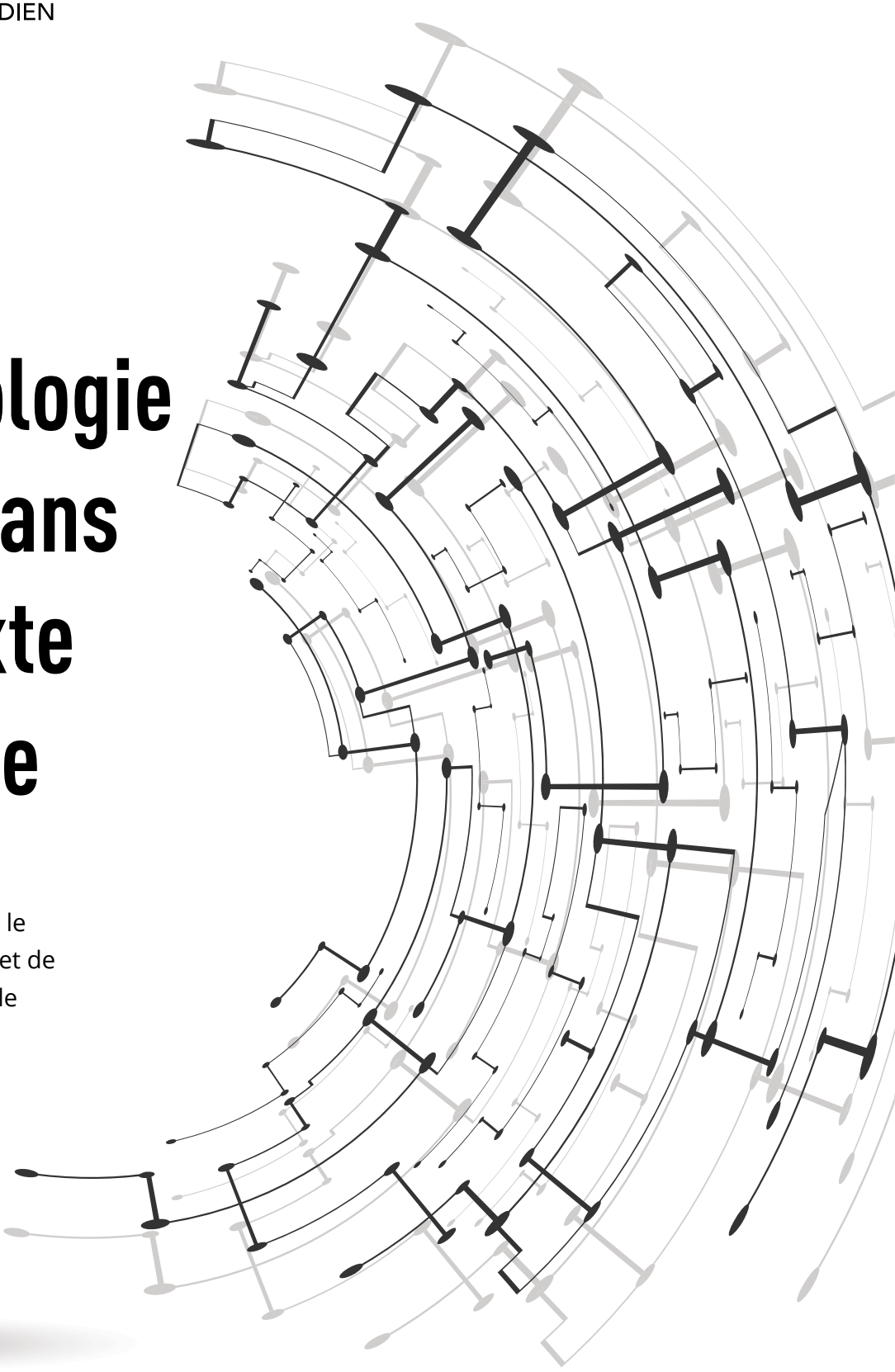
L'ASSOCIATION DU
BARREAU CANADIEN



La déontologie du droit dans un contexte numérique

Préparé par Amy Salyzyn et
Florian Martin-Bariteau pour le
Sous-comité de déontologie et de
responsabilité professionnelle

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], des lignes directrices *Respect de l'éthique : exercer le droit avec l'assistance de la technologie* [2014] et des lignes directrices *La déontologie du droit à l'ère numérique* [2015].

La nouvelle version, du contenu au format, s'inspire des commentaires et suggestions reçus de juristes, de barreaux et d'assureurs à l'automne 2020. Nous désirons également souligner les commentaires utiles reçus sur les premières ébauches à l'hiver 2021, et notamment de Juda Strawczynski, practicePRO; Naomi Horrox et Will Morrison, Barreau de l'Ontario; Glenn Tait, Barreau des Territoires du Nord-Ouest; Barbara Buchanan c.r., Law Society of British Columbia; Darcia Senft, Société du Barreau du Manitoba, Elaine Cumming et le *Code of Professional Conduct Committee*, Nova Scotia Barristers' Society; Michael Joyce et Fyscillia Ream, SERENE-RISC; Yuan Stevens, *Ryerson Leadership Lab/Cybersecure Policy Exchange*; Monica Goyal, Caravel Law; l'Association du Barreau canadien, Sous-comité de l'accès à la justice; ainsi que les juristes à l'emploi de la Law Society of Alberta; la Law Society of Newfoundland and Labrador; et la Direction du droit des technologies de l'information et de la propriété intellectuelle, ministère de la Justice du Québec.

Nous remercions le sous-comité de déontologie et responsabilité professionnelle de l'Association du Barreau canadien: Craig Yamashiro, président, Jennifer Biernaskie, Charles B. Côté, Colin Ouellette et Leslie Walden.

Nous remercions également les boursiers de la Banque Scotia Jacob Racine, Rachael Ostroff et Samarra D'Souza pour leur aide dans la recherche et la correction d'épreuves du document en anglais.

Table des matières

INTRODUCTION 5

Comprendre les obligations déontologiques dans un contexte numérique 6

1. UTILISER LA TECHNOLOGIE POUR FOURNIR DES SERVICES JURIDIQUES EFFICACES, EFFICIENTS ET ÉTHIQUES AUX CLIENTS .. 9

Utilisation de la technologie juridique appropriée 10

Choix de la technologie juridique et diligence raisonnable..... 13

Considérations pour l'accès à la justice 14

Normes d'accessibilité..... 15

2. SAUVEGARDE ET GESTION APPROPRIÉES DES DONNÉES NUMÉRIQUES ET DES ENREGISTREMENTS ÉLECTRONIQUES 16

Sécurité des données..... 19

Fondamentaux du chiffrement 20

Protection des mots de passe 21

Intégrité et accessibilité des données 23

Protection des données dans le temps (sauvegardes).....23

Suppression des donnée..... 24

Stockage et outils de l'infonuagique..... 25

Courriel 27

Confidentialité..... 27

Usurpation d'identité électronique et hameçonnage 28

Pièce jointe malveillante, piratage, logiciels espions et rançongiciels..... 29

Divulgation des métadonnées..... 31

Voyager avec des appareils électroniques..... 32

Services externes de protection des données..... 33

Préparation, intervention en cas d'incident et assurance contre les risques numériques 34

3. TÉLÉTRAVAIL AVEC LES CLIENTS, LES COLLABORATEURS ET LES TRIBUNAUX 35

Bureau virtuel 38

Authentification de signature et attestation à distance 40

Identification et vérification d'identité à distance des clients 42

Réunions, audiences et entrevues à distance 44

Signatures électroniques 46

4. PRÉSENCE EN LIGNE DES JURISTES 47

Accessibilité du contenu Web 49

Règles de commercialisation du barreau 50

Éviter les relations juriste-client involontaires 51

Problèmes déontologiques découlant de l'utilisation des médias sociaux 51

Messages courriel non sollicités et lois antipourriel 54

Introduction

La technologie fait depuis longtemps partie de la pratique juridique. Il y a de nombreuses années, par exemple, les juristes ont commencé à tirer parti de la disponibilité d'outils comme les machines à écrire et les dictaphones pour offrir des services juridiques meilleurs et plus efficaces. Plus tard, l'avènement de la télécopie a donné aux juristes un moyen rapide et relativement sûr de communiquer avec les clients et les tribunaux. L'arrivée des ordinateurs en milieu de travail juridique a apporté encore plus de changements.

Mais beaucoup de choses ont changé en relativement peu de temps. Les juristes se retrouvent désormais à exercer dans un contexte forcément numérique. *La déontologie du droit dans un contexte numérique* traite des nouvelles possibilités et des nouveaux risques auxquels les juristes sont confrontés dans notre contexte numérique actuel, alors que d'immenses quantités de données peuvent être stockées et partagées électroniquement, et que de nouveaux outils émergent continuellement pour habiliter les juristes et leurs clients de manière sans précédent.

L'objectif de ce document est d'aider les juristes à interagir de façon productive et responsable avec la technologie dans leurs pratiques juridiques. Le document présente les domaines présentant des avantages et des risques potentiels, ainsi que des pratiques exemplaires et des ressources supplémentaires.

Le recours à des outils technologiques pertinents n'est plus facultatif pour les juristes canadiens. Comme indiqué dans la section suivante, les règles de déontologie professionnelle exigent implicitement et, dans certains cas, maintenant explicitement que les juristes utilisent la technologie avec compétence.

Outre les règles, la maîtrise des outils technologiques pertinents peut s'avérer nettement avantageuse pour les juristes et les clients. Ainsi, il y a des gains à réaliser en matière d'efficacité et d'efficience. De même, être en mesure de protéger son cabinet et ses clients des risques technologiques est désormais un élément clé d'une pratique prudente et responsable.

Au niveau systémique, l'utilisation appropriée et équitable des outils technologiques par les juristes peut aider à faciliter un accès accru à la justice et à améliorer l'administration de la justice. Cela dit, il faut aussi reconnaître que les outils technologiques ne sont pas également accessibles à tous les juristes et clients. Dans certains cas, l'utilisation ou l'application obligatoire de la technologie peut créer de nouvelles barrières. Le thème de la technologie, de l'accès à la justice et de la prestation de services juridiques nécessite une discussion contextuelle et nuancée.

En général, les renvois à des règles dans le présent document se rapportent au document *Code type de déontologie professionnelle* de la Fédération des ordres professionnels de juristes du Canada. Lors de l'examen de ce document et des suggestions de ressources, les juristes doivent se rappeler que leurs obligations déontologiques et juridiques sont régies par le code de conduite professionnelle, les règles et règlements du barreau et les lois applicables dans leur territoire (les références aux règles du *Code type* ont des hyperliens à sa version interactive qui inclut une référence aux règles équivalentes pour les différents barreaux).

En outre, le contenu de ce document doit être évalué en fonction de son caractère actuel; les changements technologiques et les règles et directives subséquentes du barreau peuvent survenir rapidement. Les juristes sont encouragés à communiquer avec leur ordre professionnel s'ils s'interrogent quant à l'applicabilité réglementaire d'une pratique ou d'une ressource particulière.

Comprendre les obligations déontologiques dans un contexte numérique

Avant de traiter de questions pratiques spécifiques, cette section préalable explique, avec plus de précision, comment la technologie peut recouper les obligations des juristes en vertu des codes de déontologie professionnelle.

Tout d'abord, dans la mesure où la compréhension et l'utilisation de la technologie par un juriste peuvent conduire à une prestation **efficace** de services juridiques, l'obligation pour un juriste de fournir des services juridiques efficaces dans le cadre de la règle 3.2-1 et de la règle 4.1-1 est en cause. En outre, la règle 3.6-1 « Honoraires et débours raisonnables » implique aussi indirectement des pratiques de travail efficaces en prescrivant « [qu']un juriste ne doit pas demander ou accepter des honoraires ou des débours, y compris des intérêts, à moins qu'ils soient justes et raisonnables et qu'ils aient été divulgués en temps opportun ». Les honoraires du juriste peuvent ne pas être considérés comme « justes et raisonnables » si le juriste facture des honoraires plus élevés en raison de l'absence d'utilisation d'une technologie pertinente qui aurait pu générer des gains d'efficacité, ou si le client ne bénéficie pas des économies de coûts résultant de l'utilisation de la technologie.

Deuxièmement, si une technologie est nécessaire pour produire des résultats appropriés pour les clients, l'utilisation de cette technologie implique l'obligation d'un juriste de fournir des services juridiques avec **compétence** en vertu de la règle 3.1-2. Agir en tant que « juriste compétent », tel que défini dans les règles de déontologie professionnelle, comprend également « gérer son cabinet de manière efficace » et « s'adapter aux exigences, aux normes, aux techniques et aux pratiques professionnelles qui pourraient changer » (règle 3.11 [i], et [k]). Notamment, en octobre 2019, la Fédération des ordres

professionnels de juristes du Canada a ajouté le commentaire suivant sur la compétence technologique au *Code type* :

> [4A] Pour conserver le niveau de compétence nécessaire, le juriste doit développer les connaissances et les aptitudes nécessaires pour utiliser la technologie en fonction de son champ d'exercice et de ses responsabilités. Il doit être en mesure d'apprécier les avantages et les risques liés à la technologie pertinente, compte tenu de son obligation d'assurer la protection des renseignements confidentiels exposée à l'article 3.3.
>
> [4B] Le niveau de compétence technologique nécessaire sera fonction du fait que l'utilisation ou la connaissance de la technologie est nécessaire par rapport au champ d'exercice et aux responsabilités du juriste et du fait que la technologie pertinente lui est raisonnablement accessible. Pour déterminer si la technologie pertinente est raisonnablement accessible, il faut tenir compte notamment des facteurs suivants :
>
> a) le champ d'exercice du juriste ou de son cabinet;
>
> b) les endroits où exercent le juriste ou son cabinet;
>
> c) les besoins des clients.

Plusieurs ordres professionnels de juristes provinciaux et territoriaux ont déjà adopté ce commentaire dans leurs codes de déontologie professionnelle, et d'autres suivront probablement. Vous trouverez de plus amples informations sur ce commentaire dans la section « Pour en savoir plus » ci-dessous.

Une obligation de compétence en matière de technologie implique non seulement d'*utiliser* une technologie adaptée à sa pratique et au dossier spécifique du client, mais aussi de *comprendre* la technologie utilisée, y compris ses limites ou ses risques.

Troisièmement, comme le suggère le commentaire ci-dessus, la compréhension et l'utilisation de la technologie par un juriste peuvent toucher son obligation de **protéger les renseignements confidentiels des clients** en vertu de la règle 3.3-1. Si un juriste ne prend pas les mesures appropriées pour protéger ses fichiers numériques des risques de cybersécurité, les renseignements confidentiels des clients et les documents en sa possession peuvent être accessibles de manière inappropriée par des tiers malveillants. Une utilisation incorrecte ou négligente de la technologie peut également entraîner la divulgation involontaire de documents confidentiels.

Quatrièmement, et en lien avec les points ci-dessus, dans certains cas, l'utilisation

appropriée d'une technologie pertinente peut aider les juristes à **satisfaire de manière compétente à leurs autres obligations professionnelles**, telles que :

- l'utilisation d'outils technologiques pour aider à la détection de conflits d'intérêts potentiels (règle 3.4-1);
- la mise en place de précautions techniques appropriées afin de préserver et de protéger de manière appropriée les biens et les fonds des clients (règle 3.5 et les statuts et règlements pertinents du barreau);
- l'utilisation d'outils technologiques pour aider à respecter les obligations en matière de tenue du temps, de tenue des registres et de comptabilité (règle 3.5, règle 3.6 et règlements administratifs pertinents du barreau);
- l'utilisation d'outils de communications électroniques tels que des plateformes de réunions virtuelles, des outils de messagerie numérique et des portails clients pour satisfaire aux obligations de communiquer avec les clients de manière rapide et efficace (règle 3.1-1 [d] et règle 3.1-2);
- l'adoption de pratiques appropriées en matière de commercialisation numérique et de médias sociaux (règle 4.2 et règle 7.2-1).

