THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
INFLUENCE. LEADERSHIP. PROTECTION.

La déontologie du droit à l'ère numérique

Comité de déontologie et de responsabilité professionnelle de l'ABC

(Les présentes lignes directrices s'inspirent des *Lignes directrices pour un exercice du droit conforme à la déontologie dans le cadre des nouvelles technologies de l'information* [2008], des *Lignes directrices d'éthique dans les pratiques de marketing recourant aux nouvelles technologies de l'information* [2009] et des lignes directrices *Respect de l'éthique : exercer le droit avec l'assistance de la technologie* [2014].)

865, avenue Carling, bureau 500, Ottawa (Ontario) Canada K1S 5S8
Tel/tél. : 613-237-2925 | **Toll free/sans frais :** 1-800-267-8860 | **Fax/téléc. :** 613-237-0185 | www.cba.org
Membership/adhésion : memberservice@cba.org | **PD/DP :** pd@cba.org | **Sections :** cba.sections@cba.org | **General/général :** info@cba.org

La déontologie du droit à l'ère numérique

Table des matières

Introduction

De nos jours, la technologie fait partie intégrante de la pratique du droit. Les avocats doivent savoir quand l'employer pour offrir des services juridiques efficaces, et ce, de façon responsable et éthique[1]. Au Canada, bien que les codes de déontologie n'imposent pas l'emploi de la technologie[2], contrairement aux États-Unis[3], ils contiennent tout de même plusieurs obligations qui laissent entendre qu'une utilisation adéquate de la technologie doit être envisagée. Pour mémoire, voici deux exemples de ces obligations : « s'adapter aux exigences, aux normes, aux techniques et aux pratiques professionnelles qui pourraient changer[4] » et « embaucher du personnel et entretenir les installations et le matériel nécessaires à l'exercice de sa profession[5] ». Si vous utilisez des moyens technologiques pour offrir des services juridiques ou gérer votre cabinet, d'autres règles de déontologie s'appliquent, dont celles qui régissent le secret professionnel et les pratiques de marketing des avocats. Le présent document a pour objet de vous aider à concilier technologie et déontologie.

Dans son rapport sommaire de 2013, *Atteindre l'égalité devant la justice : une invitation à l'imagination et à l'action,* le Comité de l'accès à la justice de l'ABC constate que « [l]a technologie (y compris la technologie de l'information) peut être mise à profit pour améliorer l'accès à la justice. [...] Une planification attentive est [toutefois] nécessaire pour éviter que des innovations technologiques créent ou renforcent des obstacles à l'égalité devant la justice[6]. » Ce comité recommande que « [l]a Fédération des ordres professionnels de juristes et le Comité de déontologie de l'ABC communiquent des indications sur les obligations éthiques et professionnelles dans l'utilisation de la technologie pour la prestation de services juridiques[7] ». On note également ceci dans le rapport préliminaire du projet de l'ABC Avenirs en droit : « À mesure qu'un nombre croissant de transactions seront effectuées en

---

1 Elaine Craig, « Examining the Websites of Canada's "Top Sex Crime Lawyers": The Ethical Parameters of Online Commercial Expression by the Criminal Defence Bar », *SSRN*, 2014. À paraître dans *UBC Law Review*.

2 Même le nouveau *Code de déontologie des avocats* du Québec (RLRQ, chap. B-1) ne mentionne aucune obligation de ce genre.

3 En 2012, par exemple, le commentaire de l'article 1.1 du code type de déontologie de l'American Bar Association (*Model Rules of Professional Conduct*) a été modifié afin d'établir sans équivoque que les avocats devaient se tenir informés des avantages et des risques liés à l'utilisation de la technologie.

4 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 3.1-1 (k). Notez que nous ferons souvent référence à ce *Code*. Même s'il n'a pas de valeur normative officielle, la plupart des barreaux du pays l'ont adopté, en tout ou en partie. Veuillez consulter les dispositions équivalentes dans le code de votre barreau.

5 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, commentaire de la r. 3.2-1.

6 Comité de l'accès à la justice de l'ABC, *Atteindre l'égalité devant la justice : une invitation à l'imagination et à l'action*, Ottawa, 2013, p. 21.

7 Comité de l'accès à la justice de l'ABC, *Atteindre l'égalité devant la justice : une invitation à l'imagination et à l'action*, Ottawa, 2013, p. 22.

ligne, il pourrait être nécessaire de reconsidérer les dispositions législatives et réglementaires pour assurer un degré suffisant de surveillance[8]. »

Compte tenu des multiples questions d'ordre déontologique soulevées par l'utilisation de la technologie dans la pratique du droit, et de la diversité de cette pratique, nous ne prétendons pas offrir une ressource complète ou normative. Notre but est de vous aider à reconnaître les enjeux d'éthique concernant l'emploi de la technologie et de vous faire connaître les ressources nécessaires pour adopter des pratiques exemplaires et trouver des solutions adaptées à vos besoins. Le rapport couvre les trois domaines de la technologie qui posent les plus grands risques en matière de déontologie : sécurité, marketing et prestation de services par voie électronique. Il existe d'autres domaines de préoccupation (voir section 4, « Les autres utilisations de la technologie »), et de nouveaux enjeux se profileront au fur et à mesure que l'exercice du droit et la technologie évolueront : la maîtrise des outils technologiques et l'exercice éthique du droit demandent un effort constant.

Lorsque vous consulterez les ressources répertoriées, n'oubliez pas que vos obligations déontologiques et juridiques sont régies par le code de déontologie professionnelle du barreau auquel vous êtes inscrit. Vous devez aussi prendre en considération l'actualité des ressources; nous avons l'intention de mettre à jour le présent document tous les deux ou trois ans, mais ce ne sera probablement pas suffisant pour suivre les progrès technologiques (vos codes de déontologie professionnelle pourraient aussi être modifiés, mais à une fréquence moindre). Si vous avez des questions concernant l'applicabilité d'une pratique ou d'une ressource, sur le plan juridique ou réglementaire, veuillez consulter votre barreau.

---

8 Projet de l'ABC *Avenirs en droit, L'avenir des services juridiques au Canada : tendances et enjeux*, Ottawa, 2013, p. 29.

1. La sécurité

- ✓ Vos mesures de sécurité physiques, organisationnelles et informatiques sont-elles adéquates?
- ✓ Vos ordinateurs sont-ils protégés par des câbles de sécurité ou d'autres mesures physiques?
- ✓ Votre utilisation des coupe-feu et des logiciels de détection d'intrusion est-elle adéquate?
- ✓ Votre utilisation des logiciels anti-programme malveillant est-elle adéquate?
- ✓ Votre cabinet a-t-il mis en place des politiques sur l'utilisation des technologies?
- ✓ Les avocats et le personnel du cabinet ont-ils reçu une formation adéquate en matière de technologies?
- ✓ Avez-vous pris les mesures nécessaires pour protéger l'intégrité de vos données?
- ✓ Si vous utilisez une signature électronique, respectez-vous les obligations juridiques et professionnelles applicables?
- ✓ Avez-vous fait une sauvegarde de vos données?
- ✓ Avez-vous évalué vos pratiques et vos politiques pour vérifier qu'elles ne faisaient pas obstacle à l'accessibilité et, le cas échéant, avez-vous pris les mesures nécessaires pour éliminer les obstacles?
- ✓ Vos mots de passe, vos autres limitations d'accès et vos protocoles d'authentification sont-ils suffisamment sécuritaires?
- ✓ Avez-vous recours au chiffrement lorsque c'est nécessaire?
- ✓ Lorsque vous voyagez à l'étranger, prenez-vous des mesures adéquates pour protéger les renseignements de vos clients?
- ✓ Avant de vous débarrasser de vos appareils électroniques, prenez-vous les mesures nécessaires pour éviter toute divulgation non autorisée de renseignements sur vos clients?
- ✓ Avez-vous pris des mesures de protection adéquates pour prévenir la divulgation involontaire de métadonnées?
- ✓ Votre utilisation d'un système infonuagique basé à l'étranger compromet-elle la confidentialité des renseignements de vos clients?
- ✓ Avez-vous mis au point un plan d'intervention en cas d'incident?

Vos mesures de sécurité physiques, organisationnelles et informatiques sont-elles adéquates?

Comme tous les professionnels, les avocats sont tenus de protéger les renseignements personnels[9] ou confidentiels[10] qu'ils se voient confier par leurs clients ou qu'ils obtiennent autrement. Ils doivent pour cela adopter des mesures de protection

---

9 *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, chap. 5, annexe 1, art. 4.7.

10 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 3.3-1. Il est bon de noter que certaines données, comme les secrets industriels, peuvent, selon les circonstances, être considérées comme des biens (*Cadbury Schweppes Inc. c. Aliments FBI Ltée*, [1999], 1 R.C.S. 142, para 47), et qu'un juriste doit « prendre soin des biens du client tout comme le ferait un propriétaire consciencieux et prudent avec des biens semblables » (Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 3.5-2).

physiques (cadenas, câbles, dispositifs de localisation pour les ordinateurs portables, systèmes d'alarme, etc. [11]), organisationnelles (politiques de sécurité[12], formation[13], etc.) et informatiques (coupe-feu[14], logiciels de détection d'intrusion, logiciels antivirus ou anti-programme malveillant[15], entre autres[16])[17].

Pour bien comprendre cette obligation, il importe de savoir ce contre quoi vous protègent ces mesures de sécurité. Comme l'a dit un auteur, [TRADUCTION] « il n'y a que six accidents possibles en ce qui concerne les données : elles peuvent être divulguées, détruites ou modifiées, accidentellement ou intentionnellement[18] ».

