logiciels ou les renseignements électroniques stockés sur l'ordinateur, et qui comprend les virus informatiques, les vers, les logiciels publicitaires, les logiciels espions et les chevaux de Troie);
- l'utilisation de technologies de communication sans fil qui risquent d'être interceptées si elles ne sont pas mises en place convenablement avec des mesures de sécurité telles que le cryptage;
- l'interception non autorisée et la copie de données; et
- la perte de données due au vol, la perte accidentelle, la défaillance, l'obsolescence, l'altération ou la dégradation des supports de stockage, les catastrophes ainsi que les pannes d'électricité et les surtensions.

Les pratiques exemplaires en matière de sécurité

La sécurité des communications et des renseignements confidentiels électroniques peut être accrue et le risque de perte des données et d'accès non autorisé aux communications et aux données peut être considérablement réduit en prenant des mesures telles que :

- l'exigence d'une authentification (*p. ex.* des mots de passe forts);
- le recours au cryptage;
- l'installation de coupe-feu et de logiciels de détection des intrusions;
- le recours à des logiciels antivirus;
- la mise en place de politiques précises destinées à ceux qui utilisent les ordinateurs pour assurer la sécurité et l'intégrité des données du cabinet sur Internet, sur les ordinateurs portatifs et sur les ordinateurs de bureau; et
- la sécurisation des réseaux sans fil.

(Veuillez consulter l'[annexe 3 : Mesures à prendre pour améliorer la sécurité des technologies de l'information](#))

8. La commercialisation

Le Code de déontologie de l'ABC : la commercialisation

La règle du chapitre XIV (Règle XIV) sur « La publicité, la sollicitation et la disponibilité des services » énonce ce qui suit :

Les avocats doivent veiller à ce que les services juridiques soient mis à la disposition du public de façon à susciter son respect et sa confiance, et ce, par des moyens compatibles avec l'intégrité, l'indépendance et l'efficacité de la profession.

Le troisième principe directeur de la Règle XIV prévoit que :

Bien que l'avocat ait un intérêt économique à gagner sa vie, la publicité doit être conforme aux règles prescrites par les ordres professionnels et à l'intérêt public et ne saurait déroger aux principes d'intégrité, d'indépendance ou d'efficacité de la profession juridique. La publicité ne doit pas induire en erreur la personne non informée ni faire naître des espoirs mal fondés et des attentes irréalistes. Elle ne doit pas nuire à la qualité des services juridiques ni être si inconvenante ou offensante qu'elle porterait préjudice à l'intérêt public et à la profession juridique.

Le septième principe directeur de la Règle XIV prévoit notamment ce qui suit :

Les avocats peuvent offrir leurs services professionnels à des clients éventuels par n'importe quel moyen, sauf si les moyens : (a) sont faux ou trompeurs [...] ou (e) jettent par ailleurs le discrédit sur la profession ou sur l'administration de la justice.

Les pratiques exemplaires en matière de commercialisation

La publicité qui utilise des technologies de l'information, telles que des sites Web, des gestionnaires de listes de diffusion, des blogues et des wikis, doit être conforme à ces principes.

Les avocats doivent être aussi soucieux de l'intégrité de leurs communications lorsqu'ils utilisent des technologies de l'information que lorsqu'ils ont recours à des moyens traditionnels de publicité, tels que des dépliants publicitaires imprimés, des annonces publicitaires télévisées ou des annuaires téléphoniques. Ils doivent se soumettre aux règles de leur ordre professionnel en ce qui concerne la publicité en ligne et au moyen d'autres technologies de l'information.

Ils doivent également se conformer aux lois applicables ainsi qu'aux règles et règlements de leur ordre professionnel sur les courriels commerciaux non sollicités.

Il existe des ressources disponibles en ligne qui permettent de s'assurer qu'un site Web fonctionne convenablement. Elles vérifient que les liens des sites Web n'ont pas été rompus et elles attestent que les balises HTML et XHTML de la page Web sont conformes aux normes du *Consortium World Wide Web*. Ces ressources en ligne sont disponibles en tapant dans le moteur de recherche des mots-clés tels que « compatibilité des navigateurs », « liens rompus », « conformité aux normes », « validation des liens », « validation HTML » ou « validation XHTML ».

(Veuillez consulter l'annexe 1 : Les sources documentaires, 5c.)

9. L'accessibilité

Le Code de déontologie de l'ABC : l'accessibilité

La règle du chapitre XX (Règle XX) sur la « Non-discrimination » prévoit que :

Sauf lorsqu'un traitement différent est autorisé par la loi, l'avocat ne doit pas exercer de discrimination [...] en se fondant, entre autres, sur les motifs que sont l'ascendance d'une personne, sa couleur, sa race perçue, sa nationalité, son origine nationale, son origine ou sa culture ethnique, sa langue, sa religion, ses croyances religieuses, son appartenance ou ses activités religieuses, son âge, son sexe, ses caractéristiques physiques, la grossesse, son orientation sexuelle, son statut matrimonial ou familial, ses sources de revenus, ses convictions, son appartenance ou ses activités politiques, ou sa déficience physique ou mentale.

Le premier commentaire sur la Règle XX, « Obligation de non-discrimination », souligne que :

1. La discrimination s'entend de toute distinction qui entraîne des conséquences disproportionnées et néfastes pour une personne ou un groupe spécifique et fondée sur les motifs énumérés dans la présente règle et qui n'a pas d'incidence sur d'autres personnes ou groupes. Cette obligation comprend notamment : (a) l'exigence que l'avocat ne puisse pas refuser ses services et donner des services de qualité inférieure pour l'un des motifs susmentionnés dans la règle...

Les pratiques exemplaires en matière d'accessibilité

Les technologies de l'information facilitent l'accès au droit et aux ressources juridiques en permettant d'accéder aux renseignements plus rapidement et à moindres frais et en favorisant ainsi l'accès à la justice. Le matériel, les logiciels et les technologies d'assistance, telles que les lecteurs d'écran, les écrans tactiles, les technologies de reconnaissance de la voix, les contrôles à un seul bouton ou les systèmes mains libres, peuvent considérablement renforcer l'accès à la justice pour les personnes atteintes d'une déficience. Toutefois, il est important que la technologie choisie ne dépasse pas la capacité du client de l'utiliser. Tous les clients ne disposent pas d'un système informatique doté d'une grande capacité de stockage et tous ne peuvent se permettre d'acheter la version la plus récente d'un logiciel.

De même, bien que la conception du site Web et les formats technologiques permettent aux gens d'accéder aux ressources, quelles que soient leurs aptitudes particulières physiques ou sensorielles, l'utilité des sites Web suppose que leur conception soit compatible avec les technologies d'assistance.

Les Directives pour l'accessibilité aux contenus Web (DACW) du *Consortium World Wide Web* (W3C) offrent des directives reconnues sur l'accessibilité aux sites Web. (Veuillez consulter l'annexe 1 : Les sources documentaires, 5d).