Cinquièmement, et enfin, l'obligation d'un juriste **d'encourager le respect par le public de l'administration de justice et de s'efforcer d'améliorer l'administration de la justice** en vertu de la règle 5.6-1 suggère également qu'il incombe aux juristes d'être attentifs aux avantages systémiques potentiels (et aux risques) de l'utilisation de la technologie dans le système de justice dans le cadre de leur obligation en tant que champions et gardiens de l'administration juste et équitable de la justice au Canada.

Pour en savoir plus :

- Fédération des ordres professionnels de juristes du Canada, Code type de déontologie professionnelle interactif (novembre 2020).
- Amy Salyzyn, A Taxonomy for Lawyer Technological Competence, *Slaw* (18 décembre 2020).
- Amy Salyzyn, It Finally (Sort of!) Here: A Duty of Technological Competence for Canadian Lawyers, *Slaw* (26 novembre 2019).
- Jason Morris, Duty of Technical Competence: Missing the Point, *Slaw* (10 décembre 2020).
- Law Society of Alberta, Code of Conduct Changes (27 février 2020).

1. Utiliser la technologie pour fournir des services juridiques efficaces, efficients et éthiques aux clients

L'utilisation d'outils technologiques pertinents et appropriés peut se traduire par des services juridiques moins coûteux, plus accessibles et améliorés. La technologie peut également être un outil clé pour satisfaire à d'autres obligations professionnelles, comme éviter d'agir en conflit d'intérêts et se conformer aux exigences de tenue des registres et de comptabilité. Toutefois, lorsqu'il envisage l'utilisation d'une technologie, un juriste doit également être attentif à la possibilité que cette utilisation puisse créer des obstacles pour certains membres du public et prendre des mesures pour atténuer ces obstacles ou fournir un processus ou un mode de prestation alternatif.

Les juristes doivent également faire preuve de diligence raisonnable avant d'adopter toute solution technologique particulière afin de s'assurer que la technologie est fiable et adaptée à leur pratique.

Objectif : La technologie est utilisée de manière optimale pour fournir des services juridiques efficaces, efficients et éthiques.

Vous trouverez ci-dessous un certain nombre des questions à poser dans le cadre de l'évaluation de la conformité, ainsi que les possibles systèmes et pratiques à mettre en œuvre pour parvenir à ladite conformité.

Q: Des outils technologiques ont-ils été adoptés lorsqu'ils conviennent à la tâche?

Déterminer si l'utilisation des types de technologie suivants serait utile et appropriée :

- ✓ Outils de gestion de pratique (p. ex. logiciel de gestion du temps et de facturation, gestion des fichiers, systèmes de vérification des conflits).
- ✓ Outils de gestion et de stockage des documents.
- ✓ Outils de gestion de la relation client (p. ex. portails de communication client, options de paiement en ligne).
- ✓ Logiciels de sécurité.
- ✓ Outils d'accès à distance.
- ✓ Formulaires et documents automatisés.
- ✓ Logiciel de filtrage des listes de sanctions et de surveillance.

Q: Avant d'adopter une technologie, a-t-on appliqué une diligence raisonnable?

Dans la mesure du possible, mener les recherches suivantes avant d'adopter une technologie :

- ✓ Examiner les antécédents du fournisseur (p. ex. depuis combien de temps le fournisseur est en activité, son modèle d'affaires et ses autres clients).
- ✓ Prendre en compte les caractéristiques de sécurité.
- ✓ Examiner le niveau et la nature du soutien continu.
- ✓ Examiner les conditions de service applicables et les risques qui en découlent (y compris, par exemple, si le juriste sera en mesure de conserver la garde et le contrôle des dossiers confidentiels).
- ✓ Passer en revue les conseils de pratique du barreau ou contacter les conseillers en pratique du barreau pour obtenir des conseils généraux.
- ✓ Chercher des recommandations et des informations dans les événements de formation continue et les publications des barreaux.

Q: Les processus technologiques adoptés sont-ils suffisamment inclusifs?

- ✓ Si une technologie est employée, s'assurer que des solutions de rechange adéquates sont en place lorsqu'il y a des obstacles à l'accès pour les clients.
- ✓ Adopter des normes d'accessibilité applicables à l'égard des documents et processus électroniques.

Utilisation de la technologie juridique appropriée

Les juristes doivent se demander s'ils ont adopté des solutions technologiques appropriées pour leur pratique juridique.

L'expression « technologie juridique » est vaste et englobe de nombreux types différents d'outils matériels et numériques. Comme point de départ, disposer du matériel approprié, comme des ordinateurs et des systèmes informatiques fonctionnant correctement, est évidemment essentiel pour fournir des services juridiques compétents et efficients. La nature du matériel qui sera approprié variera considérablement parmi les pratiques juridiques.

Il n'existe pas de liste des technologies juridiques « obligatoires » que les juristes doivent adopter. De plus, comme l'a relevé la Law Society of Alberta, le nouveau commentaire du *Code type* sur la compétence technologique n'exige pas que les juristes achètent les solutions technologiques les plus récentes et les plus coûteuses. En effet, le coût d'un outil technologique par rapport aux avantages potentiels qu'il peut apporter, tels que l'amélioration de la qualité ou les économies, est un facteur important à prendre en compte pour décider d'adopter ou non un outil particulier.

Dans certains contextes, cependant, l'utilisation d'une technologie particulière peut s'imposer en raison de réglementations existantes ou de règles judiciaires. Certains tribunaux, par exemple, imposent maintenant le dépôt électronique. En pratique

immobilière, il peut être nécessaire d'enregistrer électroniquement les biens.

Dans le contexte des litiges, les tribunaux peuvent publier des directives au cas par cas sur la façon dont les juristes devraient utiliser la technologie. Les juristes devront avoir un ensemble de compétences de base et se sentir à l'aise par rapport aux outils technologiques d'usage courant.[1] Bien qu'ils doivent se conformer aux directives du tribunal, les juristes peuvent aussi vouloir suggérer proactivement des technologies particulières lors des étapes de gestion de cas ou précédant l'instruction, aussi simples que la production électronique de précédents et d'autres documents aux tribunaux, lorsque cela peut être plus efficient, et réduire les coûts pour leurs clients, ainsi que d'autres intervenants impliqués dans l'affaire.

En matière pénale, les tribunaux ont jugé que la Couronne a le pouvoir discrétionnaire de divulguer du matériel par voie électronique tant qu'il est raisonnablement accessible.[2] Bien que les tribunaux tiennent compte des circonstances et de l'expertise relative de l'accusé et de son avocat lorsqu'ils détermineront si les preuves électroniques sont « raisonnablement accessibles », les tribunaux attendront également du juriste un niveau minimal de compétence technologique.[3]

Une exigence d'utilisation d'une technologie particulière peut également être déduite de pratiques générales, dans certains cas. Par exemple, dans le cadre d'un litige, il est admis que les juristes doivent effectuer des recherches juridiques à l'aide de bases de données électroniques et peuvent potentiellement s'exposer à des plaintes pour négligence ou à des plaintes auprès du barreau si la qualité des services juridiques qu'ils fournissent est inadéquate en raison du fait qu'ils ne s'appuient que sur des imprimés de sténographes.[4]

---

[1] Voir, p. ex. *Arconti v. Smith*, 2020 ONSC 2782 au paragraphe 33 ([traduction] « en 2020, l'utilisation de technologies facilement disponibles fait partie des *compétences* de base requises pour les plaideurs civils et les tribunaux. Ce n'est pas nouveau et, contrairement à la pandémie, ce n'est pas survenu soudainement. Cependant, la nécessité pour le tribunal de fonctionner pendant la pandémie a mis en évidence la disponibilité de processus alternatifs et l'impératif de compétence technologique. Des efforts peuvent et doivent être faits pour aider les gens encore mal à l'aise à obtenir toute formation et éducation nécessaire. Les parties et les avocats peuvent demander un certain délai pour laisser une partie ou les deux se préparer à faire face à un environnement inconnu. »).

[2] Voir par exemple *R. v. Therrien*, 2005 BCSC 592, aux par. 2728, *R v. Sawchuk*, 2019 ABQB 252 au par. 30, *R. v. Cuffie*, 2020 ONSC 4488 aux par. 2733

[3] Pour les précédents relatifs aux tribunaux adoptant une analyse contextuelle, voir, par exemple, *R. v. Sawchuk*, 2019 ABQB 252 au par. 30 et *R. v. Cuffie*, 2020 ONSC 4488 au par. 32; *R. v. Piaskowski* et al, 2007 MBQB 68 au par. 43. Pour des commentaires judiciaires sur les compétences technologiques minimales, voir, p. ex. *R. v. Oszenaris*, 2008 NLCA 53 au par. 20 (indiquant que [traduction] « dans le monde d'aujourd'hui, il n'est pas déraisonnable de s'attendre à ce que les avocats soient en mesure d'utiliser un ordinateur pour la gestion de gros volumes de matériel ») et *R. v. Beckett*, 2014 BCSC 731 au par. 8 (indiquant que [traduction] « l'absence actuelle de compétences informatiques d'un accusé ou d'un avocat n'est pas un obstacle à la divulgation électronique, si ces compétences peuvent être acquises relativement facilement »).

[4] Voir, p. ex. *Aram Systems Ltd. v. Nov* Atel *Inc*., 2010 ABQB 152 au par. 23 (indiquant que [traduction] « la perception de la recherche juridique informatisée comme simple alternative n'est plus conforme à la réalité de la pratique juridique actuelle. Ces recherches sont maintenant attendues des avocats, tant par leurs clients, qui se tournent vers les avocats pour présenter le meilleur dossier possible, que par les tribunaux, qui comptent sur les avocats pour présenter les précédents les plus pertinents. En effet, il pourrait

Plus récemment, les tribunaux ont également suggéré que les outils de recherche juridique fondés sur l'IA peuvent être un moyen pour un juriste de réduire les coûts lorsqu'il agit sur un dossier de litige.[5]

En outre, les règles des codes de déontologie professionnelles peuvent suggérer indirectement l'utilisation d'outils technologiques appropriés. Par exemple, alors que pratiquement tous les juristes peuvent déjà être joints par leurs clients par téléphone et par courriel, les juristes devraient se demander si l'utilisation d'outils de communication numériques supplémentaires, comme des services de messagerie privée ou des portails de communication client, aiderait aux communications opportunes et appropriées aux clients (règle 3.1-1 [d] et règle 3.1-2). Toutefois, dans l'utilisation d'outils de communication numérique supplémentaires, les juristes doivent veiller à ce que toutes les communications, quelle que soit la plateforme, soient correctement incluses dans le dossier client et que des mesures de sécurité adéquates soient prises *(les problèmes de sécurité des données sont abordés à la Section 2, Sauvegarde et gestion appropriées des données numériques et des dossiers électroniques).*

Les juristes peuvent envisager l'automatisation comme un moyen de faciliter des services juridiques plus efficaces et améliorés pour leurs clients (règle 3.1-1, règle 3.2-1 et règle 3.6-1). De fait, l'adoption de procédés automatisés bénéficie tant aux juristes qu'à leurs clients. En automatisant des tâches administratives, les juristes peuvent libérer du temps pour se concentrer sur un travail juridique plus substantiel qui sera probablement plus gratifiant tant psychologiquement que financièrement. Dans certains cas, les processus automatisés peuvent également réduire les possibilités d'erreur humaine; par exemple, si un logiciel de gestion de cabinet remplit automatiquement les renseignements personnels d'un client dans plusieurs parties du système de gestion de l'information d'un cabinet, cela peut éviter des erreurs comme l'entrée inexacte du nom ou du numéro de téléphone d'un client. Les principaux domaines à prendre en compte pour l'automatisation comprennent la gestion de la pratique (par exemple, inscription des nouveaux clients et facturation) et la création de documents. En parallèle, les juristes doivent garder à l'esprit que les outils de traitement des données en infonuagique (de l'assistance à la révision jusqu'à l'analyse) peuvent présenter des préoccupations quant à la confidentialité des renseignements des clients.

Enfin, les juristes devraient examiner comment la technologie peut les aider à se conformer à leur obligation d'éviter d'agir en cas de conflit d'intérêts et de respecter

être soutenu qu'un avocat qui choisit de renoncer à la recherche juridique informatisée est négligent à cet égard… La pratique du droit a évolué au point où la recherche juridique informatisée n'est plus une question de choix. »)

[5] Voir, p. ex. *Cass v. 1410088 Ontario Inc.*, 2018 ONSC 6959 au par. 34 (indiquant [traduction] qu'« il n'était pas nécessaire de procéder à des recherches extérieures ou de tiers. Si des sources d'intelligence artificielle étaient employées, il ne fait aucun doute que le temps de préparation des avocats aurait été considérablement réduit. »)

d'autres obligations en matière de conformité. Par exemple, le passage à un système informatisé de vérification des conflits de la base de données constitue généralement une amélioration par rapport au système papier, car il peut permettre une saisie et une récupération rapides des données et peut également mieux gérer et analyser de grandes quantités d'informations. De même, il est généralement recommandé que les juristes utilisent des systèmes financiers électroniques pour aider à se conformer aux exigences de tenue de registres et de comptabilité. Dans certains cas, les juristes peuvent vouloir utiliser des outils technologiques pour aider à filtrer les clients relativement aux règlements sur les sanctions et à surveiller les listes qui interdisent ou restreignent les relations avec des personnes ou entités spécifiques.

Pour en savoir plus :

- Michelle Wong, A Beginner's Guide to Law Office Automation, *Clio* (dernière mise à jour en 2021).
- Heidi Alexander, The Advantages of Automation: Experienced Practitioners Discuss their Successful Solutions for Automating Their Practice, ABA (1er janvier 2020).
- Barreau de l'Ontario, Lignes directrices sur la gestion d'un cabinet juridique : Technologies (dernière mise à jour 2020).
- Association du Barreau canadien, Trousse de documents modèles sur les conflits d'intérêts(2020).
- Sharon D. Nelson, John Simek et Michael Maschke, The 2020 Solo and Small Firm Legal Technology Guide (ABA Book Publishing, 2019).

Choix de la technologie juridique et diligence raisonnable

Les technologies juridiques ne conviennent pas toutes à chaque pratique juridique. En outre, bien que de nombreuses technologies juridiques disponibles sur le marché, sinon la plupart, proviennent de fournisseurs réputés, tous les outils ne sont pas nécessairement de la même qualité ou ne fournissent pas les mêmes protections pour les données des juristes et des clients. Il n'existe pas de liste faisant autorité de technologies juridiques « approuvées » auxquelles les juristes canadiens peuvent se référer. Par conséquent, les juristes doivent s'assurer qu'ils exercent une diligence raisonnable appropriée, notamment en s'informant des antécédents du fournisseur ainsi que des caractéristiques de sécurité et de l'assistance fournies. Avant d'adopter une technologie, les juristes devraient également examiner les modalités de service applicables et tenir compte des risques qui en découlent.