---

11 Pour en savoir plus sur les mesures de sécurité physiques, voir Dan Pinnington, « Cybercrimes and Law Firms: The Risks and Dangers are Real », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 6.

12 De nombreux exemples de politiques types sont disponibles en ligne; elles portent notamment sur la bonne utilisation du courriel et d'Internet, les restrictions sur le téléchargement et l'utilisation d'appareils mobiles. Voir par exemple : Law Society Of British Columbia, « Sample internet and email use policy »; LawPRO, « Model Electronic Document Handling Policy »; LawPRO, « Model Portable Device Security, Privacy and Usage Policy »; LawPRO, « Model Technology Usage Policy »; John W. Simek et Sharon D. Nelson, « Essential Law Firm Technology Policies and Plans », *Law Practice Magazine,* vol. 38, nº 2, 2012.

13 La formation joue un rôle important dans la sécurité des renseignements; elle permet d'acquérir des compétences techniques et de comprendre les enjeux déontologiques qui s'y rapportent. Par exemple, pour éliminer ou atténuer les risques liés à la cybercriminalité, on doit être en mesure de reconnaître certains problèmes (comme un accès non autorisé ou un ordinateur infecté). Pour connaître les symptômes d'un ordinateur infecté, voir par exemple Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 16.

14 Un coupe-feu est un logiciel ou un périphérique qui protège un ordinateur ou un réseau d'ordinateurs en autorisant ou refusant l'entrée ou la sortie de données au moyen d'un système de règles définies. Les versions récentes des systèmes d'exploitation comportent des coupe-feu intégrés pouvant être activés pour protéger les ordinateurs. Pour en savoir plus, voir Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 17.

15 Les virus, les vers informatiques, les logiciels de publicité, les réseaux de zombies, les logiciels espions, les programmes malveillants furtifs, les faux logiciels antivirus, les logiciels de rançon et les chevaux de Troie sont tous des exemples de logiciels malveillants. Les avocats auront avantage à utiliser des logiciels anti-programme malveillant pour détecter, bloquer et supprimer ces logiciels. Voir par exemple : Dave Bilinsky, « Tech security for lawyers », *Benchers' Bulletin,* nº 1, 2012, p. 9; Cyber Author, « Five Ways to Avoid a Cyber Attack at Your Law Firm », *ALPS 411,* 2014; Adam Carlson, « 3 Reasons Anti-Virus Software Alone Is No Longer Enough », *Law Technology Today,* 2013; Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take » *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 10.

16 Vous trouverez cette liste et la définition de chacun de ces termes dans Dan Pinnington, « Cybercrimes and Law Firms: The Risks and Dangers are Real », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 6 et 9.

17 *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, chap. 5, annexe 1, art. 4.7.3.

18 Peter S. Browne, « Computer security – A survey », *ACM SIGMIS Database,* vol. 4, nº 3, 1972, p. 1.

Pour prévenir ces « accidents », les mesures de sécurité doivent protéger a) l'intégrité, b) l'accessibilité et c) la confidentialité des renseignements des clients et des autres données confidentielles[19].

Avez-vous pris les mesures nécessaires pour protéger l'intégrité de vos données?

a) L'intégrité

Quand on parle d'intégrité en matière de protection de l'information, il n'est pas question du « devoir d'un juriste de respecter les normes et la réputation de la profession juridique[20] », mais plutôt de l'intégrité des documents ou des données. Cela implique que les données « sont identiques à l'original et qu'elles n'ont pas été modifiées, falsifiées ou détruites, par accident ou avec de mauvaises intentions[21] ». Non seulement la protection de l'intégrité des données est obligatoire en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*[22], mais elle est aussi inhérente à la compétence du juriste, puisque « l'obligation d'être compétent et de rendre des services satisfaisants suppose que l'opinion est fondée sur des renseignements suffisants[23] ». Évidemment, des données incomplètes ou corrompues ne peuvent être suffisantes.

Les avocats doivent adopter des mesures pour protéger l'intégrité des données qu'ils recueillent ou qu'ils conservent. Pensons aux signatures électroniques, aux politiques de conservation, à la comparaison des métadonnées ou à la sauvegarde des documents, qui permet de remplacer un fichier corrompu par une copie fidèle à l'original.

Si vous utilisez une signature électronique, respectez-vous les obligations juridiques et professionnelles applicables?

Intégrité est aussi synonyme d'authenticité, de non-répudiation et de traçabilité, ce qui est habituellement garanti par les signatures électroniques. Les juristes doivent apprivoiser cette technologie et connaître les lois applicables en la matière[24]. Par exemple, la légalité des signatures électroniques fait l'objet de dispositions dans la

---

19 Ces lignes directrices visent à souligner les risques liés aux données que détiennent les avocats. La protection des renseignements étant complexe, nous vous conseillons fortement de consulter un spécialiste externe pour déterminer les mesures de sécurité et de gestion du risque qui vous conviennent. Voir Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take » *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 10. : [TRADUCTION] « LawPRO encourage les cabinets à consulter des experts au besoin. »

20 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 2.1-2.

21 Harold F. Tipton et Micki Krause, *Information Security Management Handbook,* 6e éd., Auerbach, Boca Raton, 2007, p. 3043.

22 *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, chap. 5, annexe 1, art. 4.7.1.

23 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, commentaire de la r. 7.2-7.

24 Pour en savoir plus sur l'utilisation des signatures électroniques, voir par exemple Marg Bruineman, « Signing on the dotted line easy as 1-2 in the digital world », *Canadian Lawyer,* 2013; David Bilinsky, « E-billing, e-signatures and paperless offices », *Benchers' Bulletin,* nº 2, 2012; Catherine Sanders Reach, « Sign on the Dotted Line », *Slaw,* 2014.

Loi sur la protection des renseignements personnels et les documents électroniques[25] et dans la *Loi de 2000 sur le commerce électronique*. Il est à noter que la définition du terme *signature électronique* peut varier d'une province à une autre[26].

Nous vous invitons à vous doter de pratiques administratives réglementaires pour limiter l'accès à votre signature électronique et établir une liste des personnes autorisées à l'utiliser, définir les documents sur lesquels elle peut être apposée et déterminer dans quelles circonstances elle peut être utilisée[27].

Avez-vous fait une sauvegarde de vos données?

b) L'accessibilité

L'accessibilité des données peut être définie comme suit : possibilité, pour une entité autorisée, d'obtenir et d'utiliser des données sur demande[28]. Un juriste compétent doit notamment « communiquer les renseignements rapidement et efficacement à toutes les étapes de l'affaire[29] », ce qu'il ne pourra faire si les données concernées sont inaccessibles en raison de la maintenance des serveurs, d'une coupure de courant ou d'autres incidents comme des cyberattaques, de dégâts d'eau ou de systèmes désuets qui limitent l'accès aux dossiers numériques.

C'est pourquoi la sauvegarde des fichiers doit faire partie de toute politique de sécurité[30]. Selon la *Ligne directrice en matière de technologies* du Barreau du Haut-Canada : « L'avocate ou l'avocat devrait mettre en œuvre des mesures de sauvegarde et des plans de procédures de reprise après incident en matière de technologies de l'information. » Il est aussi recommandé de faire ce qui suit :

- sauvegarder fréquemment les données;
- entreposer les disques ou cassettes de sauvegarde hors du lieu de travail et en lieu sûr;

---

25 Barreau du Haut-Canada, « Electronic Signatures ».

26 Au Québec, par exemple, taper son nom au bas d'un document est considéré comme une signature électronique valide dans bien des contextes, alors qu'ailleurs, les signatures électroniques se limitent aux signatures qui utilisent des algorithmes de chiffrement afin de garantir l'authenticité d'un document. Voir la *Loi concernant le cadre juridique des technologies de l'information,* RLRQ, chap. C-1.1, art. 39.

27 Le Barreau du Haut-Canada conseille notamment ceci : aucune règle du *Code de déontologie des juristes* (*Code des juristes*) ou du *Code de déontologie des parajuristes* (*Code des parajuristes*) n'interdit l'utilisation des signatures électroniques. Si vous décidez d'utiliser une telle signature, vous devez mettre en place des mesures de sécurité pour empêcher qu'elle soit obtenue, utilisée ou copiée sans autorisation. Si un employé est chargé d'apposer votre signature à votre place, vous devez le superviser pour vous assurer que votre signature est utilisée adéquatement. [Partie I du règlement administratif 7.1; règle 5.01 du *Code des juristes*; paragraphe 8.01 (3) du *Code des parajuristes*].

28 Harold F. Tipton et Micki Krause, *Information Security Management Handbook,* 6e éd., Auerbach, Boca Raton, 2007, p. 3020.

29 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 3.1-1.

30 Voir par exemple : LawPRO, « Backup Best Practices and Strategies »; American Bar Association, « FYI: Data Backup »; Barreau du Québec, *Guide des TI : Gestion et sécurité des technologies de l'information pour l'avocat et son équipe*.

- effectuer des vérifications régulières pour garantir que les données puissent être récupérées;
- souscrire une assurance couvrant les coûts de récupération en cas de perte de pièces d'équipement ou de données numérisées[31].

Il est particulièrement important de suivre ces conseils lorsque les données sont conservées sur des serveurs appartenant à un tiers – que ce soit aux termes d'un contrat d'hébergement de base ou dans une infrastructure infonuagique –, étant donné le risque accru que les données se trouvent temporairement inaccessibles en raison de problèmes de connexion, ou parce que le fournisseur de service a décidé d'en limiter l'accès en raison d'un arriéré de paiement ou d'une autre mésentente contractuelle.