10. La prestation de service

Le Code de déontologie de l'ABC : la prestation de service

La prestation de services juridiques au moyen d'Internet peut violer les règles des ordres professionnels sur l'exercice illégal du droit. Veuillez consulter la règle énoncée au chapitre XVII du Code et les dispositions des ordres professionnels sur l'exercice de la profession par des personnes non autorisées.

Les pratiques exemplaires en matière de prestation de service

La vitesse et la nature globale d'Internet soulèvent un certain nombre de questions déontologiques. Les avocats doivent s'assurer que la prestation électronique de services juridiques soit conforme aux principes du Code sur les conflits d'intérêts et la confidentialité. Ils ne doivent pas donner l'impression qu'ils offrent leurs services dans une juridiction où ils ne sont pas autorisés à exercer.

En offrant leurs services au moyen de technologies de l'information, telles que des courriels ou la messagerie texte, les avocats doivent veiller à ce que les renseignements ne soient pas, par inadvertance, divulgués à ceux à qui ils n'étaient pas destinés. Les avocats doivent vérifier les adresses électroniques afin de s'assurer que seuls les récipiendaires à qui ces renseignements sont destinés reçoivent leurs communications.

Ils doivent redoubler de prudence et être certains de leur intention avant d'utiliser les fonctions suivantes :

- la fonction « répondre à tous » dans leurs courriels;
- la fonction de remplissage automatique dans les applications courriel; ou
- la fonction « répondre » avec un gestionnaire de liste de diffusion de groupe, ce qui pourrait avoir pour conséquence que la réponse soit envoyée à toutes les adresses électroniques inscrites sur la liste de diffusion des courriels de groupe.

11. La propriété intellectuelle et les logiciels

Exigences en matière de licences

Les logiciels sont généralement accompagnés d'un contrat de licence d'utilisation, qui mentionne les conditions d'utilisation de la propriété intellectuelle liée au logiciel et qui accorde l'autorisation d'utiliser celle-ci.

Les licences portent généralement sur les ententes suivantes :

- une licence propre à l'utilisateur qui restreint l'utilisation du logiciel à un seul utilisateur;
- une licence d'utilisation sur site qui autorise l'utilisation de la licence à un emplacement spécifique; et
- une licence de réseau qui autorise un nombre maximal d'utilisateurs à utiliser le logiciel en même temps.

La licence peut également prévoir une date à compter de laquelle l'acheteur n'a plus le droit d'utiliser le logiciel.

Les vendeurs peuvent fournir les conditions de la licence en les incluant dans la boîte accompagnant le logiciel (licence d'adhésion par déballage) ou en les présentant en ligne durant la procédure d'installation du logiciel (par clic ou par affichage sur le site Web).

Les logiciels libres sont également disponibles en vertu de diverses licences à source ouverte.

Les pratiques exemplaires en matière de propriété intellectuelle et de logiciels

Les avocats doivent lire avec soin les conditions liées aux licences d'utilisation des logiciels et se conformer à celles-ci. Les mesures à prendre à cet égard consistent à procéder à l'audit des logiciels à intervalles réguliers, à instaurer des politiques concernant les logiciels, à tenir un journal d'exploitation et à apprendre aux avocats et au personnel à se conformer aux conditions d'utilisation des logiciels.

(Veuillez consulter l'annexe 1 : Les sources documentaires, 5e).

12. Les sources juridiques électroniques et la recherche documentaire

De plus en plus de sources électroniques de qualité et dignes de foi permettant de trouver des documents primaires et secondaires sont accessibles à partir des services de recherche sur Internet et dans les bases de données en ligne et sur CD- ROM. Un grand nombre de ces sources peuvent être consultées sans frais : c'est le cas notamment des documents sur les portails juridiques CanLII et LexUM ainsi que des bases de données de lois et de jurisprudence (Veuillez consulter l'annexe 1 : Les sources documentaires, 5f).

Internet permet d'avoir des renseignements dynamiques et mis à jour. Cependant, ce côté dynamique d'Internet peut aussi comporter des inconvénients. Les « liens périmés » ou les « liens rompus » renvoient à des situations courantes dans lesquelles les URL vont être modifiés, le site Web déplacé, le contenu modifié, le site Web reconçu, ou dans lesquelles le site Web ou la page Web a cessé d'exister ou encore dans lesquelles un URL est devenu inactif et ne mène plus l'utilisateur à une version courante de la page Web. En outre, les renseignements sur les sites Web, et plus particulièrement les sites qui mettent constamment à jour leur contenu, peuvent cesser d'être disponibles au même emplacement.

Les pratiques exemplaires en matière de recherche électronique juridique et d'extraction de documents

Si la loi requiert une copie officielle (p. ex. pour le dépôt d'un document auprès d'un tribunal), il est recommandé de vérifier au préalable l'état des renseignements disponibles en ligne (officiels ou non officiels) sur le site Web.

Il est généralement plus prudent d'enregistrer en format PDF les sites Web, y compris l'URL et la date d'accès, afin de conserver ces renseignements et de s'assurer ainsi que ces sources puissent être attribuées et citées correctement. Les sources documentaires en ligne, tout comme les autres sources qui sont citées dans les documents juridiques, doivent contenir des renseignements appropriés au sujet de leurs auteurs et pour permettre aux lecteurs de retrouver les références citées.

(Veuillez consulter l'annexe 1 : Les sources documentaires, 5f).

13. La participation aux discussions en ligne

Le Code de déontologie de l'ABC : les discussions en ligne

La règle au chapitre XVIII (Règle XVIII) prévoit que :

L'avocat qui paraît en public ou qui fait des déclarations publiques doit, ce faisant, se conformer aux principes du Code.

La participation aux discussions en ligne constitue un type d'apparition publique qui peut contribuer largement à la vulgarisation du droit à l'égard du public (règle du chapitre XV et commentaires 7 à 9 et 11 à 13 sur la Règle XVIII).

Dans le même temps, la participation aux forums en ligne peut entraîner des problèmes en ce qui concerne :

- le devoir de confidentialité envers le client (règle du chapitre IV);
- la formation involontaire de rapports avec des clients (voir la définition de « client » à l'article « Interprétation » du Code; la règle du chapitre III, « La consultation »); et
- les conflits d'intérêts (règles des chapitres V et VI; sixième commentaire sur la règle du chapitre VI).

La règle du chapitre VII du Code sur l'« Incompatibilité de fonctions » (Règle VII) prévoit que :

L'avocat qui, en même temps qu'il pratique le droit, exerce une autre profession, fait des affaires ou occupe un emploi ne doit jamais laisser ces fonctions externes compromettre son intégrité, son indépendance ou sa compétence professionnelle.

Les pratiques exemplaires en matière de discussions en ligne

Internet offre aux avocats beaucoup d'occasions de communiquer avec d'autres avocats ainsi qu'avec des non-avocats au Canada et à l'échelle mondiale. La participation aux discussions en ligne peut prendre la forme d'articles et de commentaires sur les blogues, les wikis, les forums de clavardage, les forums sur Internet, listes de diffusion, les réseaux sociaux en ligne et autres forums et médias électroniques. Les communications d'avocats au moyen de forums publics en ligne constituent des déclarations publiques qui doivent être conformes au Code.