Lorsqu'ils décident de l'utilisation d'un outil technologique, les juristes peuvent souhaiter consulter le matériel de conseil de leur barreau ou contacter les conseillers en pratique de leur barreau pour obtenir des conseils sur l'utilisation des technologies. Cependant, les barreaux canadiens n'approuvent généralement pas ou ne préconisent pas autrement l'utilisation par les juristes d'un outil technologique particulier.[6] De plus en plus, les événements de formation continue et les publications des barreaux contiennent des renseignements utiles sur des outils technologiques spécifiques et peuvent constituer de bonnes ressources de référence pour les juristes. La compatibilité des outils technologiques avec d'autres juristes et cabinets juridiques exerçant dans le même domaine est également un facteur important à prendre en compte, lorsque la compatibilité des outils constitue un facteur pertinent (par exemple, les plateformes de vidéoconférence).

Pour en savoir plus :

- Nicole Black, Vetting Legal Technology and Software: 3 Tips from the Experts, *My Case* (dernière mise à jour en 2021).
- Derek Bolen, What Technology Does Your Law Firm Actually Need?, *Clio* (dernière mise à jour en 2021).
- LawPro, Technology Products for Lawyers and Law Firms, *PracticePRO* (mis à jour en novembre 2020).
- Sharon D. Nelson, John Simek et Michael Maschke, The 2020 Solo and Small Firm Legal Technology Guide (ABA Book Publishing, 2019).

Considérations pour l'accès à la justice

Il y a eu une augmentation significative de l'utilisation de la technologie dans la pratique juridique et au tribunal. Dans certains cas, l'utilisation de la technologie dans la prestation de services juridiques peut améliorer l'accès véritable à la justice. Par exemple, si l'automatisation sert à réduire le coût de traitement des affaires des clients, ces économies peuvent se traduire par une réduction des honoraires pour les clients. Autre exemple, certains clients peuvent trouver l'utilisation d'un portail de communication plus facile et qu'il leur fournit des informations plus significatives sur l'état de leur affaire, au lieu d'appeler leur juriste ou de lui envoyer un courriel.

En revanche, les juristes doivent faire preuve de prudence, en particulier en ce qui

[6] La Law Society of British Columbia fait exception, prévoyant dans ses *Law Society Rules*, règle 10(3)(5), qu'elle peut déclarer que les avocats ne sont pas autorisés à utiliser un « fournisseur de stockage » particulier (y compris un fournisseur de stockage en infonuagique).

concerne l'utilisation de technologies en interaction avec les clients, afin de ne pas introduire involontairement de nouvelles barrières à l'accès. Les clients établis ou potentiels n'auront pas tous un accès fiable à Internet. Il existe des problèmes bien documentés d'accès inadéquat à la connectivité Internet dans les collectivités nordiques, rurales et éloignées du Canada. De plus, les contraintes financières peuvent avoir un impact sur la capacité d'une personne à se permettre un accès adéquat à Internet dans son foyer ou au matériel nécessaire (par exemple, ordinateurs, tablettes et téléphones intelligents) pour utiliser les technologies d'interaction avec le client. Certains clients peuvent ne pas être suffisamment « technologiquement instruits » ou à l'aise avec tous les outils technologiques qu'un juriste pourrait utiliser. Pour ces clients, il peut être important de disposer de processus alternatifs.

Bien que les fonctions des juristes relèvent principalement de leurs clients, ils ont également des obligations en matière d'amélioration de l'administration de la justice en général et doivent tenir compte des implications de leurs choix vis-à-vis d'autres intervenants du système de justice (règle 5.6-1). Plutôt que d'accroître l'accès à la justice, l'utilisation de la technologie peut créer des obstacles pour les parties adverses, en particulier pour les plaideurs non représentés et les communautés marginalisées. Bien que les juristes puissent vouloir recommander au tribunal des technologies plus efficaces, ils devraient aussi rejeter, réduire ou modifier toute utilisation de la technologie qui pourrait entraver le système de justice équitable et abordable pour les Canadiens.

Pour en savoir plus :

- Jena McGill, Amy Salyzyn, Suzanne Bouclin et Karin Galldin, Emerging Technological Solutions to Access to Justice Problems : Opportunities and Risks of Mobile and WebBased Apps (13 octobre 2016).

Normes d'accessibilité

Les juristes doivent également veiller à ce que les documents et les communications soient accessibles aux personnes handicapées, qu'il s'agisse de collègues, de clients ou de recrues potentiels. Ainsi, certains clients peuvent demander ou exiger un mode de communication spécifique en raison d'un handicap.[7] Les règles du barreau reconnaissent qu'un juriste est « particulièrement tenu » de respecter les lois relatives aux droits de la personne (règle 6.3-1, commentaire [1]). Les normes d'accessibilité, particulièrement en ce qui concerne les documents électroniques, diffèrent d'une province à l'autre. Vous devez

[7] ARCH Disability Law Centre, Fiche d'information - conseil pour avocats et parajuristes en Ontario: mesures d'adaptation pour les clients au moyen de communication par courriel (1er octobre 2019)

connaître les normes applicables et évaluer votre conformité *(les problèmes d'accessibilité au Web sont abordés cidessous à la Section 4, « Présence en ligne des avocats ».)*. Lorsque cela est possible et pertinent, les juristes doivent également envisager d'adopter des approches de conception inclusives ou « universelles », qui mettent l'accent sur la conception de processus ou de documents dans une optique d'inclusion dès le départ, plutôt que d'éliminer les obstacles de manière réactive ou de prendre des mesures d'adaptation individuelles.

Pour en savoir plus :

- Vers l'accessibilité, *Module sur la norme d'accessibilité de l'information et des communications* (dernière consultation le 29 janvier 2021).
- Gouvernement du Canada, *Boîte à outils d'accessibilité numérique* (dernière mise à jour le 12 septembre 2020).
- ARCH Disability Law Centre, *Tips for Lawyers and Paralegals on Providing Accessible Legal Services to Persons with Disabilities in Ontario* (janvier 2019)
- Commission ontarienne des droits de la personne, *Politique sur le capacitisme et la discrimination fondée sur le handicap* (2016)

2. Sauvegarde et gestion appropriées des données numériques et des enregistrements électroniques

Les juristes ont l'obligation déontologique de protéger les informations confidentielles des clients et de protéger les biens des clients en leur possession, y compris les fonds des clients. Les juristes sont également tenus de respecter les lois sur la protection de la vie privée dans la gestion de leurs pratiques. Les risques technologiques, qu'ils soient d'origine malveillante ou bénigne, peuvent entraver les efforts des juristes pour s'acquitter de ces obligations et, dans certains cas, entraîner des violations de la déontologie ou de la réglementation. De telles violations peuvent avoir des conséquences négatives sur le plan financier et sur la réputation des juristes. En étant conscients des risques technologiques et en prenant des mesures pour s'en protéger, les juristes peuvent se prémunir contre de telles conséquences négatives et garantir aux clients actuels (et potentiels) que leurs renseignements et leurs biens seront correctement gardés et sécurisés.

Alors que la pratique juridique évolue de plus en plus vers la numérisation, il est important que les juristes comprennent les principaux risques liés à la sécurité et à la protection des

renseignements personnels et adoptent de solides pratiques en matière de cybersécurité. Pour les juristes moins familiers avec la technologie, de nombreuses ressources sont à leur disposition afin de mieux comprendre ces concepts. Des chercheurs canadiens de premier plan en matière de cybersécurité ont notamment développé des modules de formation en ligne gratuits, avec des vidéos, des lexiques, ainsi que des aide-mémoire et des documents, disponibles sur le site **www.cybersec101.ca**. Ces ressources pourraient également être utiles aux cabinets juridiques pour fournir une formation essentielle en cybersécurité à tous les membres de leur organisation.

Objectif : Les données numériques et les documents électroniques sont protégés et gérés de manière appropriée.

Vous trouverez ci-dessous un certain nombre des questions à poser dans le cadre de l'évaluation de la conformité, ainsi que les possibles systèmes et pratiques à mettre en œuvre pour parvenir à ladite conformité.

Q: Des mesures de sécurité appropriées ont-elles été adoptées?

Envisager de munir tous les appareils numériques des éléments suivants :

- ✓ Protection par mot de passe.
- ✓ Chiffrement intégral du disque dur.
- ✓ Pare feu.
- ✓ Logiciel antivirus/anti maliciel, et logiciel de détection d'intrusion.
- ✓ Solutions de chiffrement pour l'envoi de renseignements sensibles.
- ✓ Logiciel de localisation du dispositif, avec capacité d'effacement à distance.

Veiller à garder à jour en permanence :

- ✓ Systèmes d'exploitation de tous les appareils, des serveurs aux routeurs en passant par les téléphones intelligents (si possible, automatiser les mises à jour de sécurité).
- ✓ Tous les logiciels tiers, des antivirus et pare feu à la gestion de bureau en passant par le traitement de texte.

Veiller à ce que tous les individus prennent de bonnes précautions pour les mots de passe :

- ✓ Les mots de passe ne sont pas partagés ou divulgués.
- ✓ Utilisation de mots de passe robustes et uniques.
- ✓ Utilisation de gestionnaires de mots de passe le cas échéant.
- ✓ Authentification en deux étapes ou Multi facteurs.

Q: Des mesures appropriées ont-elles été adoptées pour surveiller l'intégrité des données collectées ou détenues?

Envisager d'utiliser les outils suivants pour garantir l'intégrité des données :

- ✓ Signatures numériques.
- ✓ Politiques d'archivage.
- ✓ Comparaison des métadonnées.
- ✓ S'assurer que les documents sont sauvegardés afin qu'un fichier corrompu puisse être remplacé par une copie intacte.

Q: Les données demeurent-elles adéquatement accessibles avec le temps?

S'assurer que les pratiques de sauvegarde appropriées sont respectées :

- ✓ Disposer d'un plan de sauvegarde et de reprise d'activité pour l'ensemble des données.
- ✓ Maintenir plusieurs sauvegardes.
- ✓ Envisager d'utiliser un processus de sauvegarde automatisé.
- ✓ Décaler et séparer les sauvegardes du reste du réseau.

Q: Des pratiques appropriées ont-elles été adoptées en matière de suppression des données?

Veiller à la suppression des données dans le respect des obligations professionnelles :

- ✓ Avant de supprimer des données, s'assurer que la suppression proposée est conforme aux obligations de conservation des dossiers.
- ✓ Lors de la suppression de données, s'assurer de respecter les obligations de confidentialité du client (cela nécessite de comprendre comment supprimer correctement les données d'un appareil numérique).

Q: L'utilisation du stockage et des outils en infonuagique a-t-elle été envisagée?

Tenir compte des avantages potentiels des solutions basées sur l'infonuagique :

- ✓ Accès à des applications et services logiciels nouveaux.
- ✓ Maintenance matérielle et logicielle externalisée.
- ✓ Accès virtuel facile aux données.
- ✓ Sauvegarde automatisée des données.

Si vous envisagez une solution infonuagique, exercer une diligence raisonnable appropriée :

- ✓ Consulter la liste de contrôle *Cloud Computing Checklist* de la Law Society of British Columbia (noter les modifications nécessaires compte tenu du territoire dans

lequel vous exercez).

Q: Est-on suffisamment sensibilisé aux risques liés à la sécurité des données et préparé en cas d'exposition à une attaque ou à un événement naturel?

Élaborer un cadre de gestion de la sécurité de l'information, incluant ce qui suit :

- ✓ Politique de sécurité de l'information.
- ✓ Politique de confidentialité.
- ✓ Plan d'intervention en cas d'incident.
- ✓ Plan de formation en sécurité des données afin que toutes les personnes travaillant dans l'organisation reçoivent une éducation continue concernant les cybermenaces, y compris la gestion des renseignements sensibles, l'hameçonnage, les rançongiciels et les précautions de protection des mots de passe.
- ✓ Assurance contre la cybercriminalité/risque numérique.

Q: Est-ce que l'on comprend suffisamment les métadonnées et comment se prémunir contre leur divulgation inappropriée?

- ✓ Des mesures doivent être prises pour minimiser la création de métadonnées ou pour les effacer des fichiers ou documents envoyés sur une plateforme Web (sauf lorsqu'il existe une obligation légale de conserver et de divulguer des métadonnées, p. ex. des obligations de communication préalable).
- ✓ Comprendre quand les métadonnées intégrées dans un courriel ou un message sur les réseaux sociaux peuvent contenir des informations de localisation et prendre les mesures nécessaires pour éviter de divulguer des données localisées lorsqu'il s'agit de renseignements sensibles.

Q: A-t-on adopté des pratiques exemplaires lorsque des appareils électroniques traversent les frontières?

- ✓ Consulter les documents d'orientation préparés par l'ABC et la FOPJC sur la question des déplacements transfrontaliers avec des appareils électroniques.

Sécurité des données

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 » (règle 3.3-1). Les juristes doivent également respecter les règles de confidentialité et de sécurité de l'information pour les intervenants du secteur privé sur la manière de gérer correctement l'information et de se conformer à leurs obligations de déclaration en cas d'atteinte à

la protection des données. Cela implique une obligation sous-jacente d'adopter des mesures de sécurité pour protéger ces données (p. ex. localisation des appareils, pare-feu et logiciel de détection des intrusions, également appelé logiciel de détection et de réponse des terminaux). Les cabinets juridiques devraient également adopter des mesures organisationnelles, notamment fournir des renseignements pertinents et de la formation aux membres de leur organisation.

Des mesures de sécurité doivent être implantées pour se prémunir contre l'accès de tiers aux données confidentielles pendant leur cycle de vie. Cela implique que les renseignements doivent être protégés depuis leur création jusqu'à leur destruction, et à chaque phase intermédiaire.

Tout comme il est essentiel que les juristes prennent des mesures pour contrôler et restreindre l'accès aux dossiers matériels (comme l'application de mesures de sécurité relatives aux bureaux et aux classeurs), des mesures doivent également être prises pour contrôler et restreindre l'accès aux renseignements numériques. À ce titre, les juristes doivent activer la protection par mot de passe sur tous leurs appareils et équiper tous leurs appareils électroniques de logiciels de sécurité appropriés, y compris des pare-feu et des logiciels antivirus/antimaliciel, et veiller à les mettre à jour régulièrement. Tous les appareils électroniques doivent être contrôlés au moyen de systèmes de localisation (p. ex. application « Localiser ») permettant d'obtenir des informations d'urgence sur des écrans verrouillés et d'effacer l'appareil à distance s'il est perdu ou volé.

Pour protéger les renseignements des clients, l'accès à tous les appareils électroniques et à toutes les données sur les disques durs ou les disques partagés doit être restreint par un accès contrôlé (p. ex. mots de passe) et selon le principe de l'accès sélectif. De même, tout appareil électronique devrait être chiffré, de préférence par chiffrement intégral du disque, ainsi que toutes les données sur les disques durs, les disques partagés ou les disques externes (p. ex. clé USB).

Lorsque vous naviguez sur Internet, assurez-vous de consulter ou de saisir des renseignements sensibles (p. ex. paiements en ligne) uniquement sur des sites Web sécurisés acheminés par connexion HTTPS,[8] afin qu'aucun tiers ne puisse intercepter illicitement votre trafic Internet.

Fondamentaux du chiffrement

Les atteintes à la protection des données sont devenues monnaie courante. Les acteurs

[8] La plupart des navigateurs affichent un cadenas à côté de l'adresse de la page Web dans la barre d'adresse pour signaler que la page Web est alimentée par une connexion sécurisée. Vous pouvez également lire l'adresse pour vous assurer qu'elle commence par « https:// » plutôt que par « http:// ».

malveillants peuvent non seulement obtenir des renseignements confidentiels sur des affaires de clients antérieurs et courants, mais également voler des renseignements personnels sensibles de votre client (p. ex. date de naissance, informations bancaires, coordonnées). Pour limiter l'impact d'une atteinte à la protection des données ou d'une interception de données, tous les juristes doivent posséder au moins une compréhension générale du chiffrement. Ils doivent disposer de solutions de chiffrement à utiliser le cas échéant et prendre des décisions éclairées sur les occasions où elles doivent être utilisées et celles où l'on peut s'en dispenser. En règle générale, toutes les données doivent être stockées de manière chiffrée et les courriels contenant des renseignements confidentiels ou sensibles doivent être envoyés chiffrés.