Avez-vous évalué vos pratiques et vos politiques pour vérifier qu'elles ne faisaient pas obstacle à l'accessibilité et, le cas échéant, avez-vous pris les mesures nécessaires pour éliminer les obstacles?

Votre obligation concernant l'accessibilité des données va toutefois plus loin qu'un accès rapide aux fichiers numériques. Ceux-ci doivent également être intelligibles pour la personne qui demande à les consulter. Cela suppose d'avoir accès au logiciel permettant de lire un document donné (une ancienne version d'un logiciel de traitement de texte comme Word Perfect, par exemple) ou de veiller à ce que les documents électroniques soient accessibles aux personnes handicapées[32], que ce soit des membres du cabinet, des clients ou des recrues[33].

Comme le soulignent les Règles pour l'accessibilité des contenus Web 2.0 du Consortium World Wide Web[34], l'accessibilité des sites Web et des contenus Web peut être particulièrement difficile pour les personnes handicapées. Il peut également être difficile de consulter des documents dont le formatage est stylisé, pour des personnes qui utilisent des accessoires fonctionnels comme des lecteurs d'écran[35].

---

31 Barreau du Haut-Canada, *Ligne directrice en matière de technologies*.

32 Pour en savoir plus, consulter ON donne accès, *Comment rendre l'information accessible pour les personnes handicapées* et Global Alliance for Accessible Technologies and Environments (GAATES), « Accessible Information and Communication: A Guide for Small Business », Toronto, 2013.

33 Les codes de déontologie reconnaissent que le « juriste est tenu de respecter les exigences des lois sur les droits de la personne qui sont en vigueur au Canada, ainsi que dans les provinces et territoires. Il est particulièrement tenu de respecter les obligations prévues par les lois sur les droits de la personne » (Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, commentaire de la r. 6.3).

34 Consortium World Wide Web, Getting Started with Web Accessibility.

35 Par l'entremise de l'Accessible Digital Office Document (ADOD) Project, des outils sont disponibles pour vous aider à produire des documents administratifs accessibles (Accessible Digital Office Document (ADOD) Project).

Les normes d'accessibilité – notamment en ce qui concerne les documents électroniques – diffèrent d'une province à une autre[36]. Renseignez-vous sur les normes en vigueur et assurez-vous de les respecter.

Vos mots de passe, vos autres limitations d'accès et vos protocoles d'authentification sont-ils suffisamment sécuritaires?

c) La confidentialité

Un « juriste est tenu en tout temps de garder dans le plus grand secret tous les renseignements qu'il apprend au sujet des affaires et des activités d'un client au cours de la relation professionnelle et ne doit divulguer aucun de ces renseignements[37] ». Au Canada, bien que les codes de déontologie professionnelle ne précisent pas les mesures à prendre pour protéger la confidentialité des renseignements des clients lorsqu'il est question de technologie[38], des lois comme la *Loi sur la protection des renseignements personnels et les documents électroniques* orientent les avocats et le public quant au type de mesures à adopter : des mesures physiques comme les classeurs verrouillés et le fait de limiter l'accès aux bureaux, des mesures organisationnelles comme les autorisations de sécurité et l'accès réservé

---

36 Par exemple, les normes d'accessibilité s'appliquant aux cabinets d'avocats sont énoncées dans la *Loi de 2005 sur l'accessibilité pour les personnes handicapées de l'Ontario*, LO 2005, chap. 11 (pour en savoir plus sur ces obligations, voir : Ministère du Développement économique, de l'Emploi et de l'Infrastructure, *Rendre l'Ontario accessible*); ON donne accès, *Guide relatif au règlement sur les Normes d'accessibilité intégrées*, 2014; Barreau du Haut-Canada, « Normes d'accessibilité intégrées de la *Loi de 2005 sur l'accessibilité pour les personnes handicapées de l'Ontario* – Obligations légales des cabinets comptant moins de 50 employés »; Barreau du Haut-Canada, « Normes d'accessibilité intégrées de la *Loi de 2005 sur l'accessibilité pour les personnes handicapées de l'Ontario* – Obligations légales des cabinets comptant 50 employés ou plus ») et dans la *Loi sur l'accessibilité pour les Manitobains*, CPLM, chap. A1.7 (pour en savoir plus sur ces obligations, voir le Bureau des personnes handicapées du gouvernement du Manitoba). En ce qui concerne l'accès général aux documents électroniques, la loi québécoise énonce ceci : « Le choix d'un support ou d'une technologie tient compte de la demande de la personne qui a droit d'accès au document, sauf si ce choix soulève des difficultés pratiques sérieuses, notamment en raison des coûts ou de la nécessité d'effectuer un transfert. » (*Loi concernant le cadre juridique des technologies de l'information*, RLRQ, chap. C-1.1, art. 23.)

37 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 3.3-1.

38 Bien que le code type de déontologie de l'American Bar Association (*Model Rules of Professional Conduct*) ne soit pas normatif, la règle 1.6 (c) et son commentaire peuvent aider les avocats à déterminer les facteurs à prendre en compte en ce qui concerne les efforts raisonnables qu'ils devront fournir pour prévenir la divulgation involontaire ou non autorisée de renseignements sur un client, notamment : le caractère délicat d'une information, les risques de divulgation en l'absence de mesures de sécurité additionnelles, le coût de ces mesures additionnelles, les difficultés liées à la mise en œuvre de ces mesures et les répercussions négatives de ces mesures sur la capacité des avocats à représenter leurs clients (ex. : si un appareil ou un logiciel important est très difficile à utiliser).

aux personnes ayant besoin de consulter les données, et des mesures informatiques comme les mots de passe[39] et le chiffrement[40]. Renseignez-vous sur les lois provinciales et fédérales, notamment les lois sur la protection de la vie privée; elles régissent vos pratiques de traitement de l'information[41].

Lorsque vous voyagez à l'étranger, prenez-vous des mesures adéquates pour protéger les renseignements de vos clients?

Les avocats devraient adopter des mesures de sécurité visant à empêcher les tiers d'accéder aux données confidentielles durant le cycle de vie de ces données, soit la période entre leur création et leur destruction. Il faut par conséquent protéger les données en tout temps. Par exemple, si des renseignements confidentiels sont transportés hors des bureaux, il faut des mécanismes de chiffrement pour les protéger[42]. En fait, lorsque c'est possible, il vaut mieux consulter l'information au

---

39 Des mots de passe forts et des authentifications à deux facteurs ou à facteurs multiples sont des exemples de mesures de protection efficaces. De plus en plus, on recommande d'avoir recours à ces modèles d'authentification. Cette mesure renforce la sécurité en jumelant un élément que vous connaissez – votre mot de passe – avec un élément que vous possédez. (Sam Glover, « Passwords: a User Guide for Lawyers and Law Firms », *Lawyerist,* 2014.) Les avocats devraient également veiller à protéger leurs mots de passe après leur création. Pour en savoir plus sur les mots de passe et leur protection : David J. Bilinsky, « Secure Passwords », *thoughtfullaw.com,* 2013; David Whelan, « Your Passwords S**** », *Slaw,* 2014; Dan Pinnington, « Keeping Your Passwords Strong and Secure », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 30; Lawyers' Insurance Association of Nova Scotia, « Data Security »; Barreau du Québec, *Guide des TI : Gestion et sécurité des technologies de l'information pour l'avocat et son équipe*.

40 On recommande parfois aux avocats de chiffrer la totalité des disques sur leurs ordinateurs et leurs appareils de travail qui contiennent des renseignements confidentiels ou particuliers sur un client (David Whelan, « Getting Started with Law Office Technology » [n'est plus disponible en ligne]). Voir également : Dave Bilinsky, « Tech security for lawyers », *Benchers' Bulletin,* nº 1, 2012, p. 9; Barreau du Québec, *Guide des TI : Gestion et sécurité des technologies de l'information pour l'avocat et son équipe*; Seth Schoen, « New Year's Resolution: Full Disk Encryption on Every Computer You Own », 2011. Si vous utilisez un réseau sans fil dans votre cabinet, il est recommandé d'utiliser le chiffrement WPA ou WPA2 (ce dernier est encore mieux), ou encore 802.1x; le chiffrement WEP, qu'on trouve sur les vieux appareils, est à éviter puisqu'il est facile de le pirater. Enfin, les avocats devraient protéger leurs réseaux sans fil en adoptant également les mesures suivantes : empêcher la diffusion de leur nom de réseau sans fil, bloquer les réseaux invités, activer le filtre MAC, personnaliser le nom et le mot de passe du routeur et désactiver la gestion à distance (Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 10.

41 Voir par exemple : Commissariat à la protection de la vie privée du Canada, *La LPRPDE et votre pratique : Guide sur la protection de la vie privée à l'intention des avocats*, Ottawa, 2011. Ce document traite entre autres de l'application et des exigences de la *Loi,* des enjeux liés à la protection de la vie privée dans la gestion d'un cabinet et de ces mêmes enjeux dans le contexte des litiges civils. Il existe également des obligations particulières en vertu des lois provinciales, en ce qui concerne les dossiers médicaux. Voir à ce sujet Nina Bombier et Paul-Erik Veel, « When Medical Records Go Missing », *Lawyers Weekly,* 2014, p. 15 (voir aussi la *Loi de 2004 sur la protection des renseignements personnels sur la santé,* LO 2004, chap. 3, annexe A).