Les avocats qui participent aux forums en ligne doivent s'assurer d'expliquer clairement lorsqu'ils y participent en qualité d'avocat et lorsqu'ils y donnent des conseils de nature juridique. Dans un tel cas, ils doivent fournir leurs coordonnées et s'assurer d'être en mesure d'identifier les personnes avec qui ils communiquent. Les pièges à conflit d'intérêt foisonnent dans le cyberspace. En outre, toute déclaration concernant les affaires du client doit servir l'intérêt supérieur du client et rester dans les limites des services demandés (deuxième commentaire sur la Règle XVIII).

Les avocats qui participent à des discussions en ligne doivent veiller à éviter de compromettre leur intégrité, leur indépendance ou leur compétence professionnelle (veuillez consulter la Règle VII, « Incompatibilité de fonctions »).

Les avocats doivent faire preuve de courtoisie et de civilité et agir de bonne foi envers toute personne avec qui ils ont des rapports au cours d'une instance ou d'une procédure. Cette règle s'applique à leurs communications dans le cadre de discussions en ligne (seizième commentaire, « Courtoisie », sur la règle du chapitre IX).

Lorsqu'ils communiquent en ligne, les avocats doivent encourager et promouvoir le respect du public envers l'administration de la justice (règle du chapitre XIII). Leurs critiques et leurs propositions pour tenter d'améliorer le système juridique doivent être empreintes de bonne foi et de raison (deuxième principe directeur de la Règle XIII).

Le troisième commentaire sur la Règle XIII souligne que « dans sa carrière publique, l'avocat doit se montrer particulièrement prudent à cet égard, car du seul fait qu'il soit avocat, on aura tendance à donner de l'importance et à porter foi à ses déclarations ».

Les avocats doivent veiller à ce que leur participation à des discussions en ligne soit empreinte du même respect envers l'administration de la justice que les déclarations publiques qu'ils font dans d'autres tribunes et au moyen d'autres médias.

Les déclarations publiques dans les forums en ligne doivent être conformes à la règle du chapitre XIV sur la publicité, la sollicitation et la disponibilité des services.

Annexe 1: Les sources documentaires

1. Renseignements d'ordre général

M. Drew Jackson et Timothy L. Taylor, *The Internet Handbook for Canadian Lawyers*, 3d. ed. (Carswell, 2000).

Carole A. Levitt et Mark E. Rosch, *The Lawyer's Guide To Fact Finding On The Internet*, 2d ed. (American Bar Association, 2004)

Barry Sookman, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions* (Toronto: Carswell, 2006)

Index d'extensions de fichiers (*p. ex.* définition des formats PDF, DOC, WPD) :
<<http://www.fileinfo.net/common.php>>.

TechnoLawyer: <http://www.technolawyer.com>

2. Les sources documentaires pour effectuer des recherches juridiques en ligne sur le droit canadien

Institut canadien d'information juridique (CanLII) : <www.canlii.ca>.

LexUM : <http://www.lexum.umontreal.ca/index.epl?lang=fr>

3. La déontologie juridique et les nouvelles technologies de l'information

(i) Les « Lignes directrices sur la déontologie et la nouvelle technologie »

Fédération des ordres professionnels de juristes du Canada, « Lignes directrices sur la déontologie et la nouvelle technologie » Équipe de travail nationale sur la déontologie du Comité national sur la technologie, Fédération des ordres professionnels de juristes du Canada (1999)

Law Society of Alberta, « Ethics and New Technology Guidelines » (modifiées), <<http://www.lawsocietyalberta.com/lawyerservices/FromTheAdvisor/FromPracticeadvisor2/ethicsandtechnology.cfm#1>>.

Law Society of British Columbia, « Guidelines on Ethics and the New Technology » (modifiées), <http://www.lawsociety.bc.ca/practice_support/articles/FedGuidelines.html>

Law Society of Newfoundland and Labrador, « Guidelines on Ethics and the New Technology » (modifiées et jointes à l'Annexe A du Code de Terre-Neuve-et-Labrador), <http://www.lawsociety.nf.ca/code/code_schedulea.asp>.

Barreau du Nouveau-Brunswick, « Lignes directrices sur la déontologie et la nouvelle technologie » (jointes en annexe au Code du Nouveau-Brunswick), <http://lawsociety-barreau.nb.ca/assets/documents/Code_de_deontologie_mars_2006.pdf>.

Barreau du Haut-Canada, « Guidelines on Ethics and the New Technology » (modifiées), <http://www.lsuc.on.ca/media/tech_guidelines.pdf>.

Nova Scotia Barristers' Society, « Guidelines on Ethics and the New Technology », <http://www.nsbs.ns.ca/publications/techno_ethics_guidelines.pdf>.

Manitoba, « Guidelines on Ethics and the New Technology » (modifiées), <http://www.lawsociety.mb.ca/pubdocs/ethics_newtech.pdf>.

Saskatchewan, « Guidelines on Ethics and New Technology » (jointes en annexe au Code of Professional Conduct) : <www.lawsociety.sk.ca/newlook/Publications/EthicsTech.pdf>.

(ii) Autres

Barreau du Haut-Canada, « Ligne directrice en matière de technologies » (modifiée), <http://rc.lsuc.on.ca/pdf/pmg/pmg_tech_fr.pdf>.

ABA, « Ethics and Technology 2006: How NOT to Commit Malpractice With Your Computer », ABA, Law Practice Management Section, Center for Professional Responsibility, Standing Committee on Lawyers' Professional Liability, et le ABA Center for Continuing Legal Education

Legal Ethics, <www.legaethics.com> (site Web renfermant des sources documentaires sur des questions déontologiques, dont la déontologie et les technologies de l'information, qui concernent essentiellement le droit américain)

4. Les sources relatives aux technologies de l'information

Consortium World Wide Web (W3C): <<http://www.w3.org/>>.

Secrétariat du Conseil du Trésor, Direction du dirigeant principal de l'information, gouvernement du Canada : <<http://www.tbs-sct.gc.ca/cio-dpi/index-fra.asp>>.

LawPRO (Assurance de la responsabilité civile professionnelle des avocats (Canada)), « Resources @ Technology Associations », sources documentaires en technologie de LawPRO's practice Pro : <<http://www.practicepro.ca/information/tassocs.asp>>.

LawPro Links : An A-Z Directory of Web Resources (basée au États-Unis; non affiliée à l'Assurance de la responsabilité civile professionnelle des avocats (Canada)) : <<http://www.llrx.com/llrxlink.htm>>.

Slaw.ca, blogue coopératif sur la recherche juridique canadienne et les TI : <<http://www.slaw.ca/>>.

5. Les sources documentaires sur des sujets particuliers

(a) Introduction

Association du Barreau canadien, Code de déontologie :
<<http://www.cba.org/abc/activities%5Ff/code/>>

(b) Le stockage, la conservation et l'archivage électroniques

Commissaire à l'information et à la protection de la vie privée de l'Alberta, Investigation Report P2006-IR-005 (septembre 2006), en ligne :
<<http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf>>

Portail canadien d'administration de la preuve électronique (LexUM) :
<http://www.lexum.umontreal.ca/e-discovery/index_fr.html>.

