Guide des TI

GESTION ET SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION POUR L'AVOCAT ET SON ÉQUIPE

Votre utilisation des technologies de l'information (TI) est-elle conforme à vos obligations quant au secret professionnel ?

Votre gestion des TI est-elle aussi efficace qu'elle devrait l'être ?

EN D'AUTRES MOTS… PASSEZ-VOUS LE TEST ?

Barreau du Québec

AVIS AU LECTEUR

Ce guide contient des conseils et des recommandations qui sont une application des règles auxquelles les membres du Barreau sont déjà assujettis. Quoique ce Guide fasse l'objet de mises à jour périodiques, seule la version en ligne, disponible à **guideTI.barreau.qc.ca**, doit être considérée comme à jour.

Bien que le contenu du guide ne soit pas contraignant et n'exclut pas l'utilisation d'autres outils, les autorités et instances disciplinaires ou judiciaires pourraient s'en inspirer pour évaluer le comportement d'un membre du Barreau.

Des experts bénévoles ont participé à l'élaboration de ce guide. Toutefois, son contenu n'engage que la responsabilité du Barreau.

Enfin, le matériel informatique et les logiciels mentionnés, de même que les références contenues dans ce guide ou les solutions proposées, ne font l'objet d'aucun cautionnement de la part du Barreau du Québec. Veuillez noter que l'utilisation de l'évaluation « 24 questions pour évaluer votre utilisation des TI » est totalement anonyme et que les données transmises ne pourront en aucun cas servir à vous identifier auprès de l'Inspection professionnelle du Barreau.

guideTI.barreau.qc.ca

24 QUESTIONS POUR ÉVALUER VOTRE UTILISATION DES TECHNOLOGIES DE L'INFORMATION

Répondez aux questions suivantes au meilleur de vos connaissances.

Si vous répondez **NON** ou si vous ignorez la réponse, ***suivez le GUIDE DES TI en ligne !***

Rendez-vous au **guideTI.barreau.qc.ca** pour trouver l'information sur chacune des questions de ce test.

Dans votre cabinet ou votre organisation		OUI	NON	NE SAIS PAS	SUIVEZ LE GUIDE !
1	Avez-vous mis en place des mesures de sécurité pour protéger votre réseau informatique?	○	○	○	Réseautique
	Si oui, existe-t-il une politique sur l'utilisation des TI qui documente ces mesures de sécurité?	○	○	○	
2	Chaque utilisateur utilise-t-il un nom d'usager et un mot de passe pour ouvrir une session de travail sur son ordinateur?	○	○	○	• Mot de passe • Réseautique
3	Si oui, le mot de passe est-il obligatoirement : • Modifié au moins tous les 30 jours?	○	○	○	Mot de passe
	• Composé d'un minimum de 10 caractères incluant au moins une majuscule, une minuscule, un chiffre et un symbole?	○	○	○	
4	Les sessions de travail sont-elles verrouillées automatiquement avec un écran de veille et un mot de passe lorsqu'un poste de travail reste inactif pendant une période maximale de trois minutes?	○	○	○	Réseautique
5	Votre réseau est-il protégé par un pare-feu mis à jour régulièrement (aussi nommé coupe-feu ou *firewall* en anglais)?	○	○	○	Réseautique
6	Chaque poste de travail est-il protégé par un antivirus mis à jour automatiquement?	○	○	○	Réseautique
7	Vos logiciels (ex. : Word ou Explorer) et vos systèmes d'exploitation (ex. : Windows ou Mac OS) sont-ils mis à jour automatiquement?	○	○	○	Réseautique
8	Si vous avez un réseau sans fil (WiFi) : • Avez-vous modifié le code d'administrateur par défaut du routeur sans fil (point d'accès où les ordinateurs se connectent)?	○	○	○	Réseautique
	• Avez-vous modifié le mot de passe par défaut du routeur sans fil?	○	○	○	
	• Avez-vous mis en place une méthode de chiffrement (cryptage) des données qui transitent sur le réseau sans fil?	○	○	○	
	• Avez-vous configuré le routeur sans fil afin qu'il accepte seulement les communications en provenance des ordinateurs de votre réseau?	○	○	○	
	• Avez-vous bloqué la diffusion publique du nom de votre réseau sans fil?	○	○	○	
9	Les données enregistrées par les utilisateurs sur un ordinateur portable, une tablette ou sur des supports amovibles (clé USB, disque dur externe, etc.) sont-elles chiffrées?	○	○	○	Réseautique
10	Autorisez-vous vos employés à travailler avec leur équipement informatique personnel?	○	○	○	Équipement personnel
	Si oui, avez-vous une politique permettant de vous assurer de la sécurité de ces appareils et de la gestion des risques?	○	○	○	
11	Les utilisateurs qui travaillent de leur résidence disposent-ils d'une connexion RPV (Réseau privé virtuel — VPN en anglais) protégeant leur session de travail?	○	○	○	Réseautique