42 Commissariat à la protection de la vie privée du Canada, *La LPRPDE et votre pratique : Guide sur la protection de la vie privée à l'intention des avocats*, Ottawa, 2011, p. 11. Voir aussi : Barreau du Québec, *Guide des TI : Gestion et sécurité des technologies de l'information pour l'avocat et son équipe*.

moyen d'une connexion VPN[43] sécurisée que de transporter des fichiers sur le disque dur d'un ordinateur portable ou une clé USB. Pensez-y quand vous voyagez à l'international : les appareils électroniques peuvent faire l'objet d'un contrôle à la douane[44]. Lorsque vous n'êtes pas au bureau, prenez garde aux réseaux sans fil; ils sont sujets à des effractions qui peuvent compromettre la confidentialité des renseignements des clients[45].

Avant de vous débarrasser de vos appareils électroniques, prenez-vous les mesures nécessaires pour éviter toute divulgation non autorisée de renseignements sur vos clients?

Quand les données d'un client ne servent plus, elles devraient être détruites pour de bon[46]. Sur un ordinateur, une tablette ou un téléphone intelligent, la fonction ordinaire de suppression n'est pas suffisante pour empêcher un tiers de récupérer un fichier supprimé. Bien que l'option la plus sécuritaire consiste à détruire physiquement le support sur lequel sont conservées les données confidentielles, le nettoyage, la purge ou le broyage sont des formes de suppression plutôt efficaces[47]. Il existe de nombreux programmes de nettoyage de fichiers. N'oubliez pas que les disques durs des photocopieuses et des imprimantes peuvent aussi stocker des images des documents[48].

Avez-vous pris des mesures de protection adéquates pour prévenir la divulgation involontaire de métadonnées?

Quand vous communiquez électroniquement avec l'avocat de la partie adverse, assurez-vous que les documents envoyés par courriel ne contiennent pas de métadonnées confidentielles[49]. On peut décrire les métadonnées comme des renseignements sur d'autres données. De nombreux logiciels intègrent des renseignements à la sortie du programme au moment où celui-ci est créé, ouvert et enregistré. Bien qu'elles soient masquées en vue normale, les métadonnées peuvent être consultées par d'autres

---

43 Un VPN, ou réseau privé virtuel, offre aux avocats une connexion sécurisée à leur réseau privé, sur Internet.

44 Luigi Benetton, « Comment protéger les données dans son ordinateur portatif avant de traverser la frontière », *En pratique de l'ABC,* 2009. Voir aussi : Barreau du Haut-Canada, « Technology Practice Tips: Clean Devices (Transcript) »; Seth Schoen, Marcia Hofmann et Rowan Reynolds, « Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices », *Electronic Frontier Foundation,* 2011.

45 Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 10.

46 Barreau du Québec, *Guide des TI : Gestion et sécurité des technologies de l'information pour l'avocat et son équipe*.

47 Pour en apprendre davantage sur la suppression sécuritaire des fichiers électroniques, voir : Law Society of British Columbia, « Closed Files – Retention and Disposition », 2015; Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 10; Sharon D. Nelson et John W. Simek, « Technology and the Sale of a Law Practice », *GP Solo,* vol. 29, nº 4, 2012.

48 Pour en savoir plus, voir Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 10.

49 Barreau du Québec, *Guide des TI : Gestion et sécurité des technologies de l'information pour l'avocat et son équipe*.

personnes lorsque le document est diffusé par voie électronique. Les métadonnées peuvent comprendre le nom de l'auteur du document, sa date de création, les révisions qui y ont été apportées (y compris les insertions et les suppressions, le suivi des modifications et les commentaires ajoutés par les auteurs des révisions) et l'emplacement du fichier[50]. Par conséquent, à l'exception des cas où l'avocat est tenu par la loi de communiquer les métadonnées (p. ex. : obligation de communication préalable), il vaut mieux éviter de créer des métadonnées ou les supprimer avant d'envoyer des documents[51].

Votre utilisation d'un système infonuagique basé à l'étranger compromet-elle la confidentialité des renseignements de vos clients?

La question de la confidentialité se pose également lorsque les renseignements sont conservés sur des serveurs basés hors du Canada, certains gouvernements étrangers ayant adopté des lois leur donnant accès à ces renseignements[52]. La Law Society of British Columbia s'est dotée de règles strictes concernant l'utilisation de systèmes infonuagiques ou de services externes dont les serveurs se trouvent à l'étranger[53]. Même des serveurs situés au Canada peuvent être assujettis à d'autres lois que les nôtres s'ils appartiennent à des intérêts étrangers. De la même façon, les renseignements envoyés par voie électronique qui transitent par d'autres pays (un routage à effet boomerang) peuvent être soumis aux lois de ces pays. C'est pourquoi, sauf indication contraire du client, les renseignements confidentiels envoyés à un serveur ou à un tiers au moyen d'Internet doivent être chiffrés[54].

---

50 Pour consulter une liste plus exhaustive des renseignements compris dans les métadonnées, voir Dan Pinnington, « Beware the Dangers of Metadata », *LawPRO Magazine,* 2004, p. 36.

51 Voir par exemple : « Supprimer des données masquées et des informations personnelles dans des documents Office »; « Supprimer des données masquées et des informations personnelles en inspectant des documents »; « Suppression de contenu confidentiel dans les fichiers PDF »; Dan Pinnington, « Beware the Dangers of Metadata », *LawPRO Magazine,* 2004, p. 36; David Bilinsky, « Beware of Tracked Changes in Word », *Slaw,* 2010; Donna Payne, « Metadata: The Good, the Bad, and the Misunderstood », *GP Solo,* vol. 30, nº 2, 2013; District of New Jersey, « Guidelines for Editing Metadata ».

52 Le risque demeure important, car si vous placez vos données, et celles de vos clients, entre les mains de tiers, des problèmes de sécurité, de confidentialité, de conformité et de gestion du risque peuvent notamment survenir (Law Society of British Columbia, « Cloud Computing Checklist, 2013 »). Le risque gagne d'ailleurs en importance si le fournisseur de services se situe à l'étranger, dans un pays où les règlements en matière de secret professionnel et de confidentialité sont différents (Association du Barreau canadien, *Secret professionnel et confidentialité pour les conseillers juridiques d'entreprises : FAQ,* 2012).

53 Dave Bilinsky, « Frequently Asked Questions (And Answers) on BC Lawyers' Use of Cloud Computing », *Slaw,* 2014.

54 Pour en savoir plus, voir : David Fraser, « L'infonuagique : La "Foire aux questions" sur le respect de la vie privée », *National,* 2014; Law Society of British Columbia, « Cloud Computing Checklist », 2013; Law Society of British Columbia, « Cloud Computing Due Diligence Guidelines », 2012; Dan Pinnington, « Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 10; David Whelan, « Step by Step Cloud Computing For Lawyers », 2013.

Avez-vous mis au point un plan d'intervention en cas d'incident?

Malgré toutes les mesures de sécurité, il y a toujours un risque que les données des clients soient divulguées, détruites ou modifiées. Les cabinets sont donc encouragés à se doter d'un plan d'intervention en cas d'incident. Les spécialistes sont nombreux à insister sur l'importance d'un tel plan pour gérer les cas d'atteinte à la sécurité[55].

---

55 Voir par exemple : Cyber Author, « Five Ways to Avoid a Cyber Attack at Your Law Firm », *ALPS 411,* 2014; Nora Rock, « Be Ready with an Incident Response Plan », *LawPRO Magazine,* vol. 12, nº 4, 2013, p. 28; Pablo Fuchs, « La protection des données », *National,* 2013.

2. Le marketing

- ✓ Votre présence dans le cyberespace respecte-t-elle les règles de déontologie sur le marketing?
- ✓ Vos communications électroniques à des fins de marketing respectent-elles la loi anti-pourriel?
- ✓ Connaissez-vous les risques déontologiques du marketing dans les médias sociaux?
- ✓ Votre utilisation des médias sociaux entraîne-t-elle des risques de divulgation par inadvertance de renseignements confidentiels?
- ✓ Avez-vous mis en place une politique sur les médias sociaux?

Votre présence dans le cyberespace respecte-t-elle les règles de déontologie sur le marketing?

Les avocats qui font la promotion de leurs services doivent respecter des règles de déontologie. Par exemple, la règle 4.2-1 du *Code type de déontologie professionnelle* de la Fédération stipule qu'« [u]n juriste peut commercialiser ses services professionnels pourvu que : (a) il puisse démontrer que cette publicité est vraie, exacte et vérifiable; (b) cette publicité ne soit pas mensongère, ne prête pas à confusion ou ne soit pas trompeuse, ou qu'elle ne risque pas d'induire en erreur, de prêter à confusion ou de tromper; (c) cette publicité soit dans le meilleur intérêt du public et respecte un niveau élevé de professionnalisme[56]. » Il va sans dire que ces normes déontologiques s'appliquent à toutes les formes de publicité, qu'elles soient imprimées ou électroniques, comme les sites Web, les courriels ou les médias sociaux (Facebook, LinkedIn ou Twitter, par exemple).