Guidelines for the Discovery of Electronic Documents in Ontario :
<http://www.oba.org/en/pdf_newsletter/E-DiscoveryGuidelines.pdf>.

Discovery Task Force E-Discovery Guidelines and Resource page, Association du Barreau de l'Ontario : <http://www.oba.org/en/main/ediscovery_en/default.aspx>.

Commissaire à l'information et à la protection de la vie privée/Ontario, ordonnance HO-004 (mars 2007), en ligne :
<http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf>

Sedona Canada Principles: Addressing Electronic Document Production (ébauche de février 2007 fondée sur les commentaires du public) :
<http://www.lexum.umontreal.ca/e-discovery/2_07WG7pubcomment.pdf>
(divulgaration de renseignements stockés par voie électronique dans le cadre de litiges civils canadiens)

Les Sedona Canada Principles : La Production des Documents Électroniques (Mai 2007, version publique pour commentaires) : <http://www.lexum.umontreal.ca/e-discovery/5_07SedonaCanadaFrancais.pdf>.

The Sedona Conference Glossary for E-Discovery and Digital Information Management (version de janvier 2008) :
http://www.thesedonaconference.org/content/miscFiles/canada_pincpls_FINAL_108.pdf

Practice PRO, « Electronic Discovery: A Reading List »,
<http://www.practicepro.ca/practice/eDiscovery_Rlist.asp>.

E-discovery Amendments and Committee Notes, United States Federal Rules of Civil Procedure (en vigueur à compter de décembre 2006) :
<http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf>.

Ann Macaulay, « How to Make Your Office (Almost) Paperless », <<http://www.cba.org/cba/PracticeLink/TAYP/paperless.aspx>>.

(c) La commercialisation

Service de validation des fichiers HTML et XHTML du W3C (Consortium World Wide Web) : <<http://validator.w3.org/>>.

(d) L'accessibilité

Conseil du Trésor du Canada, « NSI—Accessibilité » (2004) : <<http://www.tbs-sct.gc.ca/clf-nsi/inter/inter-01-00-fra.asp>>.

Consortium World Wide Web (W3C), « Web Content Accessibility Guidelines (WCAG) » : <<http://www.w3.org/TR/WAI-WEBCONTENT/>>.

Renseignements fournis par Adobe pour améliorer l'accès en ligne; son guide pour rendre les documents en format PDF accessibles à ceux qui souffrent de handicaps visuels, auditifs, de difficultés d'apprentissage, de déficience motrice ou de troubles de dextérité; offre également des directives pour permettre aux lecteurs d'écran d'avoir accès aux documents en format PDF : <www.adobe.com/accessibility/>.

Service de conversion d'Adobe (où l'adresse URL d'un document de format PDF peut être envoyée à Adobe et Adobe en renvoie le contenu en HTML ou en texte en clair pour logiciels de conversion vocale) : <http://www.adobe.com/products/acrobat/access_onlinetools.html>.

D'autres sources documentaires sur l'accessibilité à la technologie de l'information peuvent être trouvées à l'aide d'un engin de recherche en se servant de mots-clés tels que « accès à la page Web », « accès HTML », « compatibilité des navigateurs », « WCAG » ou « article 508 » (norme d'accessibilité aux États-Unis).

(e) La propriété intellectuelle et les logiciels

Des listes de logiciels libres pour application bureautique courants sont disponibles à :

<<http://www.webi.org/>> et <http://en.wikipedia.org/wiki/List_of_open_source_software_packages>.

(f) Sources juridiques électroniques et recherche documentaire

CanLII : < <http://www.canlii.ca/> >

LexUM : < <http://www.lexum.umontreal.ca/> >

Ministère de la Justice (Canada) : < <http://laws.justice.gc.ca/fr> >

Cours d'appel :

Cour suprême du Canada : <http://www.scc-csc.gc.ca/ef-de/gl-ld-fra.asp>

< <http://scc.lexum.umontreal.ca/fr/index.html> > (jugements)

Alberta : < <http://www.albertacourts.ab.ca> >

Colombie-Britannique : < <http://www.courts.gov.bc.ca/ca> >

Manitoba : < <http://www.manitobacourts.mb.ca/index.fr.html> / >;

< <http://www.canlii.org/en/mb/mbca/index.html> > (jugements)

Nouveau-Brunswick : < <http://www.gnb.ca/cour/03COA1/index-f.asp> >;

< <http://www.canlii.org/fr/nb/nbca/index.html> > (jugements)

Terre-Neuve : < <http://www.justice.gov.nl.ca/just/lawcourt/appeal.htm> >;

< <http://www.canlii.org/nl/cas/nlca> > (jugements)

Nouvelle-Écosse : < www.courts.ns.ca/Appeals/index_ca.htm >

Ontario : < <http://www.ontariocourts.on.ca/coa/fr/index.htm> >

Île-du-Prince-Édouard : < <http://www.gov.pe.ca/courts/supreme/index.php3> >;

< <http://www.canlii.org/fr/pe/pescad/index.html> > (jugements)

Québec : < <http://www.tribunaux.qc.ca/c-appel/index-ca.html> >

Saskatchewan : < <http://www.lawsociety.sk.ca/newlook/Library/database.htm> > (jugements)

Nunavut : < <http://www.nucj.ca/index.htm> >;

< <http://www.canlii.org/fr/nu/nuca/index.html> > (jugements)

Territoires du Nord-Ouest : < www.justice.gov.nt.ca/dbtw-wpd/nwtjqbe.htm >

Yukon : < <http://www.yukoncourts.ca/courts/appeal.html> >

Cour d'appel fédérale : < <http://decisions.fca-caf.gc.ca/fr/index.html> >

États-Unis :

Portail du gouvernement américain : < <http://www.usa.gov/> >

LII : Legal Information Institute (Cornell)

< www.law.cornell.edu/ >

Union européenne :

< <http://eur-lex.europa.eu/fr/index.htm> > (Français)

< <http://eur-lex.europa.eu/en/index.htm> > (Anglais)

World Legal Information Institutes :

< <http://www.worldlii.org/> >

Annexe 2 : Renseignements et sources documentaires sur les métadonnées

1. Les sources documentaires

Electronic Frontier Foundation, « List of Printers Which Do or Do Not Display Tracking Dots » < <http://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots> >

Electronic Frontier Foundation, « Harry Potter and the Digital Footprints » < <http://www.eff.org/deeplinks/2007/07/harry-potter-and-digital-fingerprints> >.

2. Les pratiques de rédaction qui créent ou transfèrent des métadonnées

Les pratiques de rédaction courantes peuvent créer ou contenir des métadonnées. L'utilisation de la fonction « enregistrer sous » avec un document existant peut transférer les métadonnées liées au document original. Des outils collaboratifs, tels que les commentaires et les suivis de modifications, créent des métadonnées sur les réviseurs, les auteurs, les versions précédentes, les révisions, la mise en page et les renseignements qui ont été supprimés. L'inclusion de l'emplacement du fichier (spécialement lorsqu'il s'agit de renseignements sur le client) en en-tête ou en pied de page peut révéler par inadvertance plus de renseignements que ce qui est souhaité (*p. ex.* une relation avocat-client) si le document est par la suite distribué à d'autres.