Lors de l'examen des solutions et de leurs pratiques, les juristes doivent s'assurer que les données contenant des renseignements sensibles sont chiffrées à la fois *en stockage* et *en transit*. Les données doivent être chiffrées en stockage, c'est-à-dire stockées avec chiffrement intégral sur vos disques durs ou services d'infonuagique, de sorte qu'un tiers pouvant accéder au système de stockage ne serait pas en mesure de les lire. Les données doivent également être chiffrées de bout en bout pendant leur transit, c'est-à-dire pendant leur transmission entre votre appareil et un autre, soit vers un service d'infonuagique, soit vers une autre boîte aux lettres, de sorte qu'un tiers qui pourrait tenter d'intercepter le trafic Internet ne puisse pas les lire.

Protection des mots de passe

Même le chiffrement et le système sécurisé les plus robustes peuvent être pris en défaut s'il n'y a pas une bonne protection de mot de passe par les utilisateurs autorisés. Pour assurer la sécurité des données, il est essentiel que les juristes maintiennent une bonne protection des mots de passe. En effet, les mauvaises habitudes en matière de mots de passe (p. ex. le partage ou la réutilisation de mots de passe, l'utilisation d'informations personnelles, l'utilisation de mots de passe simples tels que « 1234 » ou « mot de passe », ou le maintien des mots de passe par défaut) sont souvent l'un des maillons les plus faibles des pratiques de sécurité des données.

Les identifiants ne doivent jamais être partagés et divulgués, même en interne, afin de garantir la séparation des utilisateurs en cas de cyberattaque et de permettre la révocation rapide de l'accès lorsqu'une personne quitte une organisation. Les mots de passe ne doivent pas être écrits de manière à être facilement visibles, sur papier (p. ex. une note sur votre écran ou à proximité) ou même enregistrés sur votre ordinateur.

Sans que cette pratique élimine tous les risques liés aux mots de passe, les juristes devraient envisager le recours à des gestionnaires de mots de passe qui génèrent des

mots de passe uniques créés aléatoirement et les stockent dans un lieu unique et sécurisé. La plupart des gestionnaires produisent également des alertes en cas de réutilisation des mots de passe ou si certaines plateformes présentent des risques de sécurité connus. Vous ne devez mémoriser qu'un seul mot de passe pour accéder à l'application. Cela signifie, bien sûr, qu'il faut être extrêmement prudent dans le choix et la protection de ce mot de passe maître.

Les juristes devraient utiliser une authentification en deux étapes (également appelée authentification à facteurs multiples) le cas échéant. En plus de votre mot de passe, vous aurez besoin d'un second jeton pour être authentifié (p. ex. un code généré par une application sur votre téléphone, ou un code généré par un jeton matériel, ou une empreinte digitale). Il est recommandé d'éviter d'utiliser les codes envoyés par SMS mobile pour les systèmes sensibles, car le piratage et l'échange de carte SIM sont de plus en plus fréquents.

Si un juriste soupçonne qu'il a été piraté, il devrait changer son mot de passe immédiatement et inspecter l'activité récente sur son système ou son compte. Le juriste devrait également s'assurer qu'il respecte les obligations de signalement *(voir ci-dessous la section intitulée « Préparation, intervention en cas d'incident et assurance contre les risques numériques »).*

Pour en savoir plus :

- Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de base pour les petites et moyennes organisations* (février 2020).
- LawPRO, Cybersecurity and Fraud Prevention Tip *PracticePRO* (2021*)*
- Derek Bolen, What Lawyers Need to Know about Encryption, *Clio* (dernière mise à jour en 2021).
- Lawyers Insurance Association of Nova Scotia, Data Security (dernière mise à jour en 2021).
- Barreau de l'Ontario, Lignes directrices sur la gestion d'un cabinet juridique : Technologies (dernière mise à jour 2020).
- Matt Burges, How to Know If You've Been Hacked, and What to Do About it, *Wired* (19 juillet 2020).
- Serene Risc, Cybersecurity Tips (dernière mise à jour en 2019).
- LawPro, Fraud Fact Sheet: Cybercrime and Bad Cheque Scams *PracticePRO (2018)*.
- LawPRO, Encryption Made Simple for Lawyers, *PracticePRO*

(15 décembre 2017).

- Barreau du Québec, *Guide des TI* (2016).
- Commissariat à la protection de la vie privée du Canada, La LPRPDE et votre pratique juridique (dernière modification en 2015).

Intégrité et accessibilité des données

Les juristes doivent garantir l'intégrité et l'accessibilité des documents et données de leurs dossiers.

Afin de garantir l'intégrité des données, les juristes doivent prendre des mesures pour se prémunir contre la modification, l'altération ou la destruction, intentionnelle ou non, de leurs données. Cela peut se faire au moyen de signatures numériques, de politiques d'archivage, de comparaisons de métadonnées et en s'assurant que les documents sont sauvegardés afin qu'un fichier corrompu puisse être remplacé par une copie intacte.

Les juristes doivent également veiller à ce que leurs données soient accessibles à tout moment et dans la durée. L'accès significatif aux données exige que les renseignements et les fichiers soient intelligibles pour la personne qui en a besoin. Cela implique que la personne a accès au logiciel nécessaire pour lire un fichier donné (p. ex. un fichier créé avec une ancienne version ou une version différente d'un logiciel de traitement de texte comme WordPerfect). Lorsque cela est possible et compatible avec les règles d'intégrité des données, l'accessibilité à long terme peut exiger des juristes qu'ils envisagent une sauvegarde dans un format ouvert (c'est-à-dire non soumis à une licence ou à l'utilisation d'un logiciel propriétaire) et multi plateforme.

Non seulement il s'agit d'assurer l'intégrité et l'accessibilité des données nécessaires dans plusieurs cadres réglementaires et statutaires, mais c'est le principe fondamental des obligations d'un juriste en matière de compétence et de qualité de service, ce qui inclut la gestion efficace du cabinet et fournir au client des informations pertinentes complètes et précises sur une affaire (règle 3.1-1 [d] et [i] et règle 3.2-1, commentaire [5]). Des données inaccessibles, incomplètes ou corrompues peuvent conduire un juriste à donner des renseignements ou des conseils inexacts à un client ou à d'autres tiers auxquels il pourrait être tenu de fournir de l'information. Par exemple, des données altérées peuvent entrer en conflit avec l'obligation d'un juriste de répondre rapidement et complètement aux demandes d'information et de documents émanant de son barreau (règle 7.1-1).

Protection des données dans le temps (sauvegardes)

Les juristes doivent être conscients des risques liés à la perte potentielle de données

et se prémunir contre ces risques. Par exemple, un disque dur matériel peut devenir inaccessible et des données peuvent être perdues. Cela peut se produire pour de nombreuses raisons, y compris les cyberattaques, mais plus probablement en raison de causes non malveillantes allant de l'absence de maintenance de serveur, de pannes d'électricité, de dégâts d'eau ou de vieux disques durs qui limitent l'accès aux fichiers informatisés.

La sauvegarde des fichiers est une composante nécessaire et essentielle d'une gestion compétente des données et des fichiers. Les juristes devraient disposer de plans de sauvegarde et de reprise après sinistre pour toutes les données qu'ils gèrent et doivent conserver, que ce soit du point de vue de la gestion du cabinet ou conformément à la loi. Il est recommandé que les juristes disposent de plusieurs sauvegardes, et que le processus de sauvegarde soit automatisé, si possible, en temps réel. Il est recommandé d'échelonner vos sauvegardes et de conserver plusieurs versions différentes de la sauvegarde, chacune sauvegardée à différents moments, et de vérifier régulièrement que les données de sauvegarde peuvent être restaurées.

Les sauvegardes complètes devraient être séparées du reste du réseau. Si vos sauvegardes sont connectées à votre système, elles sont soumises aux mêmes risques de perte de données que les autres ordinateurs de votre réseau. Bien qu'une sauvegarde automatisée puisse se trouver sur le même réseau, une sauvegarde complète doit être régulièrement déplacée hors réseau (« isolement physique »), si possible, vers un emplacement sécurisé hors site (notamment pour réduire les risques en cas d'intrusion physique ou de dommage dans votre lieu de travail principal). Dans tous les cas, votre sauvegarde doit également être chiffrée intégralement.

Pour en savoir plus :

- Barreau de l'Ontario, Technologies (dernière mise à jour en 2020).
- LawPath, Data Integrity: Why Does It Matter for Businesses? (3 novembre 2020).
- Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de base pour les petites et moyennes organisations* (février 2020).
- Barreau du Québec, *Guide des TI* (2016).

Suppression des données

Une fois que les données ne sont plus nécessaires et n'ont plus à être conservées conformément aux obligations professionnelles ou autres obligations légales d'un juriste, elles doivent être correctement supprimées. L'un des avantages de la suppression de

données inutiles est qu'elle peut minimiser l'impact potentiel de toute violation de sécurité relative aux dossiers du juriste.

Avant de supprimer des données, les juristes devraient se familiariser avec les règles de déontologie professionnelle pertinentes (voir, p. ex. règle 3.5) et les règles et réglementations du barreau dans leur territoire relatives à la conservation des documents.

Lors de la suppression de données, les juristes doivent également s'assurer qu'ils respectent leurs obligations de confidentialité envers leurs clients. Par exemple, l'utilisation de la fonction standard « supprimer » sur un ordinateur, une tablette ou un téléphone intelligent est insuffisante pour empêcher des tiers de récupérer ultérieurement un fichier. Bien que l'option la plus sécuritaire soit la destruction matérielle du support qui stocke les données confidentielles, les moyens de « nettoyer », « d'épurer » ou « de purger » sont également des formes de suppression relativement sécuritaires. Plusieurs outils d'épuration de fichiers existent à cet effet. Lors de la suppression de données, les juristes ne devraient pas négliger les disques durs des copieurs et imprimantes qui stockent des images de documents.

Pour en savoir plus :

- Lawyers Insurance Association of Nova Scotia, File/Record Retention (dernière mise à jour en 2021).
- Barreau de l'Ontario, Gestion de dossiers (dernière mise à jour en 2020).
- Law Society of British Columbia, Closed Files—Retention and Disposition (août 2017).
- Barreau du Québec, Guide des TI (2016).
- Barreau de l'Ontario, Guide sur la conservation et de destruction des dossiers fermés des clients pour les avocats (dernière mise à jour en 2014).

Stockage et outils de l'infonuagique

Les outils et services de l'infonuagique offrent de nombreux avantages aux juristes et permettent d'accéder à une gamme d'applications et services logiciels nouveaux. Ils permettent également aux juristes d'externaliser la maintenance et la mise à jour du matériel et des logiciels vers les fournisseurs d'infonuagique. Enfin, ils permettent d'accéder aux données de pratiquement tous les coins du monde et de réduire d'importants investissements.

Le stockage et les outils d'infonuagique peuvent également aider à résoudre certains des risques mentionnés précédemment. Cependant, le stockage ou la transmission d'informations avec des fournisseurs tiers peut aussi entraîner de nouveaux risques en ce qui concerne la confidentialité des renseignements et le secret professionnel de l'avocat, car le juriste met les données entre les mains de tiers. Il se pose notamment des questions de sécurité et de confidentialité, de conformité réglementaire et de gestion des risques.

La confidentialité est particulièrement préoccupante lorsque des renseignements sont hébergés sur des serveurs à l'extérieur du Canada, car certains gouvernements étrangers ont adopté des lois leur permettant d'accéder à ces renseignements. Même des serveurs situés au Canada pourraient relever d'une juridiction étrangère s'ils sont exploités par des fournisseurs ayant des intérêts étrangers.

Outre le fait qu'il s'agit d'une bonne pratique de conserver ses données sur des serveurs canadiens, certains documents (p. ex. les registres d'entreprise et fiscaux) doivent être conservés au Canada en vertu de la loi.[9] Le fait que les données soient *accessibles* depuis le Canada ne répond pas à cette exigence. Par conséquent, les juristes devraient s'enquérir de l'emplacement des données auprès de leur fournisseur de stockage infonuagique et exiger contractuellement que leurs données soient stockées sur des serveurs situés au Canada.

Sauf instruction contraire du client, les renseignements confidentiels envoyés par Internet à un serveur ou à une autre personne doivent être chiffrés, y compris aux services d'infonuagique. Lors de l'examen des solutions d'infonuagique, les juristes devraient confirmer si les données sont chiffrées en stockage ou en transit *(voir section ci-dessus sur les « Fondamentaux du chiffrement »).*

Les juristes devraient également lire les modalités de service pour se renseigner sur le moment ou la façon dont un service d'infonuagique répond à une notification juridique ou à une demande de divulgation de données. Pour éviter d'éventuelles atteintes à la confidentialité, les juristes devraient privilégier les services où ils peuvent être les seuls propriétaires des clés de chiffrement. De fait, les services d'infonuagique peuvent être contraints par la loi de divulguer des données, ce qui peut inclure d'être contraint de déchiffrer des données et de les communiquer, parfois sans en avertir quiconque. Si les clés de chiffrement sont gérées par le service d'infonuagique, alors le service a également la possibilité de déchiffrer et d'accéder à tout moment aux renseignements en question, ainsi que tout tiers qui pourrait, de façon légale ou malveillante, obtenir l'accès aux données stockées.

Enfin, les juristes devraient rechercher des services d'infonuagique qui permettent

[9] Voir, par exemple, les consignes de l'Agence du revenu du Canada concernant le stockage numérique des registres fiscaux.

une sauvegarde « locale », le juriste pouvant conserver une sauvegarde sur son propre ordinateur. Avec cette fonctionnalité, si Internet ou le service d'infonuagique devient indisponible (p. ex. problème de connectivité, retard de paiement, litiges contractuels, demande de tiers), la sauvegarde locale permettra au juriste de continuer à travailler.

Pour en savoir plus :

- Law Society of British Columbia, Cloud Computing Checklist v. 3.0 (dernière mise à jour en avril 2020).
- Derek Bolen, What Lawyers Need to Know about Encryption, *Clio* (dernière mise à jour en 2021).
- Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de base pour les petites et moyennes organisations* (février 2020).
- LawPRO, How to Safely Put Your Data in the Cloud, *PracticePRO* (1er janvier 2018).
- David Fraser, L'infonuagique : Foire aux questions sur le respect de la vie privée, magazine ABC National (2014).

Courriel

Le courriel est un moyen facile de partager des informations et de communiquer avec les autres, mais son utilisation comporte de nombreux risques, notamment en ce qui concerne la protection de la confidentialité de la correspondance. En outre, les courriels sont souvent les premiers et les plus faciles points d'attaque pour les cybercriminels.