Les cabinets juridiques utilisant principalement les sites Web comme fenêtre sur la Toile, ces sites font l'objet d'une surveillance nettement accrue en raison du non-respect, par certains, des règles de déontologie. Une étude indique que [TRADUCTION] « [c]ertains sites Web d'avocats […] ne respectant apparemment pas ces règles contiennent : du matériel promotionnel paraissant vanter l'acquittement de clients qui seraient en fait coupables ou vanter la combativité du juriste; du matériel banalisant la violence sexuelle; de la publicité glorifiant certaines stratégies de défense en cour; et du contenu comportant des inexactitudes au regard de la loi ou des renseignements juridiques prêtant à confusion[57]. »

Outil marketing précieux pour un cabinet, le site Web peut aussi servir l'intérêt public en favorisant l'accès à la justice. Après tout, cet accès [TRADUCTION] « postule que le public puisse obtenir des renseignements compréhensibles sur le système de justice, ses ressources et les moyens d'y accéder[58] ». Les sites des cabinets peuvent rapprocher la justice des particuliers [TRADUCTION] « en produisant et en diffusant de

---

56 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r 4.2-1.

57 Elaine Craig, « Examining the Websites of Canada's 'Top Sex Crime Lawyers': The Ethical Parameters of Online Commercial Expression by the Criminal Defence Bar », *SSRN*. À paraître dans *UBC Law Review*.

58 Washington State Supreme Court, *Washington State Access to Justice Technology Principles*, 2004.

l'information et du matériel sous des formes et par des moyens susceptibles de rejoindre le public le plus large et varié possible[59] ». En ce sens, [TRADUCTION] « le blogue d'un cabinet est l'expression moderne des services publics que rendent les juristes[60] ». Pour que votre site Web soit un outil vraiment efficace de promotion comme d'accès à la justice, assurez-vous que son contenu est à la portée des clients potentiels. Comme le suggère un expert :

- utilisez un langage accessible et des phrases simples;
- usez de points, titres, phrases et paragraphes concis;
- insérez des hyperliens facilitant la navigation vers des renseignements utiles;
- rendez vos coordonnées et les renseignements sur vos employés immédiatement accessibles;
- projetez une image professionnelle… sans abuser du jargon juridique[61].

Cela dit, offrir gratuitement des renseignements juridiques sur votre site Web est risqué pour bien des raisons. Primo, ils pourraient être faussement interprétés comme étant un avis juridique[62]. Secundo, admettons que vous publiiez l'analyse d'une décision récente et qu'elle soit infirmée par la suite; ceux qui la liront dans les mois ou les années suivantes pourraient être induits en erreur[63]. Tertio – nous en reparlerons à la section suivante –, des résidents d'autres provinces ou territoires pourraient découvrir et utiliser ces renseignements, vous faisant accuser d'exercice illégal de la profession là où vous n'y êtes pas habilité[64]. De telles accusations pourraient aussi résulter de l'offre d'outils automatisés aidant les particuliers à rédiger eux-mêmes leurs documents juridiques[65].

---

59 Washington State Supreme Court, *Washington State Access to Justice Technology Principles*, 2004.

60 William R. Peterson et Clark E Smith, « Law Firm Websites: An Ethical Minefield », *The Bencher*, 2013.

61 Sphere UP, *5 Tips That Can Help Your Law Firm Website Attract Clients*, 2013.

62 William R. Peterson et Clark E Smith, « Law Firm Websites: An Ethical Minefield », *The Bencher*, 2013; James E. Cabral et coll., « Using Technology to Enhance Access to Justice », *Harvard Journal of Law & Technology*, vol. 26, nº 1, 2012, p. 241-317.

63 William R. Peterson et Clark E Smith, « Law Firm Websites: An Ethical Minefield », *The Bencher*, 2013.

64 William R. Peterson et Clark E Smith, « Law Firm Websites: An Ethical Minefield », *The Bencher*, 2013; James E. Cabral et coll., « Using Technology to Enhance Access to Justice », *Harvard Journal of Law & Technology*, vol. 26, nº 1, 2012, p. 241-317.

65 James E. Cabral et coll., « Using Technology to Enhance Access to Justice », *Harvard Journal of Law & Technology*, vol. 26, nº 1, 2012, p. 241-317.

Bien que ces outils et renseignements gratuits aident à promouvoir l'accès à la justice, des administrateurs de sites Web ont été reconnus coupables d'exercice illégal du droit[66]. Les cabinets devraient donc afficher un avis de dégagement de responsabilité en bonne et due forme parmi les conditions d'utilisation ou sur une autre page de leur site[67].

Vos communications électroniques à des fins de marketing respectent-elles la loi anti-pourriel?

Si vous décidez d'utiliser les médias sociaux ou les courriels comme plate-forme de marketing, prenez connaissance des lois et règlements canadiens anti-pourriel. Ceux-ci s'appliquent aux juristes et régissent l'envoi de communications électroniques commerciales non sollicitées (« pourriels »)[68].

Connaissez-vous les risques déontologiques du marketing dans les médias sociaux?

Comme l'a fait remarquer le Barreau du Haut-Canada, les médias sociaux peuvent s'avérer des outils de marketing efficaces, mais les avocats se doivent de respecter les règles du jeu[69]. Le terme « médias sociaux » peut désigner toute une variété de technologies[70], chacune présentant ses propres risques associés au marketing. Prenez le temps de bien saisir leurs différences et les risques en découlant[71], et évitez

---

66 James E. Cabral et coll., « Using Technology to Enhance Access to Justice », *Harvard Journal of Law & Technology*, vol. 26, nº 1, p. 241-319.

67 Modèle : Association du Barreau canadien, *Modèle des conditions d'utilisation du site Web du cabinet et dégagement de responsabilité*, 2008.

68 L.C. 2010, ch. 23. Pour en savoir plus : Ava Chisling, « What's it all about? How anti-spam legislation can affect your firm », *EnPratique de l'ABC*. Le gouvernement du Canada et le CRTC ont tous deux des sites Web permettant aux organisations de vérifier si leurs politiques de marketing par courriel sont conformes à la *Loi*. Voyez la *Loi canadienne anti-pourriel* et le Conseil de la radiodiffusion et des télécommunications canadiennes.

69 Barreau du Haut-Canada, « Social media can provide helpful marketing tools – but lawyers must play by the rules », *La revue des juristes de l'Ontario,* 2010, p. 10.

70 Phil Brown et Davis Whelan, *The Ethics of Social Media for Lawyers*, 2012. Par exemple, la page *Social Media* (20 décembre 2011) de la Law Society of England and Wales énumère huit formes différentes de média sociaux : 1) les forums et les sections de commentaires des sites Web d'information; 2) les sites Web de réseautage social, comme Facebook et LinkedIn; 3) les sites Web de diffusion de vidéos et de photos, comme Flickr et YouTube; 4) les blogues, y compris les blogues d'entreprise et les blogues personnels; 5) les sites de microblogage, comme Twitter; 6) les forums et babillards électroniques, comme Yahoo! Groupes ou Google Groupes; 7) les sites wiki où des collaborateurs peuvent participer à la rédaction du contenu, comme Wikipédia; 8) tout autre site Web où des particuliers et entreprises peuvent utiliser des outils simples de publication.

71 Vous pouvez trouver de nombreuses ressources utiles en ligne pour vous renseigner sur les différents types de médias sociaux et sur les risques de problèmes déontologiques posés par chacun d'entre eux. Voir, par exemple : Phil Brown et Davis Whelan, *The Ethics of Social Media for Lawyers*, 2012; Meritas, *Social Media Guide for Lawyers*, 2011; Dan Pinnington, « Social Media: How? – A primer on using social media in a law firm », *LawPRO Magazine,* vol. 8, nº 4, 2009, p. 12; Ernie Svenson, *Blogging in One Hour for Lawyers*, American Bar Association, Chicago, 2013; Dennis Kennedy et Allison C. Shields, *Facebook in One Hour for Lawyers*, American Bar Association, Chicago, 2012; Ruth Carter, *The Legal Side of Blogging for Lawyers*, American Bar Association, Chicago, 2014; Dennis Kennedy et Allison C. Shields, *LinkedIn in One Hour for Lawyers*, 2e éd., American Bar Association, Chicago, 2013; Jared Correia, *Twitter in One Hour for Lawyers*, American Bar Association, Chicago, 2012.

d'assouplir vos normes si vous faites la promotion de vos services dans cet environnement informel (par opposition aux sites Web officiels). Dans le cas contraire, vous pourriez contrevenir à la loi[72].

Votre utilisation des médias sociaux entraîne-t-elle des risques de divulgation par inadvertance de renseignements confidentiels?

La divulgation involontaire de renseignements confidentiels est un risque qu'implique l'utilisation des médias sociaux[73]. Par exemple, la création de réseaux par l'entremise des médias sociaux (en ajoutant des amis ou des abonnements à un compte) risque d'indiquer qu'un client a retenu les services d'un avocat en particulier. De plus, certains services des médias sociaux peuvent dévoiler l'emplacement des utilisateurs (on pourrait ainsi savoir qu'un avocat se trouve dans la ville ou le quartier où l'entreprise de son client est établie[74]).

Avez-vous mis en place une politique sur les médias sociaux?

Pour ces raisons et bien d'autres, les cabinets juridiques doivent se doter d'une politique sur les médias sociaux[75]. Une telle politique permet aux avocats et aux autres membres du personnel du cabinet de connaître les normes et protocoles concernant leur utilisation. On évite ainsi qu'un mauvais usage des médias sociaux porte préjudice à la réputation du cabinet[76].