3. La réduction et la suppression des métadonnées

Les créateurs de documents peuvent prendre les mesures suivantes :

- a) réduire autant que possible la création de métadonnées;
- b) supprimer les métadonnées afin de produire une copie « propre » du document.

a. La réduction de la production de métadonnées

On peut réduire la production de métadonnées en se conformant aux pratiques suivantes :

- i. amorcer la rédaction d'un document en utilisant un modèle qui ne comporte qu'un minimum de renseignements (sans lien avec un client particulier). Par contre, lorsque des documents sont « réutilisés » et qu'on les enregistre sous un nouveau nom, il y a un risque que les métadonnées du document original soient transférées au document « réutilisé »;
- ii. accepter les suivis de modifications avant que les documents ne soient distribués. Le seul fait de passer à un mode de visualisation qui ne montre pas le suivi des modifications (*p. ex.*, en passant de « Final » à « Final avec marques »), n'a pas pour effet de supprimer ces renseignements. Pour les supprimer, il faut sélectionner « Accepter tout ». Quant aux documents où il n'est pas nécessaire d'activer les fonctions collaboratives de suivi des

modifications et de commentaires, il serait préférable de désactiver au préalable ces fonctions afin d'éviter de créer des métadonnées; ou

- iii. ne pas autoriser d'enregistrements rapides. Cette fonction peut être désactivée dans Microsoft Word, PowerPoint et Excel en cliquant sur Outils>Options>onglet Enregistrement et en décochant la case « Autoriser les enregistrements rapides »

b. La gestion et la suppression des métadonnées

Les métadonnées des documents peuvent être gérées, réduites et supprimées de la manière suivante :

- i. en utilisant des fonctions intégrées au programme qui permettent d'afficher et de supprimer les renseignements signalétiques masqués;
- ii. en installant les logiciels compagnons du fournisseur de programme (*p. ex.* Microsoft, Adobe, Corel); ou
- iii. en utilisant des programmes de fournisseurs indépendants.

Les programmes pourvus de fonctions pour gérer la création et la suppression de métadonnées et la production de copies « propres » de documents sont souvent appelés « programmes de nettoyage des métadonnées », « outils de suppression des métadonnées » ou « logiciels de gestion des métadonnées ». Ces programmes peuvent être utilisés pour empêcher que des renseignements critiques ne soient divulgués par inadvertance.

(i) L'utilisation des fonctions intégrées au programme

Il nous est impossible de passer en revue toutes les applications et tous les programmes utilisés dans les cabinets d'avocats, mais les recommandations qui suivent montrent comment accéder aux fonctions internes des programmes les plus couramment utilisés.

Microsoft Office Word 2003 ou Word XP

Dans Microsoft Office Word 2003 ou Word XP, en cliquant sur Ouvrir>Fichier>Propriétés>, on peut obtenir les métadonnées d'un document. Les onglets de la boîte de dialogue Général, Résumé et Statistiques fournissent des renseignements sur le document. Pour supprimer ces métadonnées d'identification pour un document créé dans Word 2002 ou Word 2003, cliquez sur Outils>Options>Sécurité et cochez la case Supprimer les informations personnelles de ce fichier lors de l'enregistrement (Word 2002) ou Supprimer les informations personnelles des propriétés de ce fichier lors de l'enregistrement (Word 2003), puis cliquez sur OK.

Cet onglet Sécurité offre également des options qui peuvent être utilisées pour émettre un avertissement avant d'imprimer, d'enregistrer ou d'envoyer un fichier qui contient des suivis de modifications ou des commentaires; cet onglet permet également de faire

apparaître les balises masquées lorsqu'on ouvre ou lorsqu'on enregistre le document. Cette fonction souligne la présence de métadonnées dans un document, mais ne les supprime pas.

Pour créer une copie « propre » d'un document, copiez le document dans un fichier net en cliquant sur Édition>Sélectionner tout (Ctrl + A), puis copiez le document (Ctrl + C), ouvrez un nouveau document (Ctrl + N), collez-y le contenu du document (Ctrl + V) et enregistrez ce document sous un nouveau nom à l'aide de la fonction « Enregistrer sous ». Afin d'obtenir une copie nette du nouveau document, il faut recourir à la fonction « Enregistrer sous ». Renommer un document préexistant à l'aide de la fonction « Enregistrer sous » (c.-à-d. ouvrir un nouveau document et s'en servir comme modèle électronique pour un nouveau document) a pour effet de transférer les métadonnées du document original.

PowerPoint 2002

Dans PowerPoint 2002, les métadonnées peuvent être supprimées en cliquant sur Fichier>Enregistrer sous>Outils> options Sécurité >, puis en cochant « Supprimer les informations personnelles de ce fichier lors de l'enregistrement » dans la case à cocher et en cliquant enfin sur OK. Pour de l'information additionnelle, veuillez consulter la Base de connaissances de Microsoft, « Comment réduire les métadonnées dans des présentations PowerPoint 2002 ».

Microsoft Excel

Pour Microsoft Excel, veuillez consulter la Base de connaissances de Microsoft, « Comment faire pour minimiser la quantité de métadonnées dans les classeurs Microsoft Excel ».

En outre, la fonction Gestion des droits relatifs à l'information (IRM) dans Office 2003 peut être réglée de façon à réduire les métadonnées.

WordPerfect

Pour visualiser les métadonnées d'un document créé dans WordPerfect, cliquez sur Fichier>Propriétés pour les statistiques sommaires. On peut consulter l'historique des révisions en cliquant sur Édition>Annuler/Refaire. L'option historique des révisions peut être désactivée en décochant la case « Enregistrer actions Annuler/Refaire avec le document » dans la boîte Édition/Annuler/Refaire/Options. Corel offre un programme pour les documents WordPerfect Office X3 sous Fichier>Enregistrer sans métadonnées. Vous pourrez trouver des renseignements supplémentaires dans la Base de connaissances de Corel, <http://support.corel.com/scripts/rightnow.cfg/php.exe/enduser/std_alp.php>, n^{os} de réponses 753605 et 759035.

Le format de document portable d'Adobe

Le format de document portable d'Adobe (communément appelé format « PDF ») contient habituellement moins de métadonnées que les applications de Microsoft Office et autres logiciels de productivité bureautique, mais il peut encore y avoir des métadonnées dans un document de format PDF. Les métadonnées peuvent être intégrées à un document de format PDF au moyen des fonctions mêmes d'Acrobat (telles les « notes récurrentes »); cette intégration peut être également due au fait que ces

renseignements existaient dans un document antérieur, créé dans un autre programme (*p. ex.* WordPerfect ou Word) avant la conversion du document en format PDF, et les métadonnées de ce programme ont alors été transférées au document de format PDF. Les métadonnées dans les documents de format PDF peuvent prendre la forme de mots-clés, d'annotations, de commentaires ou d'informations sur les champs.