Confidentialité

Un courriel envoyé à un client peut ne jamais atteindre sa destination, être intercepté par un tiers ou être bloqué par erreur par le filtre anti pourriel du client. Pour ces raisons, il faudrait préalablement convenir avec un client que le courriel (ou un autre moyen de communication) sera utilisé. Lorsque l'on discute d'un moyen de communication avec un client, il devrait être informé des risques associés à ce moyen de communication et les accepter. Par exemple, les clients devraient savoir que les fournisseurs de services de messagerie électronique gratuits, ou les employeurs si une adresse de courriel professionnelle est utilisée, sont souvent autorisés contractuellement à accéder à leurs conversations privées. Il convient également d'expliquer aux clients que l'envoi d'une copie à des tiers dans un courriel peut être interprété comme une renonciation au secret professionnel. Un juriste doit également être prudent lorsqu'il répond lui-même aux courriels; des juristes ont été réprimandés pour avoir envoyé un courriel à la mauvaise

adresse, ou pour avoir cliqué sur « répondre à tous » plutôt que sur « répondre » dans le cadre d'un échange confidentiel.[10]

De même, un juriste qui reçoit par erreur une communication par courriel d'une partie adverse ou de son avocat doit agir avec prudence et respecter les règles de déontologie professionnelle applicables concernant la réception de communications involontaires (voir règle 7.2-10).

La facilité d'utilisation du courriel en fait également une cible attrayante pour les cybercriminels. Pour se protéger et protéger leurs clients, les juristes devraient envoyer des informations confidentielles et sensibles par courriel chiffré *(voir section « Fondamentaux du chiffrement » ci-dessus).* Les juristes doivent cependant se rappeler que le chiffrement des courriels ne masque que leur contenu; les métadonnées, y compris de qui à qui, pourraient encore être visibles *(voir ci-dessous la section « Métadonnées »).*

Usurpation d'identité électronique et hameçonnage

L'hameçonnage implique l'utilisation d'un courriel, d'un texto ou d'un appel téléphonique qui semble provenir d'une source ou d'une institution, d'un fournisseur ou d'une entreprise de confiance, mais qui provient en réalité d'un imposteur tiers. Les attaques d'hameçonnage sont de plus en plus utilisées contre les cabinets juridiques et autres organisations juridiques.[11] Ces attaques sont également de plus en plus sophistiquées, par exemple, elles ciblent souvent une personne spécifique et sont adaptées pour mentionner des activités (comme les transferts de fonds) dans lesquelles la personne est engagée. Les messages d'hameçonnage ont pour but de vous inciter à donner des informations aux fraudeurs en vous demandant de mettre à jour ou de confirmer des renseignements personnels ou des comptes en ligne. Tous les juristes et le personnel travaillant dans l'organisation doivent être informés du potentiel et de la nature des attaques d'hameçonnage pour s'assurer de ne pas se faire prendre. Au sein des cabinets juridiques, le personnel et les juristes en début de carrière sont des cibles courantes; ainsi, dans une pratique appelée « arnaque au patron », quelqu'un contacte un employé en usurpant l'identité de son supérieur pour demander une aide urgente pour un paiement.

Comme on le mentionnait, les courriels d'hameçonnage sont de plus en plus sophistiqués, mais les signaux d'alerte des arnaques d'hameçonnage comprennent des messages génériques, des signatures de courriel différentes ou des adresses de courriel différentes.

---

[10] Voir, p. ex. *Smith c. Teixeira*, 2009 QCCQ 3402, où un avocat québécois a été jugé avoir manqué à l'éthique parce qu'il avait inclus toutes les adresses courriel de ses clients dans le champ « à » d'un courriel annonçant un déménagement de bureau, laissant ainsi chaque client voir l'identité et l'adresse de tous les autres clients.

[11] Plusieurs cas sont connus de cabinets juridiques victimes d'attaques par hameçonnage, d'usurpation d'identité pour frauder des clients ou contactés par de faux avocats, ou de piratage de clients et d'envoi d'instructions frauduleuses de virement électronique.

Dans la plupart des cas, le courriel sera envoyé à partir d'un service de messagerie gratuit (p. ex. Gmail ou Outlook/Hotmail), même lorsque le courriel est prétendument envoyé au nom d'une entité commerciale, et les entêtes du courriel ne sont pas cohérents (p, ex., nom ou adresse courriel dans le champ « De »; le courriel est envoyé « au nom » d'un autre domaine).

Dans de nombreux cas, un courriel demandera de l'argent ou des biens (par exemple des cartes-cadeaux) en évoquant une situation d'urgence (dans le but de tenter d'éviter les contrôles de conformité habituels avec la comptabilité). Une personne déclarant préférer communiquer par courriel en raison de différences de fuseau horaire ou affirmant ne pas avoir accès à un téléphone pour le moment est un signe d'arnaque potentielle.

De même, méfiez-vous s'il est nécessaire de cliquer sur un lien pour effectuer une action ou poursuivre la conversation. Vérifiez que le lien mène à un site Web légitime et que le lien renvoie vers la même URL que celle indiquée dans le message (placez votre curseur sur le lien). Si des identifiants sont demandés en cliquant sur le lien, confirmez dans la barre d'URL que vous êtes bien sur le site Web authentique. Il est généralement recommandé de ne pas cliquer sur les liens dans les courriels, mais d'aller sur le site Web de la manière habituelle.

Il faut aussi se méfier quand parfois le courriel peut sembler provenir de la bonne adresse de courriel, mais qu'il invite le destinataire à cliquer sur un lien, ou répondre à une autre adresse de courriel. Dans les attaques plus avancées, le message peut provenir des comptes de courriel authentiques, à la suite du piratage des comptes de tiers, y compris des clients, des juristes, du personnel d'un cabinet, des avocats adverses et des parties adverses. Le fraudeur surveillera les courriels de la partie piratée pour déterminer s'il existe une question juridique d'intérêt. Lorsque l'affaire est terminée et que l'argent est sur le point de changer de mains, comme à la suite d'un règlement de litige, de la clôture d'une transaction immobilière ou autres, le fraudeur, se présentant comme la partie légitime qui attend les fonds, enverra un courriel avec des instructions pour rediriger les fonds. Si l'on suit ces instructions, l'argent ira au fraudeur.

De nouvelles instructions de paiement (p. ex. montants différents, nouveau compte bancaire) sont souvent le signe d'une fraude potentielle. En cas de doute, il est plus sûr de confirmer avec la personne par un autre moyen de communication (comme un appel téléphonique) que vous avez utilisé auparavant avec elle.

Pièce jointe malveillante, piratage, logiciels espions et rançongiciels

Les attaques d'hameçonnage peuvent également être plus sophistiquées et aller au-delà de « simplement » essayer d'obtenir des identifiants et de voler de l'argent. En cliquant sur

un lien, les utilisateurs peuvent télécharger par inadvertance des logiciels malveillants sur leur ordinateur. Un logiciel malveillant pourrait également se cacher dans une pièce jointe de courriel, comme une fausse facture. En plus des virus qui corrompraient les données, les logiciels malveillants peuvent inclure des logiciels espions qui permettraient à des tiers d'accéder à votre ordinateur, de consulter tous vos fichiers, vos courriels et d'agir en votre nom sur votre réseau (y compris l'envoi de messages à des clients, collègues, juges). Les données recueillies peuvent servir à commettre une escroquerie envers vous ou vos clients.

Un autre type d'attaque de plus en plus courant concerne les rançongiciels.[12] Les attaques par rançongiciel résultent généralement d'un hameçonnage, où un courriel contenant un lien infecté est envoyé à un juriste ou à un membre du personnel. Une fois le lien cliqué, le rançongiciel est installé sur l'ordinateur de la victime. Il commence à travailler en arrière-plan pendant que l'ordinateur est allumé, chiffrant les documents et les rendant inaccessibles. Les responsables de l'attaque par rançongiciel demanderont ensuite d'importants paiements d'argent pour restituer les données à l'organisation.

Les utilisateurs doivent disposer d'un outil antivirus capable de scanner en direct le trafic Web et les courriels, notamment les pièces jointes et tout contenu téléchargé depuis Internet. Les paramètres de sécurité et de confidentialité des ordinateurs devraient interdire à tout logiciel de s'exécuter automatiquement après le téléchargement.

Comme mentionné précédemment, les données de sauvegarde doivent être séparées du reste du réseau. C'est un bon moyen non seulement de prévenir une attaque, mais aussi de pouvoir récupérer des données et redémarrer le travail après avoir été bloqué par un rançongiciel.

Pour en savoir plus :

- Lawyers Indemnity Fund, Fraud Prevention (dernière consultation le 14 mars 2021)
- Juda Strawczynski, Wire Fraud Scams on the Rise: 5 Tips to Reduce Your Risk (2021).
- Derek Bolen, What Lawyers Need to Know about Encryption, *Clio* (dernière mise à jour en 2021).
- LawPRO, Paying Attention to the Fraud Behind the Curtain, *PracticePRO* (1er janvier 2020).
- Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de*

[12] Ces dernières années, plusieurs avocats ont été victimes d'attaques par rançongiciel à tous les niveaux de pratique, des grands cabinets juridiques nationaux à un barreau, en passant par des cabinets au Manitoba et en Alberta.

base pour les petites et moyennes organisations (février 2020).

- Raymond G. Leclair, Firm Websites Being Impersonated by Fraudsters, *AvoidAClaim* (8 juillet 2020).
- SereneRisc, Cybersecurity Tips: Phishing (dernière mise à jour 2019).
- LawPRO, Fraud Fact Sheet: Cybercrime and Bad Cheque Scams, PracticePRO (2011).
- LawPRO, Avoid (and Recover From) a Ransomware Attack, *AvoidAClaim* (15 novembre 2017).

Divulgation des métadonnées

En plus de leur propre contenu, les documents électroniques contiennent des métadonnées, c'est-à-dire des informations sur d'autres données (dans ce cas, des informations sur le fichier). De nombreux programmes informatiques intègrent des informations dans la sortie du programme lorsqu'un fichier est créé, ouvert et sauvegardé. Bien que non visibles en affichage normal, les métadonnées peuvent être révélées et consultées par d'autres personnes lorsqu'un document est diffusé électroniquement. Les informations contenues dans les métadonnées peuvent inclure le nom de l'auteur du document, la date de création du document, les révisions du document, y compris les insertions et les suppressions, le suivi des modifications et des commentaires ajoutés par les examinateurs, et l'emplacement du fichier stocké.

Sauf lorsqu'un juriste est légalement tenu de conserver ou de communiquer des métadonnées (p. ex. obligations de communication préalable), des mesures doivent être prises pour minimiser la création de métadonnées ou pour les effacer des fichiers envoyés. Lorsque vous partagez des documents en ligne, notamment par courriel, assurez-vous que les documents envoyés par courriel ne contiennent pas de métadonnées contenant des renseignements confidentiels.[13] Cela doit également être pris en compte lors du téléchargement d'un fichier sur une plateforme Web, même à des fins personnelles, car les métadonnées pourraient divulguer des informations sur votre localisation, et donc sur votre client et vos activités.

En plus de la pièce jointe, le courriel en soi contiendra des métadonnées, notamment pour en assurer l'authenticité. Cependant, les métadonnées dans l'entête du courriel pourraient également divulguer votre emplacement et les réseaux auxquels vous êtes connecté, et donc divulguer involontairement des informations confidentielles potentielles et des

[13] Bien que certains outils commerciaux offrent de gommer les métadonnées des fichiers, la plupart des logiciels de traitement de texte et PDF offrent également une option pour supprimer les métadonnées lors de l'enregistrement du document (p. ex. dans les options « protéger » ou « inspecter » les documents dans Microsoft Word; dans les options « expurger » d'Adobe Acrobat).

relations à des tiers.

Pour en savoir plus :

- Administrative Office of the U.S. Courts, Guidelines for Editing Metadata (septembre 2018).
- LawPRO, Beware of the Dangers of Metadata, *PracticePRO* (2004).
- Commissariat à la protection de la vie privée du Canada, Métadonnées et vie privée (octobre 2014).

Voyager avec des appareils électroniques

Il est important que les juristes comprennent comment les intérêts de leurs clients en matière de protection de la vie privée, et leur obligation de protéger les renseignements confidentiels de ces clients peuvent être affectés lorsqu'un juriste traverse une frontière internationale avec un appareil électronique. En franchissant une frontière internationale, y compris à destination ou en provenance du Canada, les juristes ne peuvent pas nécessairement se fier à une revendication du secret professionnel de l'avocat pour protéger adéquatement les renseignements confidentiels des clients en raison de la vaste interprétation par les organismes frontaliers des « marchandises » qu'ils ont le pouvoir d'examiner.[14] Les agents peuvent examiner les données stockées sur tout appareil électronique en possession effective d'un voyageur ou dans les bagages qui l'accompagnent. Ils peuvent également demander des mots de passe pour les appareils.

La fouille du dispositif électronique (c.-à-d. téléphones, tablettes, ordinateurs portables ou clés USB) d'un juriste lorsque celui-ci franchit une frontière internationale peut porter atteinte au secret professionnel de l'avocat et entraîner une violation de la règle 3.31 qui impose aux juristes de protéger les renseignements confidentiels des clients. Outre les obligations figurant dans les codes de déontologie professionnelle, les juristes peuvent également avoir des obligations en vertu des règles de leur barreau respectif et des lois applicables en matière de protection de la vie privée.

Plusieurs mesures pratiques ont été proposées aux juristes pour atténuer le risque que des

[14] Notons que, dans *R. v. Canfield*, 2020 ABCA 383, la Cour d'appel de l'Alberta a jugé que le par. 99(1)a) de la *Loi sur les douanes* est anticonstitutionnel dans la mesure où il n'impose aucune limite aux recherches d'appareils électroniques à la frontière, et qu'il n'est pas sauvegardé par l'application de l'art. 1 de la Charte. La Cour a en outre déclaré la définition de « marchandises » au par. 2 de la *Loi sur les douanes* est inopérante dans la mesure où la définition comprend le contenu des appareils électroniques personnels aux fins du par. 99(1)a), mais a suspendu la déclaration d'invalidité pendant un an pour donner au Parlement la possibilité de modifier la législation afin de déterminer comment traiter les fouilles d'appareils électroniques personnels à la frontière. L'autorisation d'interjeter appel devant la Cour suprême du Canada a été demandée mais rejetée dans cette affaire.

renseignements confidentiels et privilégiés sur les clients soient exposés lors du passage de la frontière. La pratique la plus sûre est de traverser la frontière sans renseignements confidentiels et privilégiés des clients. Cela peut se faire en prenant des appareils « nettoyés » ou « vierges » qui ne contiennent aucune information client, en mettant l'appareil en « mode avion » (et déconnecté des services d'infonuagique), puis en accédant à tous les renseignements ou fichiers nécessaires une fois la frontière franchie par une connexion à distance sécurisée. Il est également recommandé que si les juristes voyagent avec des renseignements confidentiels ou privilégiés sur leurs clients, ils portent une pièce d'identité indiquant qu'ils sont un juriste inscrit au barreau. Les juristes peuvent choisir d'inclure dans leurs mandats de représentation les informations pertinentes concernant la protection des renseignements privilégiés en situation de voyage. Ils devraient discuter de la question avec leurs clients et fournir des conseils appropriés en la circonstance.

Pour en savoir plus :

- Association du barreau canadien, Trousse d'outils sur la gestion des renseignements confidentiels à la frontière (13 mai 2019).
- Fédération des ordres professionnels de juristes du Canada, Traverser la frontière avec des appareils électroniques : Ce que les juristes canadiens doivent savoir (14 décembre 2018).

Services externes de protection des données

Les cabinets juridiques peuvent également envisager de retenir des services externes de protection des données, car il peut être difficile pour les entreprises de développer et d'implanter leurs propres politiques et infrastructures de cybersécurité, qu'il s'agisse du coût du matériel ou de l'assurance qu'il reste à jour. Au-delà de la réduction des coûts d'infrastructure et de dotation que permet le partage, l'externalisation assure également aux juristes une protection adaptative, qui peut s'étendre au fur et à mesure de leur expansion et de la prise en charge de clients ou de dossiers plus sensibles. Les prestataires de services peuvent également assister les juristes en cas de cyberincidents, allant de la recommandation et l'installation de mesures préventives à la négociation avec les assureurs en cas de violation.