---

72 Voici des types de comportements interdits : indiquer une somme d'argent que le juriste a récupérée pour un client ou faire mention du taux de réussite du juriste dans ses dossiers antérieurs, à moins qu'une telle déclaration soit accompagnée d'une autre qui précise que les résultats antérieurs ne sont pas forcément révélateurs des résultats futurs et que la somme récupérée et l'issue d'autres litiges varieront selon les faits de chaque dossier particulier; prétendre être supérieur aux autres juristes; susciter des attentes qui ne peuvent être justifiées; laisser entendre ou prétendre que le juriste est combatif; déprécier ou rabaisser d'autres personnes, groupes, organismes ou établissements; exploiter une personne ou un groupe vulnérable; se servir de témoignages de reconnaissance ou d'appui qui lancent un appel émotionnel. Lire le commentaire accompagnant la règle 4.2-1 dans : Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*.

73 De nombreuses ressources documentaires contiennent des astuces pour protéger la confidentialité des renseignements dans les médias sociaux. Voir, par exemple : Dan Pinnington, « The Dangers of Social Networking and How to Avoid Them », *LawPRO Magazine Student Issue,* nº 2, 2014, p. 18; David Whelan, *The Practical and Ethical Use of Social Media,* 2012; Meritas, *Social Media Guide for Lawyers*, 2011.

74 Ces deux exemples sont traités dans David Whelan, *The Practical and Ethical Use of Social Media*, 2012.

75 Doug Cornelius, « Top Ten Mistakes Lawyers Make with Social Media », *EnPratique de l'ABC,* 2009.

76 Source : Law Society of England and Wales, *Social Media*, 2011. Pour en savoir plus sur ce qui fait l'efficacité d'une politique sur les médias sociaux, voir, par exemple : Law Society Of British Columbia, *Model Policy – Social Media and Social Networking*; Lawyers' Insurance Association of Nova Scotia, *Social Media in the Workplace*; Meritas, *Social Media Guide for Lawyers*, 2011.

3. La prestation de services par voie électronique

- ✓ Prenez-vous des précautions pour éviter d'établir une relation avocat-client par inadvertance en échangeant de l'information en ligne?
- ✓ Respectez-vous les exigences d'identification du client lorsque vous communiquez uniquement par voie électronique?
- ✓ Prenez-vous des mesures pour éviter les risques de conflit d'intérêts posés par votre présence en ligne?
- ✓ Veillez-vous à ce que vos clients puissent vous identifier avec certitude dans vos communications électroniques?
- ✓ Prenez-vous des mesures pour éviter d'exercer le droit illégalement dans d'autres provinces ou territoires?
- ✓ Vous assurez-vous que vos clients sont conscients des risques liés à la communication par voie électronique et qu'ils les acceptent?
- ✓ Vous assurez-vous que vos clients sont conscients des risques liés aux outils de vidéoconférence et qu'ils les acceptent?
- ✓ Vous pliez-vous à vos obligations en matière de supervision en ligne?
- ✓ Offrez-vous de l'aide en personne aux clients actuels ou potentiels qui n'ont pas les moyens ou les capacités d'utiliser les solutions technologiques?

Fournir des services juridiques par voie électronique (c.-à-d., interagir avec les clients actuels ou potentiels par courriel, médias sociaux, vidéoconférence ou par d'autres solutions de télécommunication) permet d'élargir sa clientèle et peut améliorer l'accès à la justice pour les gens mal desservis par la profession.

Cela apporte cependant de nombreux risques sur le plan de la conformité (liés aux points vus précédemment, comme la confidentialité) et d'autres dangers, comme : la création involontaire d'une relation avocat-client ou de conflits d'intérêts; l'exercice illégal du droit par inadvertance[77]; l'identification et la vérification inadéquates des clients; une supervision inadéquate; et de possibles problèmes d'accès aux services juridiques pour les clients dépourvus des moyens ou des capacités de se prévaloir des solutions technologiques.

Prenez-vous des précautions pour éviter d'établir une relation avocat-client par inadvertance en échangeant de l'information en ligne?

Offrir des renseignements juridiques en ligne peut être une bonne stratégie de marketing, mais il faut faire attention à ne pas établir une relation avocat-client par inadvertance – c'est possible, même sans entente écrite formelle. Par exemple, le *Code type* de la Fédération des ordres professionnels de juristes du Canada définit simplement un client comme « une personne qui[,] après avoir consulté le juriste, conclut raisonnablement que le juriste a accepté de rendre des services juridiques en son nom[78] ».

---

77 Plus sur ces risques et d'autres dangers : Dan Pinnington, « The Dangers of Social Networking and How to Avoid Them », *LawPRO Magazine Student Issue,* nº 2, 2014, p. 18.

78 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 1.1-1.

Des communications en ligne, comme des commentaires ou des gazouillis, peuvent être interprétées à tort comme une consultation et établir, dans l'esprit du « client », une relation avec l'avocat[79]. Une publication récente de l'American Bar Association traite de ce genre de situations : [TRADUCTION] « En raison du caractère interactif des médias sociaux (solliciter ou formuler des commentaires sur un blogue, prendre part à une discussion sur Twitter ou répondre à des questions d'ordre juridique sur un babillard électronique ou sur la page Facebook d'un cabinet d'avocats, par exemple), le risque d'établir une relation avocat-client par inadvertance est réel, surtout lorsque la personne qui demande des renseignements le fait dans le but de former une telle relation pour obtenir des renseignements sur un problème ou un besoin juridique en particulier[80]. »

Pour éviter cette situation, pensez à faire suivre vos commentaires en ligne d'un avis de dégagement de responsabilité (comme à la section précédente), et à tenir un registre de vos communications pour vous défendre contre toute allégation d'avoir donné des conseils juridiques[81].

Respectez-vous les exigences d'identification du client lorsque vous communiquez uniquement par voie électronique?

Communiquer avec vos clients par voie électronique (courriels ou autres) peut réduire les coûts et les retards, ce qui facilite l'accès à la justice. Malheureusement, des pratiques comme l'usurpation par courriel[82], l'hameçonnage[83] et le harponnage (ou hameçonnage ciblé[84]) peuvent conduire les juristes à divulguer des renseignements confidentiels à un tiers malveillant qui se fait passer pour un client, ce qui peut rendre nécessaire l'adoption de méthodes d'identification (comme les signatures numériques) plus poussées que de simplement se fier à l'adresse dans le champ « expéditeur » des courriels. Lorsque vous offrez des services en ligne, assurez-

---

79 William R. Peterson et Clark E Smith, « Law Firm Websites: An Ethical Minefield », *The Bencher*, 2013.

80 Christina Vassiliou Harvey, Mac R. McCoy et Brook Sneath, « 10 Tips for Avoiding Ethical Lapses When Using Social Media », *Business Law Today,* 2014.

81 Dan Pinnington traite de ces mesures dans son article « The Dangers of Social Networking and How to Avoid Them », *LawPRO Magazine Student Issue,* nº 2, 2014, p. 18.

82 [TRADUCTION] « L'usurpation d'identité est la falsification de l'en-tête d'un courriel pour qu'il semble émaner d'une autre source que son émetteur réel. La supercherie est souvent l'œuvre de polluposteurs, qui modifient l'adresse d'expédition du courriel. » Voir ce billet de 2014 du blogue de Lavasoft : *The Big Three Email Nuisances: Spam, Phishing and Spoofing*.

83 [TRADUCTION] « L'auteur d'un courriel d'hameçonnage cherche à soutirer au destinataire ses renseignements personnels ou l'information sur un de ses comptes afin d'accéder à celui-ci et de commettre un vol d'identité ou de la fraude. » Voir ce billet de 2014 du blogue de Lavasoft : *The Big Three Email Nuisances: Spam, Phishing and Spoofing*.

84 [TRADUCTION] « Au lieu d'envoyer des milliers de courriels aléatoirement en espérant que quelques victimes mordent à l'hameçon, les "harponneurs" ciblent un groupe de gens ayant un point commun – ils travaillent pour la même entreprise, ont un compte à la même banque, sont allés à la même université, magasinent sur les mêmes sites Web, etc. Leurs courriels semblent émaner d'organisations ou de particuliers qui écrivent habituellement aux victimes potentielles, ce qui leur donne une apparence d'autant plus trompeuse. » Consulter : FBI, « Spear Phishers : Angling to Steal Your Financial Info », *FBI.gov,* 2009.

vous de bien connaître et de respecter les règles d'identification et de vérification des clients en vigueur dans votre province ou territoire. Plus particulièrement, vous devez suivre les procédures applicables pour établir l'identité des clients lorsque vous ne les rencontrez pas en personne[85].

Prenez-vous des mesures pour éviter les risques de conflit d'intérêts posés par votre présence en ligne?

Si vous offrez des services en ligne, le caractère plutôt informel des communications et l'utilisation de pseudonymes par de nombreux internautes posent un risque : vous pourriez vous retrouver par inadvertance dans une situation de conflit d'intérêts. Pour atténuer ce risque, prenez des mesures raisonnables pour établir la véritable identité des personnes avec qui vous interagissez et, comme nous l'avons mentionné, portez une attention particulière à l'information que vous diffusez en ligne[86].

Veillez-vous à ce que vos clients puissent vous identifier avec certitude dans vos communications électroniques?

En plus de prendre toutes les mesures raisonnables pour vérifier l'identité de vos clients, vous devez bien vous identifier dans vos communications électroniques[87]. Par exemple, l'article 5.8.2 de la *Ligne directrice en matière de technologies* du Barreau du Haut-Canada[88] stipule que « [l]'avocate ou l'avocat qui émet des observations par le biais de médias électroniques accessibles au grand public devrait inclure son nom, l'adresse postale de son cabinet, le ressort où elle ou il est habilité à exercer le droit et l'adresse électronique d'au moins un avocat ou une avocate responsable du message[89] ».