Pour obtenir un sommaire des métadonnées dans un document de format PDF, cliquez sur Fichier>Propriétés du document.

Pour le réglage des options de sécurité, cochez les cases de préférences dans la boîte de dialogue qui apparaît.

Acrobat 8 comprend une fonction de suppression des métadonnées appelée Examiner le document, accessible en cliquant sur Document> Examiner le document>, puis en cliquant ensuite sur les renseignements à supprimer (métadonnées, texte masqué, annotations, commentaires et signets) et enfin en cliquant sur Supprimer tous les éléments sélectionnés. Les métadonnées sont utilisées dans les documents de format PDF pour retracer les numéros Bates, et la suppression des métadonnées aura une incidence sur le fonctionnement des fonctions reliées aux numéros Bates.

(ii) L'installation des logiciels compagnons du fournisseur de programme

Word, PowerPoint et Excel

À titre d'exemple de logiciel compagnon d'un fournisseur de programme, soulignons le logiciel gratuit de Microsoft « Remove Hidden Data » qui sert à supprimer de façon permanente les données masquées et les données de collaboration dans les versions 2003 et XP de Word, PowerPoint et Excel. Ce logiciel compagnon peut être téléchargé et installé à partir de :

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&displaylang=fr>>.

Cet outil peut être utilisé pour créer une copie « propre » du document avant que celui-ci ne soit distribué ou rendu public, tout en permettant d'activer des fonctions de collaboration tels les commentaires et les suivis de modifications pendant la rédaction du document. À partir d'un document ouvert, cliquez sur Fichier>Supprimer les données cachées>, et quand apparaît la boîte de dialogue, inscrivez le nom de la nouvelle version propre et cliquez sur suivant. Une fois le processus terminé, le journal des résultats apparaîtra.

La fonction « Supprimer les données cachées » est incluse dans la suite Office 2007.

(iii) L'utilisation de programmes de fournisseurs indépendants

À titre d'exemples de programmes de suppression des métadonnées de fournisseurs indépendants pour purger les données de sortie dans des logiciels tels que ceux de Microsoft et d'Adobe, mentionnons les programmes suivants :

- Payne Metadata Assistant <http://www.payneconsulting.com/products/>;
- Workshare Protect <http://www.workshare.com/products/>;
- Doc Scrubber < www.docscrubber.com >;
- Out-of-Sight de Softwise Consulting www.softwise.net/frameSet.html; et
- iScrub <http://esqinc.com//index.php?p=products&id=2>.

OpenDoc

Des programmes pour purger les métadonnées sont également disponibles pour la suite bureautique du logiciel libre OpenDoc, tels que le produit 3BClean de 3BView, <www.3bview.com/3bclean.html>.

Nombre de ces programmes de fournisseurs indépendants réussissent mieux à calibrer les options de personnalisation que les versions des logiciels des fabricants. Ainsi, ils peuvent comprendre des options qui maintiennent certaines métadonnées permettant au créateur du document de tirer profit de fonctions qui dépendent de ces renseignements et de mettre en place des paramètres de distribution qui fonctionnent avec d'autres programmes, tels Outlook ou Notes, et qui empêcheront que le document ne soit distribué à l'externe. Il existe dans certains programmes une fonction permettant de supprimer automatiquement les métadonnées des pièces jointes aux courriels avant que ceux-ci ne soient envoyés.

4. Références et sources documentaires au sujet des métadonnées

David Hricik, « Mining for Metadata: Is it Ethical to Take Intentional Advantage of Other People's Failures? » (33^e Convention nationale sur la responsabilité professionnelle, tenue à l'hôtel Fairmont Chicago, le 2 juin 2007), (Aspen Publishers, 2007) 1.

Commissariat à la protection de la vie privée au Canada, « Les risques associés aux métadonnées » <http://www.privcom.gc.ca/fs-fi/02_05_d_30_f.asp>.

American Bar Association, Standing Committee on Ethics and Professional Responsibility, « Review and Use of Metadata » Formal Opinion 06-442, 5 août 2006.

Microsoft, Base de connaissances, « Comment faire pour minimiser la quantité de métadonnées dans les classeurs Microsoft Excel » <<http://support.microsoft.com/kb/223789/fr/>>.

Microsoft, Base de connaissances, « Comment réduire les métadonnées dans les documents Office », article n° 22396, < <http://support.microsoft.com/kb/223396/fr> >.

Microsoft, Base de connaissances, « Comment réduire les métadonnées dans des présentations PowerPoint 2002 », < <http://support.microsoft.com/kb/314800>>.

Microsoft, Base de connaissances, « Outil de suppression des métadonnées de Microsoft Office 2003 et Office XP », article 834427, < <http://support.microsoft.com/kb/834427>>.

Microsoft, Base de connaissances, « Control metadata in your legal documents », < <http://office.microsoft.com/en-us/help/HA011400341033.aspx>>.

Corel, Base de connaissances, « How Can I Remove Metadata From WordPerfect Documents », réponse n° 753605; et « How Do I Remove Metadata From a WordPerfect Document », réponse n° 759035; disponibles à l'aide d'un moteur de recherche à : < http://support.corel.com/scripts/rightnow.cfg/php.exe/enduser/std_alp.php >.

United States National Security Agency, « Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF », < <http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf> >.

Dan Pinnington, « Beware the Dangers of Metadata », *LawPRO Magazine* (juin 2004), disponible à l'adresse suivante : < www.lawpro.ca/magazinearchives>.

« e-Discovery », numéro de septembre 2005 de *LawPRO Magazine* : < http://www.lawpro.ca/lawpro/LawPROmagazine4_2_Sep2005.pdf>.

Annexe 3 : Mesures à prendre pour améliorer la sécurité des technologies de l'information

1. Les copies de secours

Pour se prémunir contre des pertes de données dues au vol, aux pannes d'électricité, à la surtension, aux catastrophes, ou aux dommages que peuvent subir le matériel informatique et les logiciels, il est important de faire des copies de secours des données à intervalles réguliers et de stocker celles-ci en toute sécurité dans un emplacement situé à l'extérieur du cabinet (veuillez consulter également à ce sujet l'article 6 des Lignes directrices).

2. Les restrictions d'accès et les protocoles d'authentification

Les restrictions d'accès servent à restreindre l'accès à un ordinateur ou à un réseau aux utilisateurs autorisés. Les protocoles les plus couramment utilisés pour les restrictions d'accès sont les mots de passe et, de plus en plus, les cartes à puces et les systèmes biométriques.

Les mots de passe utilisés doivent être faciles à se rappeler (sans avoir à les écrire sur papier), difficiles à deviner et ils doivent être fréquemment modifiés. Un mot de passe fort est celui qui ne peut être facilement deviné par une autre personne, ni facilement établi par un ordinateur.