Pour en savoir plus :

- LawPRO, Outsourcing your law firm's cybersecurity, *PracticePRO* (1er août 2017).

Préparation, intervention en cas d'incident et assurance contre les risques numériques

Nonobstant toutes les mesures de sécurité mises en place, il y aura toujours un risque que les données des clients soient divulguées, détruites ou modifiées. En plus des risques de cybersécurité, les données peuvent également être détruites ou compromises à la suite d'événements naturels, tels que des inondations ou des incendies. Il fait partie des obligations des juristes d'élaborer un cadre de gestion de la sécurité de l'information, allant de la sécurité de l'information, des dispositifs et des politiques de confidentialité, à un plan d'intervention en cas d'incident afin d'être préparé pour de tels événements.

Pour s'assurer que des pratiques exemplaires relatives à la sécurité, à l'intégrité et à l'accessibilité des données sont adoptées et appliquées en permanence dans un milieu de travail juridique, il est recommandé que les juristes s'assurent d'implanter une politique de sécurité de l'information. Des directives doivent être communiquées aux juristes et au personnel concernant l'utilisation d'équipements personnels pour le travail, ou l'utilisation d'appareils et de réseaux de travail à des fins personnelles. Dans certains contextes, il peut être judicieux de limiter l'accès à des fichiers ou renseignements sensibles à des appareils ou des réseaux désignés.

Les milieux de travail juridiques doivent disposer d'une liste (et d'un contrôle à distance) de tous les appareils ayant accès au réseau, des logiciels et solutions utilisés sur les appareils/le site et en infonuagique, et de l'endroit où se trouvent différentes données. Le cadre de sécurité de l'information doit également inclure une liste de toutes les personnes ayant accès aux données, et à quelles données. Si un identifiant d'utilisateur ou un appareil est compromis ou si une solution présente une vulnérabilité en matière de sécurité, elle peut alors être rapidement retirée ou séparée du réseau.

Le cadre de sécurité de l'information devrait également inclure des audits réguliers, allant de la vérification que seules les personnes qui devraient avoir accès aux fichiers y ont accès, à la confirmation que tous les appareils exécutent les plus récents correctifs de sécurité.

Étant donné que la plupart des risques de cybersécurité résultent d'erreurs commises par des individus, le cadre de sécurité de l'information devrait inclure une formation et une simulation d'attaques de cybersécurité menées avec ou sans préavis aux membres de l'organisation (p. ex. une organisation peut mener une fausse campagne d'hameçonnage à titre de mesure éducative), afin de confirmer la préparation des individus.

Pour permettre une atténuation et des solutions rapides, le cadre de gestion de la sécurité de l'information doit également inclure un plan d'intervention en cas d'incident avec les

différentes mesures à prendre. Le plan d'intervention en cas d'incident doit inclure une référence à toutes les obligations de signalement que les juristes peuvent avoir, telles que les obligations de signaler les violations de la sécurité aux clients, aux barreaux ou aux assureurs (voir, p. ex. règle 7.1-3, règle 7.8-1, et règle 7.8-2) en plus des obligations légales de signalement dans les dispositifs provinciaux ou fédéral sur la protection des données.

Au sein des organisations, le cadre devrait inclure l'attribution de la responsabilité de la sécurité de l'information à une personne (et à un remplaçant en cas d'incapacité ou de congé), ayant le pouvoir d'approuver ou de rejeter les usages, de répondre aux questions des clients et des parties prenantes, et d'activer et de coordonner une intervention en cas d'incident au sein de l'organisation.

Les juristes doivent également savoir que, bien que leur assurance professionnelle couvre certains problèmes liés à la prestation de services professionnels, elle ne couvre généralement pas la perte ou la violation de données, la perte de revenus ou d'équipement après une cyberattaque ou un événement naturel. Une assurance facultative contre la cybercriminalité ou en vue de la sécurité des données peut être disponible dans certains territoires.

Pour en savoir plus :

- Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de base pour les petites et moyennes organisations* (février 2020).
- LawPRO, Does your firm need cybercrime insurance?, *PracticePRO* (1er janvier 2018).
- Lawyers Financial, Cyber Risk—Is your Law Firm Protected?, *Canadian Lawyer* (4 septembre 2018).
- LawPRO, The LawPRO $250,000 cybercrime coverage: What it covers and why, *PracticePRO* (1er décembre 2013).
- Law Society of British Columbia, *What to do Before and After a Disaster Strikes*.

3. Télétravail avec les clients, les collaborateurs et les tribunaux

L'adoption de pratiques de télétravail, telles que le travail à domicile ou à partir d'un bureau virtuel, la fourniture de services d'attestation à distance aux clients et la

participation à des réunions et auditions virtuelles, peuvent rendre les services plus efficaces et accessibles aux clients. En outre, dans la mesure où les processus et outils à distance deviennent obligatoires ou même largement utilisés dans certains processus juridiques et domaines de pratique, leur utilisation appropriée peut également être caractérisée comme une question de compétence.

Objectif : Veiller au respect de ses obligations professionnelles lors du télétravail.

Vous trouverez ci-dessous un certain nombre des questions à poser dans le cadre de l'évaluation de la conformité, ainsi que les possibles systèmes et pratiques à mettre en œuvre pour parvenir à ladite conformité.

Q: Lorsque vous travaillez dans un bureau virtuel, les obligations professionnelles en matière de confidentialité et de supervision sont-elles respectées?

Éviter d'utiliser des réseaux Wi Fi publics non sécurisés et veiller à :

- ✓ Utiliser le niveau de chiffrement le plus élevé disponible sur routeur sans fil.
- ✓ Utiliser un mot de passe robuste.
- ✓ Désactiver les réseaux d'invités.
- ✓ Désactiver l'administration à distance.
- ✓ Modifier les identifiants d'administrateur par défaut.

Si des données confidentielles sortent du bureau :

- ✓ Des mécanismes de chiffrement devraient être adoptés pour les sécuriser pendant le transport.
- ✓ Déterminer s'il est possible d'accéder à des renseignements par connexion chiffrée sécurisée ou réseau privé virtuel, ce qui est plus sûr que de transporter des fichiers sur un disque dur d'ordinateur portable ou une clé USB.

Éviter généralement de travailler sur des questions confidentielles dans des espaces publics, mais si tel est le cas, prendre des mesures pour préserver la confidentialité :

- ✓ Utiliser des écrans de confidentialité sur tous les appareils électroniques pour restreindre les personnes qui peuvent voir vos écrans.
- ✓ Utiliser des écouteurs.
- ✓ Attention à ne pas parler trop fort.

Lorsque vous supervisez des collègues en télétravail, s'assurer qu'ils sont au courant de leurs obligations de confidentialité et des pratiques exemplaires de fonctionnement dans un bureau virtuel.

Q: Lors d'une authentification de signature ou d'une attestation à distance, toutes

les exigences législatives et réglementaires applicables sont elles respectées? A-t-on adopté des pratiques exemplaires?

- ✓ Confirmer que l'authentification de signature ou l'attestation à distance est autorisée dans votre territoire.
- ✓ Examiner et respecter les règles et réglementations de votre territoire en matière d'authentification de signature ou d'attestation à distance.

Prendre des mesures pour se prémunir contre les principaux risques, notamment :

- ✓ Fraude et usurpation d'identité.
- ✓ Influence indue.
- ✓ Impacts négatifs sur le service à la clientèle.
- ✓ Difficultés de vérification liées à une technologie de qualité médiocre ou peu fiable.

Q: Les règles et règlements du barreau sont-ils respectés en cas d'utilisation d'un moyen virtuel d'identification ou de vérification de l'identité d'un client?

- ✓ Examiner les règles de votre barreau concernant les règles d'identification et de vérification des clients.

Lorsque les règles de vérification des clients exigent une vérification « face à face » et que le barreau compétent permet que cette vérification ait lieu lors d'une réunion virtuelle :

- ✓ Être attentif aux signaux d'alerte potentiels.
- ✓ Si la prudence s'impose, envisager d'utiliser une autre méthode acceptée de vérification de l'identité.
- ✓ Si vous procédez à une vérification virtuelle de l'identité (le cas échéant), envisager d'obtenir une image haute résolution du document d'identification avant la réunion virtuelle comme référence.

Q: A-t-on adopté des pratiques exemplaires pour les réunions et audiences virtuelles?

Dans les cas où le juriste a de la latitude dans le choix d'une plateforme :

- ✓ Déterminer si la réunion nécessitera un chiffrement de bout en bout véritable.
- ✓ Utiliser des contrôles d'accès tels qu'un mot de passe ou une salle d'attente virtuelle.

Si vous envisagez d'enregistrer une réunion :

- ✓ Respecter les règles de déontologie professionnelle concernant l'enregistrement

des conversations.
- ✓ Se conformer aux règles applicables du tribunal ou de la cour.

Adopter des pratiques exemplaires en matière de confidentialité :

- ✓ Si nécessaire, des écouteurs devraient être utilisés pour empêcher des tiers d'écouter la réunion.

Être attentif aux risques liés aux tiers qui influencent le témoignage et s'en prémunir :

- ✓ Vérifier si quelqu'un d'autre est présent avec le témoin ou écoute sur un appareil qui pourrait lui fournir des informations pendant l'entretien.

Q: Existe-t-il une compréhension appropriée du moment et de la manière dont les signatures électroniques peuvent être utilisées pour exécuter des documents?

- ✓ Examiner les exigences législatives avant d'utiliser des signatures électroniques.

Si une signature électronique est autorisée, s'assurer que :

- ✓ La signature électronique associe de manière fiable la personne à la signature et associe de manière fiable la signature au document.
- ✓ Des mesures de sécurité ont été mises en place pour empêcher tout accès, utilisation ou copie non autorisés.

Envisager de recourir à des pratiques exemplaires, notamment :

- ✓ Cryptographie à clé publique uniquement associée au document.
- ✓ Adoption de systèmes de signature électronique plus avancés qui comprennent l'horodatage et l'empreinte du document par l'intermédiaire d'un tiers qui pourrait attester de l'heure, de l'authenticité et de l'intégrité des documents signés.

Si le juriste utilise lui même une signature électronique, s'assurer que :

- ✓ L'accès est strictement contrôlé (les juristes doivent avoir le plein contrôle et une entière connaissance de l'utilisation).

Bureau virtuel

Lorsqu'ils utilisent un bureau virtuel, que ce soit en télétravail ou dans un lieu autre qu'un espace de bureau réservé à leur cabinet, les juristes doivent s'assurer qu'ils prennent les mesures adéquates pour respecter leurs obligations de confidentialité (règle 3.3-1) et de supervision (règle 6.1-1).

Les réseaux privés virtuels (RPV) et les applications de bureau à distance peuvent donner

aux juristes un moyen sécurisé de se connecter aux fichiers et aux renseignements des clients. Si des données numériques confidentielles sont matériellement sorties du bureau réservé d'un juriste, des mécanismes de chiffrement doivent être adoptés pour les sécuriser pendant le transport. Lorsque c'est possible, il est plus sûr d'accéder à des informations par le biais d'une connexion chiffrée sécurisée ou d'un RPV que de transporter des fichiers sur un disque dur d'ordinateur portable ou une clé USB.

Lors de l'utilisation de réseaux WiFi, les juristes devraient choisir le niveau de chiffrement le plus élevé disponible sur les routeurs de leurs réseaux sans fil (au moins WPA2, si possible WPA3) et utiliser un mot de passe robuste. Ils devraient également désactiver les réseaux d'invités et l'administration à distance, ainsi que modifier les identifiants d'administrateur par défaut de leur routeur (souvent « admin/admin ») conformément aux pratiques exemplaires de mot de passe mentionnées précédemment. Pour plus de sécurité, les juristes devraient changer le nom public de leur réseau WiFi et le cacher à des appareils non authentifiés en désactivant la diffusion du nom de leur réseau WiFi (« Diffusion SSID »). Les juristes peuvent également limiter la capacité des appareils à se connecter au réseau en activant le « filtrage d'adresse MAC » qui n'autorisera qu'une série d'appareils spécifiques à se connecter en fonction de leurs identifiants uniques.

Les juristes doivent garder à l'esprit que s'ils sont capables de se connecter à un réseau WiFi sans mot de passe, le réseau n'est pas sécurisé. Les juristes ne devraient pas utiliser le WiFi non sécurisé pour se connecter à un serveur professionnel, effectuer des opérations bancaires ou envoyer tout type de renseignements confidentiels ou personnels.

Les juristes devraient également s'assurer que tous les appareils à commande vocale qu'ils ont, tels que les haut-parleurs intelligents et les assistants virtuels, sont éteints ou ont cette fonction désactivée lorsqu'ils discutent des affaires des clients ou partagent toute autre information confidentielle. Les juristes devraient envisager de retirer ces appareils de leurs espaces de travail dans la mesure du possible et de leur environnement lorsqu'ils rencontrent des clients.

De manière générale, il convient d'éviter de traiter de questions confidentielles dans des espaces publics, dans la mesure où des tiers peuvent voir des écrans et des documents imprimés ou entendre des conversations. Dans les lieux publics (espaces partagés, cafés, trains, avions, etc.), les juristes devraient utiliser des écrans de protection de la vie privée sur tous leurs appareils électroniques pour limiter le nombre de personnes qui peuvent voir leurs écrans. De même, les juristes devraient utiliser des écouteurs et veiller à ne pas parler trop fort pour préserver la confidentialité.

Lorsque vous supervisez des collègues en télétravail, assurez-vous qu'ils sont au courant de leurs obligations de confidentialité et des pratiques exemplaires de fonctionnement

dans un bureau virtuel. Les tribunaux ont reconnu un risque que les situations de travail virtuelles puissent priver les étudiants et les juristes subalternes de contacts réguliers et informels avec les juristes de supervision et de mentorat, ce qui peut entraîner la publication d'instructions inadéquates et de documents mal examinés.[15]

Pour en savoir plus :

- Association du Barreau de l'Ontario, *Online Lawyering Checklist* (2020).
- Juda Strawczynski, Workfromhome Technology Tips, *PracticePRO* (2020).
- LawPRO, Beware of cybersecurity risks during COVID19 and working from home, *AvoidAClaim* (20 mars 2020).
- Barreau de l'Ontario, Comment puis-je assurer la confidentialité des renseignements des clients pendant que je travaille à distance? (2021)
- Barreau de l'Ontario, Mes obligations de confidentialité empêchent-elles le personnel de soutien du bureau de travailler à distance? (2021)
- Société du Barreau du Manitoba, What should I consider when working from home? (2020)
- Crystal Tse et Jonathan Browning, LockedDown Lawyers Warned Alexa Is Hearing Confidential Call, Bloomberg (20 mars 2020)

Authentification de signature et attestation à distance

Dans de nombreux territoires, les juristes sont désormais autorisés à recourir à l'attestation à distance, et l'authentification de signature à distance est autorisée dans quelques territoires. L'attestation à distance signifie la signature d'affidavits et de déclarations solennelles qui ont lieu dans un lieu matériel différent de celui du commissaire (c'est-à-dire le juriste) en utilisant la technologie audiovisuelle. L'authentification de signature à distance se définit de la même façon, mais fait référence à la signature à distance de testaments et de procurations. Différents territoires ont des règles différentes pour l'authentification de signature et l'attestation à distance, et certaines ne permettent pas ces pratiques. Les juristes doivent examiner et suivre les règles applicables dans leur territoire.