Fournir ces renseignements limite aussi le risque d'être accusé d'exercer le droit là où vous n'y êtes pas habilité.

---

85 Pour une analyse générale de la question, voyez Bob Tarantino, « Pleased to Meet You: The New 'Know Your Client' Regime », *EnPratique de l'ABC*, 2009. Pour des exemples de procédures particulières aux provinces et territoires, consulter, par exemple : *Client Identification and Verification – Frequently Asked Questions* (Colombie-Britannique); *Client Identification and Verification Flowchart* (Alberta); *Client Identification and Verification – Frequently Asked Questions* (Saskatchewan); *Client Identification and Verification – Frequently Asked Questions* (Manitoba); *Règlement administratif*, no 7.1, par. 23(8) (Ontario); *Nouvelles exigences en matière d'identification et de vérification de l'identité des clients* (Québec); *Some Questions and Answers about the new Client Identification and Verification Regulations* (Nouvelle-Écosse).

86 Dan Pinnington, « The Dangers of Social Networking and How to Avoid Them », *LawPRO Magazine Student Issue,* nº 2, 2014, p. 18.

87 Dan Pinnington, « The Dangers of Social Networking and How to Avoid Them », *LawPRO Magazine Student Issue,* nº 2, 2014, p. 18.

88 Barreau du Haut-Canada, *Technologies*.

89 Barreau du Haut-Canada, *Technologies*.

Prenez-vous des mesures pour éviter d'exercer le droit illégalement dans d'autres provinces ou territoires?

Comme les internautes ont aisément accès à des ressources de partout au pays, et qu'il est possible d'établir une relation avocat-client par inadvertance, offrir des services juridiques en ligne peut mener à l'exercice illégal de la profession[90].

Une façon de se prémunir contre ce risque est d'indiquer où vous êtes habilité à pratiquer le droit à vos clients (actuels et potentiels). Par exemple, la Law Society of Scotland a des règles spécifiant que [TRADUCTION] « [s]i le juriste est établi dans un autre État européen, le client doit être informé que le service sera fourni (par exemple) par un avocat écossais enregistré auprès du barreau d'Athènes, ainsi que de la manière d'accéder à la réglementation de ce barreau. Il est recommandé que tout courriel servant à la prestation de services en ligne (et non simplement à communiquer) contienne ces renseignements ou un lien vers eux[91]. » Les juristes canadiens devraient suivre ces conseils (avec les quelques adaptations qui s'imposent).

Vous assurez-vous que vos clients sont conscients des risques liés à la communication par voie électronique et qu'ils les acceptent?

Bien qu'on les exagère souvent, de nombreux risques sont associés à la communication en ligne avec les clients, surtout par courriels. Ceux-ci peuvent ne jamais arriver à destination, être interceptés par un tiers ou ne pas passer les filtres anti-pourriel.

C'est pourquoi vous devez convenir à l'avance d'utiliser ce moyen de communication avec vos clients[92]. Ceux-ci doivent aussi être avertis que le contrat les liant à un fournisseur de services de messagerie gratuits[93] – ou à leur employeur, s'ils utilisent leur adresse au travail[94], – permet souvent au fournisseur d'accéder à leur correspondance privée. L'utilisation de logiciels de cryptage, bien qu'optionnelle[95], pourrait s'imposer pour les communications de nature délicate[96].

---

90 Plus à ce sujet : Dan Pinnington, The Dangers of Social Networking and How to Avoid Them », *LawPRO Magazine Student Issue,* nº 2, 2014, p. 18; Barreau du Haut-Canada, *Technologies*; William R. Peterson et Clark E Smith, « Law Firm Websites: An Ethical Minefield », *The Bencher*, 2013.

91 Law Society of Scotland, Division B: Electronic Communications, article 4.4

92 Barreau du Québec, *Guide des TI : Gestion et sécurité des technologies de l'information pour l'avocat et son équipe*.

93 Consulter, par exemple, les Conditions d'utilisation de Google s'appliquant à Gmail.

94 Daniel Lublin, *Employee Email and the Attorney-Client Privilege*, 2007.

95 Barreau du Haut-Canada, *Five Questions about Encryption*.

96 Barreau du Haut-Canada, *Technologies*. Pour en lire plus sur le sujet, consulter, par exemple : David J. Bilinsky, « Protect Your Data (from Snoops and others…) », *SlawTips,* 2013; Catherine Sanders Reach, « Easy Encryption for Email – Not an Oxymoron », *Slaw.ca,* 2013; John W. Simek et David G. Ries, « 101: Encryption Made Simple for Lawyers », *Wisconsin Lawyer*, 2013.

Il faut aussi expliquer aux clients qu'envoyer une copie d'un courriel à un tiers peut être interprété comme une renonciation au secret professionnel[97]. Faites d'ailleurs attention lorsque vous répondez à des courriels : certains juristes ont reçu des réprimandes pour s'être trompés d'adresse, ou pour avoir cliqué sur « répondre à tous » au lieu de « répondre » dans un échange qui se devait confidentiel[98].

Vous assurez-vous que vos clients sont conscients des risques liés aux outils de vidéoconférence et qu'ils les acceptent?

Comme dans le cas des courriels, les services de télécommunication tels que Skype intègrent habituellement dans leurs conditions d'utilisation des clauses les autorisant à accéder au contenu des conversations, ce qui va à l'encontre de vos obligations de confidentialité. Les clients peuvent vous en délier, mais seulement s'ils sont conscients des risques et qu'ils les acceptent.

De même, certains outils de téléconférence permettent d'enregistrer les conversations. La règle 7.2-3 du *Code type* de la Fédération des ordres professionnels de juristes du Canada stipule qu'« [u]n juriste ne doit pas se servir d'un appareil quelconque pour enregistrer une conversation avec un client ou un autre juriste, même si la loi lui permet de le faire, sans d'abord aviser l'autre personne[99] ». Déterminez s'il y a des chances que la téléconférence soit enregistrée, auquel cas (toujours dans le respect de la réglementation de votre province ou territoire) veillez à ce que votre client le sache et accepte quand même d'utiliser cette méthode.

Vous pliez-vous à vos obligations en matière de supervision en ligne?

Il peut être tentant, si vous offrez des services en ligne, de déléguer certaines tâches à des membres du personnel de votre cabinet plus technophiles que vous, mais gardez à l'esprit que vous avez l'obligation déontologique de les superviser. La règle 6.1-1 du *Code type* de la Fédération des ordres professionnels de juristes du Canada prévoit ce qui suit : « Un juriste assume toute la responsabilité professionnelle des affaires qui lui sont confiées et doit encadrer directement le personnel et les adjoints à qui il délègue des tâches et des fonctions particulières[100]. » En outre, certaines tâches ne peuvent en aucun cas être déléguées. Par exemple, les

---

97 La situation a rarement été abordée par les tribunaux canadiens, mais la jurisprudence américaine a établi des règles sur l'envoi d'une copie conforme à un tiers et ses conséquences sur le privilège du secret professionnel. Voir Jane T. Davis et Matthew E. Brown, « United States: Protecting The Attorney-Client Privilege In The Digital Age », *Mondaq*, 2012.

98 Par exemple, une avocate du Québec a été reconnue coupable de manquement à la déontologie pour avoir copié l'adresse de tous ses clients dans le champ « destinataire » d'un courriel annonçant le déménagement de son cabinet, divulguant ainsi à tous ses clients l'identité et l'adresse courriel de chacun. Voir *Smith c. Teixeira,* 2009 QCCQ 3402.

99 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 7.2-3.

100 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 6.1-1.

avocats spécialisés en immobilier ne peuvent laisser un tiers accéder aux différents régimes d'enregistrement foncier par l'entremise de leurs justificatifs d'identité[101].

Offrez-vous de l'aide en personne aux clients actuels ou potentiels qui n'ont pas les moyens ou les capacités d'utiliser les solutions technologiques?

Bien qu'offrir des services par voie électronique puisse améliorer l'accès aux services juridiques, cela peut devenir un obstacle pour les clients actuels et potentiels qui n'ont pas les moyens ou les capacités d'utiliser ou de comprendre (littéracie insuffisante[102]) les solutions technologiques. Prévoyez une solution de rechange : offrez de l'aide en personne au client, ou si vos services passent exclusivement par voie électronique, redirigez-le vers un autre juriste qui pourra l'aider.

---

101 Pour en savoir plus, consulter, par exemple : Kathleen Waters, « Want trouble? Let someone access the land registry system using your credentials », *AvoidAClaim*, 2014.

102 [TRADUCTION] « Quarante-deux pour cent des Canadiens de 16 à 65 ans ont de faibles compétences en littératie. » Canadian Literacy and Learning Network, *Literacy Statistics in Canada…*, 2005.

4. Les autres utilisations de la technologie

- ✓ Faites-vous preuve de discernement dans votre utilisation des outils de recherche?
- ✓ Faites-vous preuve de discernement dans votre choix de références en ligne?
- ✓ Êtes-vous poli et courtois dans vos communications électroniques avec les tribunaux et les avocats de la partie adverse?
- ✓ Observez-vous le décorum et les règlements des tribunaux dans votre utilisation de la technologie?
- ✓ Si vous travaillez dans un bureau sans papier, respectez-vous vos obligations déontologiques?

La sécurité, le marketing et les interactions avec les clients (l'offre de services par voie électronique) ne sont pas les seuls aspects de la pratique qui posent de nouveaux dilemmes éthiques liés à la technologie. Voici d'autres situations où son utilisation a des incidences déontologiques.