Un mot de passe devrait être un ensemble de caractères alphanumériques, de lettres minuscules et majuscules, de symboles, de caractères créés avec les touches « alt » ou « ctrl » et une autre touche du clavier, et devrait compter au moins huit caractères. Un mot de passe ne devrait pas être composé d'un mot du dictionnaire (dans quelque langue que ce soit), d'un mot du dictionnaire épelé à l'envers, ou d'un mot du dictionnaire avec des chiffres uniquement au début ou à la fin du mot. De tels mots de passe sont particulièrement vulnérables aux « attaques de dictionnaires » de la part de pirates informatiques. Il ne faut pas choisir un mot de passe qui remplace des lettres par des chiffres dans un mot du dictionnaire (par exemple, le chiffre un au lieu de la lettre « l »), des séquences (telles que des chiffres en ordre chronologique ou une série de caractères qui se suivent sur un clavier), des caractères répétés (« aaa »), des noms d'utilisateurs et le mot de passe par défaut fourni par le système.

En outre, les mots de passe ne devraient pas être composés d'un nom personnel, d'un membre de la famille, du nom d'un animal de compagnie, ou encore de renseignements biographiques, tels que les dates d'anniversaires, les adresses ou les numéros de téléphone.

Il est recommandable d'exiger un mot de passe :

- lors du démarrage de l'ordinateur;
- lors du retour au travail une fois que l'ordinateur a été mis en attente (« en veille ») ou que l'économiseur d'écran a été activé;

- lors du lancement d'une application; et
- lors de l'ouverture d'un fichier.

3. Le cryptage

Le cryptage empêche que les communications ne soient lues par ceux à qui elles ne sont pas destinées.

Il y a diverses méthodes de cryptage, mais le « cryptage à clé publique » est une méthode courante et efficace de cryptage. OpenPGP est la norme de cryptage pour courriel la plus répandue. Les programmes GnuPG et PGP sont conformes à cette norme.

Parmi les programmes courants comportant des fonctions de cryptage de fichiers et de cryptage de disque dur en entier qui permettent de protéger les renseignements stockés sur un ordinateur portable, mentionnons les programmes suivants :

- SafeGuard Easy <http://americas.utimaco.com/>;
- PGP Personal 8.0 <http://www.pgp.com>;
- SecureDoc <http://www.winmagic.com>; et
- PointSec for PC <http://www.checkpoint.com/pointsec/>.

Quant aux programmes couramment utilisés pour protéger les renseignements stockés sur des dispositifs informatiques portatifs (*p. ex.* les assistants personnels, les téléphones intelligents et le courriel « poussé » sans fil) et sur les supports amovibles, on peut mentionner les programmes suivants :

- SafeGuardPDA et Safeguard PushMail <http://americas.utimaco.com/>;
- TealLock <http://www.tealpoint.com/softlock.htm>;
- PointSec Mobile
<http://www.checkpoint.com/products/datasecurity/mobile/index.html>; et
- Smartphone Security
http://www.trustedigital.com/products/smartphone_sec_client.asp.

4. Les coupe-feu et les logiciels de détection d'intrusion

La technologie du coupe-feu est un dispositif de logiciel ou de matériel informatique qui assure la sécurité d'un ordinateur ou d'un réseau d'ordinateurs en gérant l'entrée et la sortie de données au moyen d'un système de règles précises. Le Service Pack 2 pour Windows XP, par exemple, comprend le programme Windows Firewall, un programme qui contrôle le trafic entrant (mais non le trafic sortant).

5. Les logiciels antivirus et les suites logicielles de sécurité

Les « logiciels antivirus » devraient être utilisés pour détecter et supprimer les logiciels malveillants (*p. ex.* les virus informatiques, les logiciels espions, les logiciels publicitaires et les vers) sur un ordinateur ou un réseau d'ordinateurs. Vous pourrez trouver une liste des logiciels antivirus les plus connus, y compris les produits commerciaux, les logiciels libres et les logiciels à source ouverte en consultant l'adresse suivante :

http://en.wikipedia.org/wiki/List_of_antivirus_software.

Vous pouvez télécharger le logiciel *Malicious Software Removal Tool* de Microsoft à l'adresse suivante : <<http://www.microsoft.com/security/malwareremove/default.aspx>>.

Des logiciels antivirus « autonomes » sont proposés, mais ces logiciels sont habituellement inclus dans une suite logicielle qui offre une protection contre une vaste gamme de vulnérabilités liées à la sécurité informatique, tels les logiciels malveillants, l'intrusion non autorisée, le vol d'identité, l'hameçonnage, le courriel commercial non sollicité et les fenêtres contextuelles importunes sur Internet. Les suites logicielles de sécurité intègrent souvent des coupe-feu et d'autres fonctions liées à la sécurité, tel le balayage de courriels pour repérer les pièces jointes infectées et le filtrage d'URL.

On achète habituellement les logiciels antivirus et les programmes de sécurité informatique commerciaux à l'aide d'une licence d'utilisation de logiciel, qui consiste en un abonnement pour une période de temps limitée, lequel est renouvelable et donne droit aux mises à jour des logiciels transmis via Internet.

Voici les noms de quelques-uns des logiciels antivirus et suites logicielles de sécurité les plus populaires :

- Shield Deluxe de PC Security Shield :
<<http://www.pcsecurityshield.com/lp/shield-deluxe-4.aspx?trk=WTK&affid=650>>
- Trend Micro Internet Security :
<<http://us.trendmicro.com/us/products/personal/index.html>>
- ZoneAlarm Internet Security Suite de Check Point :
<http://www.checkpoint.com/products/za_iss/index.html>
- Total Protection, VirusScan Plus, et Internet Security Suite de McAfee :
<<http://www.mcafee.com/ca-fr/?langid=48>>
- Microsoft Windows Live OneCare : <<http://onecare.live.com/standard/fr-ca/default.htm>>
- Anti-Virus et Internet Security de Kaspersky : <<http://usa.kaspersky.com/>>

- Internet Security, Antivirus, et Total Security de BitDefender : <http://www.bitdefender.com/>
- Anti-Virus et Anti-Spyware de CA : <<http://www.ca.com/ca/fr/>>
- Internet Security de F-Secure : <<http://www.f-secure.com/estore/fsis2007.html>>
- Norton AntiVirus, Norton 360 et Norton Internet Security de Symantec : <<http://www.symantec.com/fr/ca/index.jsp>>.

6. Les politiques en matière de sécurité informatique pour les employés et le personnel

Des politiques de sécurité pour les employés et le personnel peuvent être mises en place relativement à l'utilisation d'Internet, des ordinateurs portatifs et des ordinateurs de bureau. Ces politiques peuvent notamment porter sur des questions telles que :

- l'utilisation appropriée de l'intranet et d'Internet;
- des restrictions sur le téléchargement, la visualisation et la dissémination du contenu discriminatoire ou importun (Règle XX);
- l'autorisation d'utiliser l'adresse électronique du cabinet juridique ou de l'entreprise;
- l'interdiction d'utiliser des supports de stockage portatifs (comme les clés USB) ou les ordinateurs portatifs pour transférer à l'extérieur du bureau des renseignements confidentiels non chiffrés, dû à l'extrême vulnérabilité de ces supports au vol et à la perte;
- les circonstances dans lesquelles des avertissements doivent être insérés dans les courriels au sujet du caractère confidentiel et protégé des renseignements; et
- les limites auxquelles sont soumis les employés et le personnel quant à l'ajout ou au téléchargement de logiciels sur les ordinateurs de réseau ou sur les ordinateurs individuels.