Dans de nombreux cas, des autorisations d'attestation et d'authentification de signature à

[15] *Polgampalage v. Devani*, 2021 ONSC 1157, par. 4043.

distance ont été données spécifiquement en réponse à la pandémie de COVID19. Bien que certains territoires aient indiqué leur intention de prolonger ces mesures après la pandémie, les juristes doivent prêter une attention particulière pour s'assurer qu'ils respectent les règles actuellement en vigueur dans leur territoire.

L'attestation à distance comporte plusieurs risques. Le Barreau de l'Ontario a identifié quatre risques majeurs et a publié des conseils pratiques concernant chaque risque :

> **Risque 1—Fraude et usurpation d'identité**
> La diminution ou l'élimination de rencontres en personne entre le commissaire et le client engendre un risque accru de fraude et de vol d'identité.

Conseil pratique
Soyez attentif aux signaux d'alerte de fraude dans l'affaire. Vérifiez s'il y a des indices de fraude en consultant les avis à la profession juridique concernant les risques de la Fédération des ordres professionnels de juristes.

> **Risque 2—Influence indue**
> Le recours à une attestation à distance entraîne un risque accru qu'une influence indue passe inaperçue. Le commissaire pourrait ne pas être en mesure de déterminer adéquatement si le déposant fait l'objet d'une influence hors champ ou s'il est contraint par d'autres personnes.

Conseil pratique
Évaluez s'il existe un risque que le client soit soumis à une influence indue ou à une contrainte. Si un tel risque existe, considérez si vous pouvez aider le client en ce moment sans se rencontrer en personne.

> **Risque 3—Niveau de service à la clientèle moindre**
> Sans mesure de protection, il existe un risque que le client n'obtienne aucune copie des documents qu'il a signés par voie électronique. Il y a également un risque que le client juge qu'il n'a pas eu une chance équitable de poser des questions ou de demander des précisions au sujet des documents qu'il signe. Ce risque est d'ailleurs accru en raison de l'absence de proximité physique.

Déterminez comment fournir au client des copies du document exécuté à distance.

Confirmez que votre client comprend bien les documents qu'il signe et donnez lui la possibilité de poser des questions pendant la vidéoconférence.

> **Risque 4—Limites ou incertitudes technologiques**
> Compte tenu du caractère variable de la qualité d'image et de la connexion réseau, ainsi

> que du fait qu'une séquence vidéo et sonore peut être manipulée, il pourrait s'avérer particulièrement difficile pour un commissaire de vérifier en toute confiance les attributs propres au document faisant l'objet de l'attestation.

Conseil pratique
Consultez les ressources sur les pratiques exemplaires pour guider et documenter votre processus d'attestation à distance.

Pour en savoir plus :

- Barreau de l'Ontario, L'attestation à distance (dernière mise à jour en 2020).
- Groupe de travail de la FOPJC sur la lutte contre le blanchiment d'argent et le financement des activités terroristes, *Avis à la profession juridique concernant les risques* (décembre 2019).
- Barreau de l'Ontario, La passation et l'attestation à distance des testaments et des procurations sont elles permises dans le contexte de la COVID19? (dernière mise à jour le 19 février 2021).
- Barreau de l'Ontario, Pratiques exemplaires en matière d'attestation à distance (dernière mise à jour le 1er août 2020).
- Barreau de l'Ontario, Liste de contrôle d'attestation à distance (dernière mise à jour le 1er août 2020).
- Law Society of British Columbia, COVID19 Response (dernière mise à jour le 25 janvier 2021).
- Law Society of Alberta, COVID19 FAQ (dernière mise à jour le 27 novembre 2020).
- Société du Barreau du Manitoba, Can I use Virtual Commissioning in the Context of COVID19? (dernière consultation le 14 mars 2021)
- Law Society of Newfoundland and Labrador, Guidance to the Membership: Temporary Alternate Witnessing of Documents Act (mai 2020).

Identification et vérification d'identité à distance des clients

Les juristes doivent s'assurer qu'ils respectent les règles d'identification et de vérification d'identité des clients adoptées par le barreau de leur territoire, afin notamment de lutter contre le blanchiment d'argent et le financement d'activités terroristes.

Face à la pandémie de COVID19, certains barreaux ont indiqué qu'ils autoriseraient la

vérification d'identité des clients, lorsque celleci est requise, lors d'une réunion virtuelle. Cependant, les barreaux ont également averti que la vérification à distance de l'identité des clients devrait être considérée comme un « dernier recours » et que les juristes doivent être attentifs aux signaux d'alerte potentiels (voir les Avis à la profession juridique concernant les risques de la FOPJC). Comme alternative à la vérification d'identité à distance, les juristes devraient envisager d'autres options pour vérifier l'identité, comme la méthode de double processus (c'est-à-dire en se référant à deux sources fiables), ou en examinant le dossier de crédit canadien pour confirmer le nom, l'adresse et la date de naissance. Dans certains cas, les juristes peuvent se fonder sur la vérification antérieure effectuée par une autre personne ou sur celle effectuée par un agent. Si vous procédez à une vérification de l'identité à distance (le cas échéant), vous devriez envisager d'obtenir une image haute résolution du document d'identification avant la réunion virtuelle comme référence lorsque l'original du document d'identification est présenté à la réunion virtuelle. Les juristes doivent être attentifs au respect de la vie privée ou à toute autre disposition légale pouvant s'appliquer au traitement et à l'enregistrement de l'identification à distance des clients.[16] Il a également été recommandé que si un juriste vérifie l'identité du client par des moyens virtuels, la transaction soit traitée comme étant à risque élevé, et que le juriste documente les efforts engagés pour vérifier l'identité du client conformément aux règles existantes et les raisons pour lesquelles ils n'ont pas été en mesure de vérifier l'identité du client conformément aux règles existantes.

Comme pour l'authentification de signature et l'attestation à distance, il s'agit d'un domaine où les juristes doivent être particulièrement attentifs à l'évolution des règles et des approches à mesure que les restrictions liées à la pandémie de COVID19 évoluent.

Pour en savoir plus :

- Law Society of British Columbia, COVID19 Response (dernière mise à jour le 25 janvier 2021).
- Barreau de l'Ontario, Réponse à la COVID19 – FAQ : Gestion de la pratique (dernière consultation le 29 janvier 2021).
- Law Society of Alberta, COVID19 FAQ (dernière mise à jour le 27 novembre 2020).
- Barbara Buchanan, Knowing Your Client—Guidance and Rules during Covid19, Law Society of British Columbia, *Benchers' Bulletin* (été 2020)

[16] Voir, p. ex. la *Loi concernant le cadre juridique ds technologies de l'information*, CQLR c. C— 1.1, dont l'art. 44 prévoit que le consentement exprès doit être obtenu avant la vérification de l'identité d'une personne au moyen d'un procédé permettant l'enregistrement des données biométriques.

- Groupe de travail de la FOPJC sur la lutte contre le blanchiment d'argent et le financement des activités terroristes, *Avis à la profession juridique concernant les risques* (décembre 2019).
- Law Society of Saskatchewan, Client Identification and Verification (dernière consultation le 14 mars 2021).
- Law Society of Saskatchewan, Client Identification and Verification (19 décembre 2019).

Réunions, audiences et entrevues à distance

Les réunions virtuelles, y compris les audiences à distance devant les tribunaux, peuvent sembler moins formelles. Cependant, comme dans toute autre communication électronique, les juristes restent tenus de respecter les règles habituelles de déontologie professionnelle, notamment de civilité (règle 7.2-1) et de confidentialité (règle 3.3-1).

Dans certains contextes, un juriste n'aura pas le choix de la plateforme utilisée (p. ex. audiences devant un tribunal). En cas de flexibilité quant à la plateforme à utiliser, les juristes devraient envisager les mesures de sécurité nécessaires ou autrement prudentes pour assurer la confidentialité des clients et l'efficacité des services et communications avec les clients (règle 3.3-1, règle 3.1-2 et règle 3.2-1).

Dans les cas où un juriste dispose de latitude pour le choix de la plateforme, il devrait déterminer si la réunion nécessitera un véritable chiffrement de bout en bout, pour que même le fournisseur de logiciels n'ait pas accès au contenu de la conversation. Comme pour le courriel, les services de télécommunication insèrent généralement dans leurs contrats d'utilisation des clauses qui leur permettent d'accéder au contenu de vos conversations, ce qui rend l'utilisation de tels outils contraire aux obligations de confidentialité d'un juriste. Les clients peuvent décharger leurs juristes de ces obligations, mais seulement s'ils sont conscients des risques et les acceptent. Souvent, la confidentialité de la communication est déjà garantie dans la version payante des plateformes. Comme pour les courriels et les fichiers, en vue d'une communication extrêmement sensible, les juristes devraient choisir une plateforme sur laquelle ils peuvent contrôler les clés de chiffrement.

Dans tous les cas, l'accès à la salle de réunion virtuelle doit être soumis à un contrôle d'accès. Un contrôle d'accès courant consiste à exiger un mot de passe pour accéder à la réunion. Les juristes devraient également envisager d'utiliser une salle d'attente virtuelle, où les participants se connecteront et attendront que l'hôte leur accorde un accès spécifique.

Certains outils permettent d'enregistrer des conversations (audio, vidéo ou clavardage). La

règle 7.2-3 prévoit ce qui suit : « Un 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 ». Déterminez s'il y a une chance que la téléconférence soit enregistrée et, dans l'affirmative (et sous réserve des règles de votre territoire), assurez-vous que votre client est au courant de cette possibilité et a accepté l'utilisation de l'outil.

Il en va de même pour les procédures judiciaires. Les règles du tribunal peuvent interdire l'enregistrement d'une procédure. Même en l'absence de telles restrictions, la procédure ne doit être enregistrée qu'avec la connaissance et le consentement du tribunal.

Si les juristes (et les clients) ne peuvent garantir la confidentialité de leur environnement, des écouteurs devraient être utilisés pour empêcher des tiers d'écouter la réunion. La possibilité que des tiers se trouvent de l'autre côté de l'écran d'un client ou d'un témoin dans une entrevue est à prendre en considération. En particulier dans le cas d'une entrevue ou d'un témoignage, les juristes doivent vérifier si une autre personne est présente avec le témoin ou écoute sur un appareil et pourrait fournir des informations au témoin pendant l'entretien (tout en étant attentif à la vie privée de la personne et au fait que tout le monde n'est pas en mesure de s'isoler totalement).

Les juristes doivent également être attentifs à ce qui peut être vu en arrière-plan de leur vidéo, et s'assurer que cela ne divulgue aucune information confidentielle (p. ex. localisation, nom du client, dossier en cours). Une bonne pratique consiste à diriger la caméra vers un arrière-plan uni ou préparé, ou à utiliser un arrière-plan virtuel. Cependant, les juristes devraient également être conscients du fait que l'utilisation d'arrière-plans virtuels peut générer des risques dans certains contextes; ainsi, un arrière-plan virtuel pourrait masquer l'emplacement d'un client ou d'un témoin, ou cacher des individus qui pourraient influencer indûment un client ou un témoin.

Enfin, comme dans toute autre réunion, le juriste doit consigner la réunion immédiatement après sa conclusion, et transcrire par écrit toutes les instructions reçues ou les conseils donnés.

Pour en savoir plus :

- Barreau de l'Ontario, Réponse à la COVID19 — FAQ : Gestion de la pratique (dernière consultation le 29 janvier 2021).
- The Advocates' Society, *Best Practices for Remote Hearings* (13 mai 2020).
- LawPRO, Ten Tips for Effective VideoConferencing, *PracticePRO*

(8 avril 2020).

- LawPRO, Checklist de vidéoconférence *PracticePRO* (mars 2020).
- Cour supérieure de justice de l'Ontario, Étiquette et pratiques exemplaires pour les audiences à distance (2020).
- Division de la Colombie-Britannique de l'ABC, *Best Practices in a Zoom Courtroom* (2020).
- Law Society of British Columbia, Video Conferencing Technology Information (dernière consultation le 14 mars 2021).
- Law Society of British Columbia, Risks and Tips when using VideoConferencing Technology (dernière consultation le 14 mars 2021).

Signatures électroniques

La signature électronique permet de garantir l'authenticité, la non-répudiation et la traçabilité des documents. La question de savoir si une signature électronique est autorisée est une question de fond régie par les lois provinciales et territoriales ainsi que par toutes les règles et directives de pratique applicables des tribunaux. Les juristes doivent examiner les exigences législatives et autres applicables avant d'utiliser des signatures électroniques. Même si un territoire autorise la signature électronique dans certains contextes, il peut ne pas les autoriser pour tous les documents.

En supposant qu'une signature électronique soit autorisée, certaines pratiques exemplaires devraient être respectées. La signature électronique associe de manière fiable la personne à la signature et associe de manière fiable la signature au document. La définition même d'une signature électronique varie d'un territoire à l'autre. Dans tous les territoires, un marquage électronique est généralement considéré comme une signature légitime dans le contexte d'affaires. C'est généralement l'option la plus rentable, mais il pourrait y avoir des problèmes de fiabilité parce que les liens entre le signataire et le document peuvent donner lieu à un déni plausible et un risque accru de fraude. Une signature numérique peut faciliter la vérification de l'acte de signature. Quand l'authentification et la documentation sont essentielles (p. ex. documents notariés), les juristes devraient envisager l'adoption de systèmes de signature électronique plus avancés qui comprennent l'horodatage et l'empreinte du document par l'intermédiaire d'un tiers qui pourrait attester de l'heure, de l'authenticité et de l'intégrité des documents signés.

L'accès aux signatures électroniques, des plus simples aux plus avancées, doit être strictement contrôlé. Les juristes devraient exercer un contrôle total et savoir comment, quand et avec qui leur preuve de signature est partagée, et ainsi garantir des protections

à la vie privée et à la sécurité du client, puisque tout est sous le contrôle du juriste. Si vous utilisez une signature électronique, vous devez vous assurer que des mesures de sécurité ont été mises en place pour empêcher tout accès, utilisation ou copie non autorisés.

Pour en savoir plus :

- Barreau de l'Ontario, Réponse à la COVID19 — FAQ : Gestion de la pratique (dernière consultation le 29 janvier 2021).
- Peter A. Aziz, Marissa Daniels et Hailey Schnier, Canada: COVID19 And Electronic Signatures : A Guide for Organizations, *Mondaq* (14 juin 2020).
- LawPRO, Understanding esignatures, *PracticePRO* (2 juin 2020).

4. Présence en ligne des juristes

De nombreux juristes ont une présence en ligne sous la forme de sites Web ou de comptes de médias sociaux de cabinets juridiques. Certains juristes utilisent également le courriel à des fins de commercialisation, ainsi que pour communiquer sur des questions juridiques. En matière de commercialisation par des moyens en ligne, les juristes doivent s'assurer qu'ils respectent les règles de déontologie applicables à la commercialisation des services de juristes (voir règle 4.2). Il est également prudent que les juristes prennent des mesures pour se prémunir contre d'éventuels conflits d'intérêts pouvant survenir si un client potentiel envoie des renseignements confidentiels non sollicités. Les juristes doivent également se conformer aux lois applicables et aux règles et règlements de l'organisme compétent sur les courriels commerciaux non sollicités, comme la *Loi canadienne anti-pourriel*.

De plus en plus, les juristes ont une présence en ligne sur les réseaux sociaux. L'utilisation des médias sociaux par un juriste est assujettie aux règles de commercialisation de son barreau, mais peut également soulever des risques particuliers liés à la civilité et à la confidentialité des clients que les juristes doivent connaître et éviter activement.