Faites-vous preuve de discernement dans votre utilisation des outils de recherche?

a) Recherche juridique

Les outils de recherche juridique en ligne comme CanLII, Westlaw ou Quicklaw permettent aux juristes de consulter un répertoire de doctrine et de jurisprudence bien plus vaste qu'il n'était possible il y a seulement quelques décennies. Grâce à eux, vous pouvez mieux vous préparer pour un procès (par exemple), mais attention à ne pas pécher par excès. Si une question de droit se défend à l'aide d'une ou deux références, résistez à la tentation de l'étayer d'une douzaine de cas supplémentaires.

L'abondance de solutions trouvables en ligne oblige les juristes à faire preuve de discernement lorsqu'ils préparent un plaidoyer, car il faut éviter de faire perdre du temps à la cour, ou de l'argent à leurs clients. Se baser sur une montagne d'arrêts peut être vu comme un signe de rigueur, oui, mais aussi comme une violation du principe de la proportionnalité, qui, selon la Cour suprême du Canada, « peut constituer la pierre d'assise de l'accès au système de justice civile[103] ».

Faites-vous preuve de discernement dans votre choix de références en ligne?

Pour les documents trouvés ailleurs sur le Web, il faut garder à l'esprit que « la facilité avec laquelle on peut y déposer des textes impose au lecteur la plus grande prudence, surtout lorsqu'il s'agit d'utiliser cette information en preuve devant un tribunal[104] ». Ne recourez pas à des sources douteuses ou infondées, et sachez que les Wikipédia et consorts, qui peuvent facilement être modifiés par des parties intéressées, ne doivent être utilisés qu'avec parcimonie, et seulement lorsque leurs articles paraissent fiables et solidement documentés.

---

103 *Hryniak c. Mauldin*, [2014] 1 RCS 87, para 30 et 31.

104 Bélec et Groupe Domotec inc., [2004] AZ-50253111 (C.L.P.), para 53.

Êtes-vous poli et courtois dans vos communications électroniques avec les avocats de la partie adverse?

b) Communication avec les avocats de la partie adverse

La vitesse et la facilité des communications en ligne font parfois oublier que les règles de courtoisie s'appliquent toujours. La règle 7.2-1 du *Code type* de la Fédération des ordres professionnels de juristes du Canada stipule qu'« [u]n juriste doit être courtois et poli et agir de bonne foi envers toutes les personnes avec qui il traite dans l'exercice de ses fonctions[105] ». Apportez le même soin à la rédaction de vos courriels que pour toute autre correspondance, et lorsque c'est possible, donnez-vous un temps de réflexion de quelques heures avant de les envoyer.

À la courtoisie élémentaire s'ajoute l'étiquette en ligne – la « nétiquette » –, qui comprend des règles sur l'envoi de communications. Par exemple, il ne faut marquer un courriel comme « urgent » que s'il est à la fois urgent *et* prioritaire, et éviter d'écrire tout en majuscules, car sur le Web, cela revient à crier[106].

Êtes-vous poli et courtois dans vos communications électroniques avec les tribunaux?

c) Communication avec les tribunaux

La technologie devrait réduire la paperasse, et non pas créer des formalités qui vous font perdre du temps à lire et à classer des documents papier habituellement disponibles – et souvent, déjà reçus – par voie électronique. Puisqu'un des buts de son utilisation est de réduire les délais dans l'appareil judiciaire et de rendre celui-ci plus accessible (et par le fait même, la justice), assurez-vous que le tribunal a besoin de la version papier d'un document avant de le lui faire parvenir. Par ailleurs, les juges se plaignent souvent d'être mis en c. c. dans un échange entre avocats qui ne regarde qu'eux, de recevoir des courriels mal écrits, ou de recevoir des courriels qui n'ont pas été envoyés aux avocats de la partie adverse[107].

L'utilisation des médias sociaux pour interagir avec les juges soulève aussi des questions d'ordre éthique. Comme l'indique un auteur, [TRADUCTION] « sauf si la cour le demande ou l'exige, l'avocat ne doit pas, hors du tribunal, [utiliser les médias sociaux] pour communiquer directement avec un juge à propos d'une cause en instance; communiquer avec un juge au sujet de questions administratives; communiquer avec le juge qui préside au cours d'une audience; ni communiquer avec un juge après une audition et en cours de délibéré[108] ».

---

105 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 7.2-1.

106 Virginia Shea, *Netiquette*, Albion Books, 2004.

107 Le laboratoire de cyberjustice de l'Université de Montréal a recueilli les doléances des juges lors de séminaires pratiques portant sur l'utilisation de la technologie par les avocats.

108 Voyez : Leonard Polsky, « Will you be my learned friend? », *The Lawyers Weekly*, 2014, p. 14; Christina Vassiliou Harvey, Mac R. McCoy et Brook Sneath, « 10 Tips for Avoiding Ethical Lapses When Using Social Media », *Business Law Today,* 2014.

Si vous travaillez dans un bureau sans papier, respectez-vous vos obligations déontologiques?

d) Bureau sans papier

Il y a de nombreux avantages à prendre le virage sans papier. Par exemple :

- Incidence réduite sur l'environnement;
- Gains de productivité (moins de temps perdu à chercher des documents);
- Économies de coûts (espace, papier, impression, entreposage);
- Accès à distance si des mesures de sécurité adéquates sont en place;
- Planification de reprise après incident facilitée[109].

Ces avantages, notamment les gains de productivité et les économies (si vous en faites bénéficier les clients) favorisent également l'accès à la justice. Il est toutefois essentiel que la technologie utilisée et les politiques en place soient adaptées à votre cabinet et qu'elles respectent les lois sur la confidentialité, les codes de déontologie et les lignes directrices sur la sécurité applicables.

Il existe toute une série de ressources présentant des astuces sur l'exploitation d'un cabinet sans papier[110]. Avant de vous lancer, assurez-vous que vous avez une infrastructure adéquate pour garantir la sécurité et la confidentialité des renseignements personnels de vos clients et pour répondre aux exigences en matière de conservation des dossiers de votre province ou territoire. Vous avez l'obligation de prendre soin des biens de vos clients comme le ferait un propriétaire prudent et consciencieux[111], et justement, certains documents devront être conservés dans leur version papier originale.

Enfin, et cela ne se limite pas aux bureaux sans papier : il faut faire attention au versionnage des documents. Établissez des mesures de contrôle pour limiter le risque que deux personnes travaillent chacune sur une version différente d'un même document[112].

---

109 Lawyers' Insurance Association of Nova Scotia, *Going Paperless*.

110 Voir, par exemple : Lawyers' Insurance Association of Nova Scotia, *Going Paperless*; David Bilinsky, « Going Paperless – Techshow Style », *Slawtips,* 2014; Association du Barreau canadien, *Le défi de la durabilité dans les cabinets juridiques de l'ABC*; Adriana Linares, « Paperless in 12 Steps », *Law Technology Today,* 2012; Sheila M. Blackford et Donna S. M. Neff, *Paperless in One Hour for Lawyers*, American Bar Association, Chicago, 2014.

111 Fédération des ordres professionnels de juristes du Canada, *Code type de déontologie professionnelle*, r. 3.5-2.

112 Voir : Patricia J.F. Warsaba, *Electronic Issues for the Commercial Lawyer*, p. 6.

Observez-vous le décorum et les règlements des tribunaux dans votre utilisation de la technologie?

e) Technologie et tribunaux

Même si les tribunaux sont de plus en plus nombreux à se doter d'ordinateurs et d'autres technologies[113], les juristes doivent utiliser ces technologies en veillant à respecter le décorum. Il faut aussi tenir compte des règlements des tribunaux, qui pourraient interdire, par exemple, les iPad et autres technologies permettant d'enregistrer une audience[114]. Même en l'absence de telles restrictions, les audiences ne doivent être enregistrées qu'avec le consentement éclairé de la cour[115].

De plus, comme on l'a souligné dans les *Washington State Access to Justice Technology Principles*, [TRADUCTION] « l'introduction de la technologie [en cour] ou les changements dans son utilisation ne doivent pas réduire l'accès et la participation au système de justice, mais bien, autant que possible, les favoriser[116] ». On revient encore au principe de la proportionnalité, selon lequel une procédure juste et équitable doit aussi être « accessible — soit proportionnée, expéditive et abordable[117] ». Après tout, [TRADUCTION] « [l]e principe dominant du système de justice est l'obtention d'un résultat juste à l'issue d'une procédure équitable menée par des décideurs impartiaux et bien informés. L'appareil judiciaire utilisera et développera la technologie à cette fin, et en rejettera, limitera ou modifiera les utilisations contraires à cet objectif[118]. »

La technologie ne doit pas être utilisée en cour pour impressionner, mais bien pour favoriser l'accès à la justice et éclairer le tribunal dans ses décisions.

---

113 Voir : Jane Bailey, *Digitization of Court Processes in Canada*, 2012.

114 Consulter, par exemple : Cour du Québec, *Lignes directrices concernant l'utilisation des technologies en salle d'audience*; Provincial Court of Alberta, *Electronic and Wireless Devices Policy*. Voyez également *Director of Child and Family Services c. D.M.P. et al.*, 2009 MBQB 193.

115 Consulter, par exemple : Provincial Court of Alberta, *Media Audio Recording Policy*.

116 Washington State Supreme Court, *Washington State Access to Justice Technology Principles*, 2004.

117 *Hryniak c. Mauldin,* [2014] 1 RCS 87, para 28.

118 Washington State Supreme Court, *Washington State Access to Justice Technology Principles*, 2004.