Il est important de mettre en œuvre des protocoles qui requièrent l'utilisation de mesures de protection technique strictes pour protéger les renseignements informatiques confidentiels et la mise à jour de ces mesures à des intervalles permettant d'assurer un degré suffisant de protection des renseignements confidentiels relatifs aux options de sécurité en vigueur.

7. La sécurité des renseignements personnels

Les renseignements personnels confidentiels doivent être convenablement protégés. Lorsqu'ils sont regroupés et stockés sur un seul emplacement de fichier, les renseignements personnels confidentiels sont plus vulnérables et plus sujets au risque de

vol d'identité. Les renseignements personnels confidentiels ne doivent pas être accessibles sur Internet.

Les mesures qui doivent être prises pour protéger les renseignements personnels confidentiels stockés dans les ordinateurs comprennent notamment :

- des mesures techniques rigoureuses, telles que le cryptage et les autres formes de contrôle de l'accès;
- des mesures matérielles, telles que des serrures, des câbles, des logiciels de suivi pour ordinateurs portatifs et des alertes; et
- des mesures administratives, telles que des vérifications de conformité et la formation des employés.

8. Les réseaux sans fil

Il est important de protéger la confidentialité des communications et de se prémunir contre les accès non autorisés au réseau. Par exemple, il existe un risque d'interception lorsqu'un ordinateur communique sans fil avec une imprimante. L'accès non autorisé à un réseau pourrait être le fait d'actions délibérées de la part de pirates informatiques, qui, dès qu'ils accèdent au réseau, peuvent s'emparer de mots de passe ou installer des logiciels malveillants. L'accès non autorisé pourrait également se produire à la suite de connexions accidentelles par ceux qui sont à proximité et dont les dispositifs sans fil se branchent sur un point d'accès sans fil insuffisamment sécurisé.

La sécurité d'un réseau sans fil peut être améliorée en prenant les mesures suivantes :

- utiliser un cryptage fort – celui de Wi-Fi Protected Access (WPA et WPA2) est un exemple de chiffrement fort pour sécuriser un réseau;
- modifier le mot de passe par défaut du routeur, qui relie les ordinateurs en réseau. Pour créer un mot de passe fort, il est recommandé d'appliquer les protocoles mentionnés sous le titre « Restrictions à l'accès et protocoles d'authentification » de la section 2 de la présente annexe;
- modifier le nom par défaut du réseau sans fil (connu sous le nom de SSID), et, en créant le nouveau nom, éviter les noms d'utilisateurs, le nom ou l'adresse de l'entreprise ou tout autre renseignement qui peut être facilement identifié;
- utiliser des coupe-feu à la fois sur le dispositif du réseau et sur l'ordinateur;
- désactiver la fonction de connexion automatique de l'ordinateur, qui permet à celui-ci de rechercher automatiquement un réseau sans fil ouvert;
- désactiver le réseau sans fil s'il y a des périodes de temps où personne ne se connectera au réseau; ou encore, restreindre l'accès 24 heures sur 24 à certains utilisateurs; et
- s'il s'agit d'activités de nature confidentielle, ne se connecter qu'à des réseaux sans fil sécuritaires.

9. Sources documentaires en matière de sécurité

« Password Security: A Guide for Students, Faculty, and Staff of the University of Michigan » University of Michigan, Information Technology Division, Reference R1192, révisé en avril 1997, < <http://www.umich.edu/~policies/pw-security.html> > (Guides pour choisir un mot de passe fort).

Microsoft, Security Central resource page :
<<http://www.microsoft.com/security/default.mspx>>.

Rutgers, « Wireless Security Recommendations »
<<http://techdir.rutgers.edu/wireless.html>>.

Microsoft, « Improve the Security of Your Wireless Home Network with Windows XP »
<<http://www.microsoft.com/windowsxp/using/networking/security/wireless.mspx>>.

Commissaire à l'information et à la protection de la vie privée de l'Alberta, Investigation Report P2006-IR-005 (septembre 2006),
<<http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf>>

Commissaire à l'information et à la vie privée de l'Ontario, ordonnance HO-004 (mars 2007), <http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf>

PracticePRO, « Managing the Security and Privacy of Electronic Data in a Law Office »
<http://www.practicepro.ca/practice/ElectronicDataSecurity.asp>

Lexique

blawg	terme anglais désignant les blogues juridiques
blogue	cybercarnets avec des inscriptions en ordre chronologique inverse
lien Internet mort	un hyperlien de renvoi qui ne fonctionne pas et qui ne conduit pas le lecteur à la bonne page Web active
clavardage	sites en ligne où les participants échangent des messages sous forme de conversation en ligne
piratage	une intrusion non autorisée dans un système informatique; le pirate est la personne à l'origine de l'intrusion
HTML	codes qui déterminent comment seront affichés les renseignements sur la page Web
forum Internet	un forum Internet comprend des groupes de discussion en ligne et des babillards électroniques
listes d'envoi électronique	listes d'envoi électronique, grâce à laquelle les messages adressés au serveur sont automatiquement redistribués à la liste d'adresses courriels des abonnés
périphérique de stockage	un dispositif de stockage de données portatif, également appelé « clé USB », « clé de mémoire » ou « disque flash »
hameçonnage	utilisation frauduleuse de communications qui consiste à revêtir l'apparence d'une entreprise légitime, telle qu'une banque, un site de vente aux enchères, un fournisseur de services Internet ou une société émettrice de cartes de crédit, en usurpant leurs marques et en amenant les internautes à divulguer des renseignements personnels critiques, tels que leur mot de passe, leur nom d'utilisateur et des renseignements sur leur compte
fenêtre contextuelle	un site Web qui ouvre automatiquement une petite fenêtre de navigateur Web sur le contenu du site Web original; les fenêtres contextuelles ont des fonctions utiles mais elles peuvent également servir à afficher de la publicité non sollicitée et être utilisées dans les stratagèmes d'hameçonnage
purge	action consistant à supprimer tout ce qu'il y a sur un disque dur de manière à empêcher qu'il ne soit restauré
réseau social en ligne	on peut citer comme exemple Facebook, YouTube, MySpace
pourriel	courriel commercial non sollicité
mot de passe fort	une combinaison de chiffres et de lettres qui ne peut être facilement devinée par une autre personne, ni facilement établie par un ordinateur
URL	une abréviation des termes <i>Uniform Resource Locator</i> , (localisateur de ressources uniformes), lequel est l'adresse que tape l'utilisateur dans la barre d'adresse d'un navigateur Web et qui le conduit à un site ou une page Web précise : <i>p. ex.</i> < http://www.cba.org/CBA/Gate.asp >
wikis	sites Web coopératifs qui peuvent être revus par quiconque a

	accès à Internet
nettoyage	action consistant à supprimer tout ce qu'il y a sur un disque dur de manière à empêcher qu'il ne soit restauré
XHTML	codes qui déterminent comment seront affichés les renseignements sur la page Web