Enfin, en créant leur présence en ligne, les juristes devraient connaître et adopter les pratiques exemplaires en matière d'accessibilité. Dans certains territoires, il y a des exigences légales sur l'accessibilité qui concernent les juristes.

Objectif : Maintenir une présence en ligne éthique et appropriée.

Vous trouverez ci-dessous un certain nombre des questions à poser dans le cadre de l'évaluation de la conformité, ainsi que les possibles systèmes et pratiques à mettre en œuvre pour parvenir

à ladite conformité.

Q: Des mesures appropriées sont-elles prises pour s'assurer que les communications électroniques sont accessibles?

- ✓ Toute présence professionnelle en ligne devrait respecter les Règles pour l'accessibilité des contenus Web (WCAG) 2.0, en veillant notamment à ce que tous les contenus soient parfaitement lisibles en texte (y compris les images).

Q: Les règles de déontologie applicables sont-elles respectées dans la commercialisation en ligne?

Les juristes devraient savoir que les pratiques suivantes peuvent contrevenir aux règles du barreau en matière de commercialisation :

- ✓ Être manifestement véridique, exacte et vérifiable.
- ✓ Ne pas être mensongère, ne pas prêter à confusion ou ne pas être trompeuse, ou ne pas risquer d'induire en erreur, de prêter à confusion ou de tromper.
- ✓ Correspondre à un haut niveau de professionnalisme.

Les juristes devraient savoir que les pratiques suivantes peuvent contrevenir aux règles du barreau en matière de commercialisation :

- × Indiquer une somme d'argent que le juriste a recouvrée pour un client ou faire référence au degré de réussite du juriste dans ses affaires antérieures, à moins que cette déclaration ne soit accompagnée d'une autre déclaration indiquant que les résultats passés ne sont pas nécessairement garants des résultats futurs et que le montant recouvré et les autres résultats d'un litige varieront en fonction des faits dans les affaires individuelles.
- × Suggérer une supériorité qualitative par rapport aux autres juristes.
- × Relever les attentes de manière injustifiée.
- × Suggérer ou impliquer que le juriste est combatif.
- × Dénigrer ou humilier d'autres personnes, groupes, organisations ou institutions.
- × Tirer profit d'une personne ou d'un groupe vulnérable.
- × Utiliser des témoignages ou des promotions qui contiennent des appels aux émotions.

Q: Des mesures sont-elles prises pour éviter de recevoir des renseignements ou documents confidentiels non sollicités ou autrement créer par inadvertance des relations avocat-client ou l'apparence de telles relations?

- ✓ Inclure des conditions d'utilisation et des avis de non-responsabilité qui avertissent les visiteurs du site de s'abstenir d'envoyer des renseignements ou des documents non sollicités au cabinet ou de laisser des renseignements

confidentiels sur la messagerie vocale, et que l'accès ou l'utilisation du site ou de la messagerie vocale du cabinet ne crée pas de relation avocat-client.

- × Éviter de répondre à des questions juridiques spécifiques ou de fournir autrement des conseils juridiques sur les médias sociaux.

Q: L'utilisation des médias sociaux est-elle conforme aux obligations déontologiques d'un juriste en matière de confidentialité, d'intégrité, de courtoisie, de discrimination et de harcèlement et d'encouragement au respect de l'administration de la justice?

- ✓ Les clients ou leurs affaires ne sont pas mentionnés dans les publications sur les réseaux sociaux, directement ou indirectement, sans le consentement des clients.
- ✓ Il convient d'être prudent avant d'utiliser les réseaux sociaux pour communiquer ou se connecter autrement avec les clients.
- ✓ Éviter de publier de matériel discriminatoire ou assimilable à du harcèlement.
- ✓ En ce qui concerne les obligations de civilité, faire preuve de jugement avant de critiquer d'autres juristes ou l'appareil judiciaire.

Q: Lors de l'envoi de courriels de commercialisation, les exigences des lois et de la réglementation canadiennes contre le pourriel sont-elles respectées?

- × Aucun message électronique commercial ne devrait être envoyé à un tiers sans son consentement préalable.

- ✓ Les messages électroniques commerciaux doivent fournir l'identité et les coordonnées de la personne qui a envoyé le message et, le cas échéant, de la personne au nom de laquelle il est envoyé; prévoir un mécanisme de désabonnement, sans frais et aussi simple que le mécanisme d'abonnement.

Accessibilité du contenu Web

Les sites et le contenu Web peuvent poser des problèmes d'accès aux personnes handicapées. Ainsi, des problèmes d'accessibilité surviennent souvent lorsque les documents sont formatés à l'aide de styles qui peuvent entraver l'accessibilité des personnes utilisant des dispositifs d'assistance comme les lecteurs d'écran.

Toutes les communications publiques des juristes devraient être accessibles et respecter les pratiques exemplaires en matière d'accessibilité telles que les Règles pour l'accessibilité des contenus Web (WCAG) 2.0 du World Wide Web Consortium (W3C) (ISO/IEC 40500). Dans certaines provinces, il s'agit désormais d'une obligation légale (par exemple en Ontario, à compter du 1er janvier 2021, toutes les entreprises de plus de 50 employés sont

tenues de respecter ces règles).

Pour en savoir plus :

- W3C, Vue d'ensemble des Règles pour l'accessibilité des contenus Web (WCAG) (dernière mise à jour le 17 octobre 2020).
- Gouvernement de l'Ontario, Comment rendre les sites Web accessibles (dernière mise à jour le 19 octobre 2020).
- ARCH Disability Law Centre, Conseils aux avocats et aux parajuristes pour fournir des services juridiques accessibles aux personnes ayant un handicap en Ontario (janvier 2019)

Règles de commercialisation du barreau

Dans leurs activités de commercialisation en ligne, que ce soit par le biais de sites Web de cabinets juridiques, de comptes de médias sociaux ou de courriels, les juristes doivent se conformer aux règles de leur code de déontologie professionnelle. De nombreux territoires ont adopté la règle 4.2-1 du *Code type*, qui stipule qu'un 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, et c) cette publicité soit dans le meilleur intérêt du public et respecte un niveau élevé de professionnalisme.[17] La règle 4.3-1 prescrit également qu'un juriste « ne doit pas annoncer sa spécialité dans un domaine particulier à moins d'avoir été agréé comme spécialiste dans ce domaine par l'ordre professionnel de juristes ».[18] Il est également recommandé que, lorsque les juristes font des déclarations dans des forums ou des formats électroniques généralement accessibles, ces déclarations comprennent le nom, l'adresse postale du cabinet juridique, le territoire d'exercice autorisé et l'adresse courriel d'au moins un juriste responsable de la communication.

Il s'agit toutefois d'un domaine où les juristes devraient tenir compte des règles pertinentes dans leur territoire. Par exemple, le *Code de déontologie* du Barreau de l'Ontario contient des commentaires supplémentaires sur l'utilisation de récompenses, de classements et d'endossements de tiers dans la commercialisation des juristes, ainsi

[17] Pour les affaires disciplinaires du barreau traitant de la règle 4.21 dans le cadre de la présence en ligne d'un avocat, voir, par exemple, L*aw Society of Ontario v. Goldfinger*, 2018 ONLSTH 10, appel accueilli en partie 2020 ONLSTA 3; *Law Society of Ontario v. Weinles*, 2018 ONLSTH 105; et *Law Society of Ontario v. Forte*, 2019 ONLSTH 9.

[18] Pour les affaires disciplinaires du barreau traitant de la règle 4.31, voir, par exemple, *Law Society of Ontario v. Goldfinger*, 2020 ONLSTA 3 et L*aw Society of Ontario v. Mazin*, 2019 ONLSTH 35.

que des exigences spécifiques sur la publicité d'un prix pour exécuter une transaction immobilière résidentielle.

Pour en savoir plus :

- Barreau de l'Ontario, Technologies, *Lignes directrices sur la gestion d'un cabinet juridique* (dernière mise à jour en 2020).
- Law Society of Alberta, Effective and Ethical Advertising (dernière consultation le 14 mars 2021).

Éviter les relations juriste-client involontaires

Recevoir des renseignements confidentiels d'une personne par le biais du site Web d'un cabinet juridique, d'un courriel ou d'un compte sur un réseau social peut créer des enjeux de conflit d'intérêts même si cette personne ne devient pas un client. Dans le même ordre d'idées, parce qu'une relation juristeclient peut être établie sans versement officiel de provision (voir, p. ex. règle 1.1-1, définition de « client »), les juristes doivent également veiller à ce que leur présence en ligne ne crée pas par inadvertance une relation juristeclient ou ne donne pas cette impression.

Afin d'éviter des problèmes, les juristes devraient envisager d'inclure sur leurs sites Web des conditions d'utilisation et des avis de non-responsabilité qui avertissent les visiteurs du site de s'abstenir d'envoyer des renseignements ou des documents non sollicités au cabinet ou de laisser des renseignements confidentiels sur la messagerie vocale, et préciser que l'accès ou l'utilisation du site ou de la messagerie vocale du cabinet ne crée pas de relation juriste-client. Pour éviter la création involontaire de relations juriste-client, les juristes doivent également veiller à ne pas répondre à des questions juridiques spécifiques sur les plateformes de médias sociaux.

Pour en savoir plus :

- ABC, Liste de vérification pour éviter les clients fantômes, *Trousse d'outils sur les conflits d'intérêts* (2020).

Problèmes déontologiques découlant de l'utilisation des médias sociaux

Sur les médias sociaux, les juristes doivent veiller à ne pas révéler de renseignements confidentiels sur les clients (règle 3.3-1). Il faut bien entendu éviter de faire explicitement référence aux clients et aux affaires des clients. En outre, comme indiqué dans les règles de déontologie professionnelle, un juriste « doit éviter les conversations et autres

communications indiscrètes… au sujet des affaires d'un client et doit rester à l'écart de tous les commérages à ce sujet même si le client n'est pas nommé ou autrement identifié » (règle 3.3-1, commentaire [8]).

Les juristes doivent également être conscients des risques liés à l'utilisation des médias sociaux et à la divulgation involontaire de renseignements confidentiels relatifs aux clients. Par exemple, les services de messagerie proposés par les plateformes de médias sociaux ne sont généralement pas sécurisés et il convient d'être prudent avant d'utiliser ces services pour communiquer avec les clients. En outre, en se connectant à un client par le biais des médias sociaux, par exemple en s'inscrivant à une liste « d'amis » ou en « suivant » un client, il est possible d'en déduire que le client a retenu les services d'un juriste. Les juristes doivent se prémunir contre les applications de médias sociaux qui consultent ou publient leurs listes de contacts dans leurs dispositifs électroniques, car cela peut également constituer une violation de la confidentialité.

Plusieurs caractéristiques des médias sociaux, leur caractère relativement informel, la rapidité des communications et le flou potentiel entre le personnel et le professionnel peuvent aussi présenter des risques pour les juristes en ce qui concerne leurs obligations en matière de civilité (voir, par exemple, règle 7.2-1 et règle 7.2-4). On sait maintenant que les plateformes de médias sociaux peuvent parfois être des lieux de conflits extrêmes et de commentaires inutilement grossiers, voire discriminatoires ou harcelants. En même temps, il est également bien établi que les barreaux doivent tenir compte de la liberté d'expression des juristes lorsqu'ils réglementent l'obligation de civilité des juristes et que les juristes ont un rôle de leadership important à jouer dans l'éducation du public et la recherche d'améliorations dans le système juridique.

Par exemple, selon la règle 5.6-1, un juriste doit « encourager le public à respecter l'administration de la justice et doit aussi s'efforcer d'améliorer l'administration de la justice ». Le commentaire de cette règle précise en outre que « la formation, la position particulière et l'expérience du juriste lui permettent d'observer le fonctionnement des lois, des institutions juridiques et des autorités publiques et d'en découvrir les forces et les faiblesses. Un juriste doit donc donner l'exemple en cherchant à améliorer le système judiciaire, mais ses critiques et suggestions doivent être faites de bonne foi et de façon éclairée ». Il faut aussi préciser que, selon la règle 5.6-2 « un juriste qui demande des modifications législatives ou administratives doit divulguer s'il agit dans son propre intérêt, dans l'intérêt du client ou dans l'intérêt du public ».

Un juriste doit également tenir compte de la règle 7.5 (« Présences en public et déclarations publiques ») et des commentaires y afférents qui stipulent, entre autres, que « en vertu de son devoir envers son client, un juriste doit s'assurer que toute

communication sert les intérêts de son client et reste dans la cadre de son mandat avant de faire une déclaration publique concernant les affaires de son client » et que « les communications publiques au sujet des affaires d'un client ne doivent pas servir à faire de la publicité pour le juriste et laisser entendre que le juriste cherche en fait à se glorifier et à servir ses propres ambitions ».

Les juristes ne devraient donc pas craindre de participer à des discussions sur les médias sociaux, y compris sur des sujets controversés. En même temps, il convient de faire preuve de prudence et de jugement afin d'agir de manière cohérente avec ses obligations professionnelles en matière de confidentialité, d'intégrité, de civilité et de discrimination et de harcèlement. Pour être plus précis sur l'équilibre à trouver, il a été récemment suggéré que les avocats évitent de publier sur les médias sociaux des commentaires critiques sur un avocat adverse identifiable, ou s'abstiennent de s'adonner à des attaques personnelles contre la justice ou de critiquer injustement des décisions judiciaires dans leurs déclarations publiques, y compris dans les médias sociaux.

Pour en savoir plus :

- La Société des plaideurs, *Principles of Civility and Professionalism for Advocates* (20 février 2020).
- Robyn Schleihauf, Conduct Unbecoming: What should the Society do when it comes to gossip, online posts and bad behaviour on social media?, *Nova Scotia Barristers Society* (février 2020).
- EPIQ, Social Media Ethical Obligations for Lawyers (2019).
- State Bar of Michigan, Ethics of Social Media—LinkedIn Frequently Asked Questions, (mai 2017).
- ABA, The Minefield of Social Media and Legal Ethics (24 mars 2017).
- Stacey McPeek, Lawyers and Social Media, *Law Society of Saskatchewan* (8 février 2017).

Messages courriel non sollicités et lois anti-pourriel

Lorsqu'ils envoient des courriels ou d'autres messages électroniques, les juristes doivent également connaître les exigences de la *Loi canadienne anti-pourriel* qui s'applique aux messages électroniques à des fins commerciales, notamment les messages qui offrent des services et qui font de la publicité ou de la promotion de ces services, ou d'une personne qui fournit ces services. Aucun message électronique commercial ne devrait être envoyé à un tiers sans son consentement préalable. Bien que le consentement devrait généralement être explicite, il peut être implicite s'il y a une relation d'affaires existante, ou si le destinataire a publié ses coordonnées en ligne, ou directement à l'expéditeur, sans mentionner qu'il n'a pas souhaité être sollicité. Au-delà du consentement, le message doit indiquer l'identité et les coordonnées de la personne qui a envoyé le message et, le cas échéant, de la personne au nom de laquelle il est envoyé; prévoir un mécanisme de désabonnement, sans frais et aussi simple que le mécanisme d'abonnement.

Pour en savoir plus :

- *Loi canadienne anti-pourriel*, SC 2010, ch. 23
- ISDE, Centre de ressources sur la Loi canadienne anti-pourriel (dernière mise à jour le 21 avril 2020).
- Ava Ghisling, What's it all about? How antispam legislation can affect your firm?, *EnPratique de l'ABC* (18 mars 2019).