Dans votre cabinet ou votre organisation	OUI	NON	NE SAIS PAS	SUIVEZ LE GUIDE !
12 En ce qui concerne les téléphones intelligents utilisés par les employés : • Une authentification par un mot de passe sécuritaire (voir question 3) est-elle nécessaire pour accéder à leurs contenus ? • La mise en veille automatique a-t-elle été configurée ? • Le chiffrement des informations a-t-il été configuré ?	○ ○ ○	○ ○ ○	○ ○ ○	• Cellulaire • Mot de passe • Chiffrement
13 Les connexions Bluetooth sont-elles configurées pour ne pas être disponibles par défaut et pour être sécurisées lorsqu'elles sont utilisées ?	○	○	○	Cellulaire
14 L'accès aux documents électroniques et aux courriels conservés sur votre réseau est-il réservé aux personnes concernées seulement ?	○	○	○	Communications électroniques
15 Les communications avec vos clients sont-elles protégées par un mot de passe, par l'utilisation d'un réseau fermé sécurisé avec le client ou par chiffrement ?	○	○	○	Communications électroniques
16 Avez-vous mis en place une méthode de classement des documents enregistrés sur vos ordinateurs et de vos courriels conforme au *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats* ?	○	○	○	• Communications électroniques • Classement des documents
17 Avez-vous mis en place une méthode de gestion des copies de sauvegarde des données enregistrées sur votre réseau (ordinateurs, serveurs, téléphones intelligents, etc.) ?	○	○	○	Copie de sauvegarde des documents
18 Saviez-vous que certains documents contiennent des données confidentielles cachées qui peuvent être transmises à votre insu (commentaires ou suivi des corrections de Word, par exemple) et prenez-vous les mesures nécessaires afin d'éviter cela ?	○	○	○	Métadonnées
19 Avez-vous des processus de sécurité informatique pour gérer le départ d'un employé (suppression de compte usager, de l'accès aux documents confidentiels, du compte de téléphonie, etc.) ?	○	○	○	Départ d'un employé
20 Les ententes conclues avec vos fournisseurs (p. ex. : technicien en informatique, service d'hébergement, infonuagique) sont-elles conformes à vos obligations déontologiques (confidentialité, etc.) ?	○	○	○	• Entente avec les fournisseurs • Infonuagique
21 Vos bureaux et votre équipement informatique sont-ils sécurisés ?	○	○	○	Sécurisation des locaux et de l'équipement
22 Avez-vous une procédure de mise au rebut ou de recyclage sécurisé du matériel informatique ?	○	○	○	Mise au rebut/ recyclage
23 Gérez-vous les alertes de sécurité concernant, par exemple, vos copies de sauvegarde ou les tentatives d'intrusion dans vos systèmes ?	○	○	○	Surveillance et alertes
24 Disposez-vous d'un plan de continuité des affaires en cas de désastre ?	○	○	○	Copie de sauvegarde des documents

Introduction

La sécurité informatique vise généralement ces objectifs :

- La confidentialité des données (rendre l'information inintelligible à d'autres personnes que celles autorisées);
- Leur intégrité (s'assurer que les données n'ont pas été altérées durant la communication de manière accidentelle ou intentionnelle);
- Leur disponibilité (garantir l'accès à un service ou à des ressources).

L'utilisation des technologies de l'information (TI) interpelle les avocats dans l'exercice de leur profession à plusieurs égards, mais principalement quant au secret professionnel et à leur devoir de compétence. Ce guide a donc été conçu afin d'aider les avocats à se conformer à leurs obligations déontologiques.

Puisque la sécurité d'un système informatique requiert une approche globale, plusieurs niveaux d'intervention seront explorés dans ce guide, par exemple :

- **La sécurité des télécommunications** (technologies réseau, serveurs, réseaux d'accès, etc.)
- **La sécurité des infrastructures matérielles (**salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail personnels, etc.)
- **La sensibilisation des utilisateurs** (formation des employés, processus internes conformes et politique en matière de sécurité, etc.)

Les conseils et recommandations contenus dans ce guide ne sont pas spécifiquement codifiés dans la législation ou la réglementation encadrant l'exercice de la profession d'avocat (y compris le *Code de déontologie*). On pourrait donc considérer que le présent guide décrit les meilleures pratiques et/ou celles généralement reconnues au moment de sa dernière mise à jour.

Ceci dit, il faut aussi garder à l'esprit que, même en l'absence d'une norme spécifique établie par la législation ou la réglementation, le Conseil de discipline possède, du fait des articles 59.2[1] et 152[2] du *Code*

[1] Article 59.2 : Nul professionnel ne peut poser un acte dérogatoire à l'honneur ou à la dignité de sa profession ou à la discipline des membres de l'ordre, (…).

[2] Article 152 **:** Le conseil décide privativement à tout tribunal, en première instance, si l'intimé a commis une infraction visée à l'article 116.

En l'absence d'une disposition du présent code, de la loi constituant l'ordre dont l'intimé est membre ou d'un règlement adopté conformément au présent code ou à cette loi et applicable au cas particulier, le conseil décide de la même manière :

1° si l'acte reproché à l'intimé est dérogatoire à l'honneur ou à la dignité de la profession ou à la discipline des membres de l'ordre, (…).

des professions, une juridiction résiduaire exclusive pour décider si une action ou une omission constitue un acte dérogatoire, ou non.

Le secret professionnel

Par la nature des tâches et des responsabilités accomplies dans l'exercice de leur profession, les membres du Barreau du Québec sont appelés à recueillir des renseignements confidentiels auprès de leurs clients[3] pour ensuite les analyser, les utiliser, les communiquer, les conserver et éventuellement, les supprimer, afin de fournir des services juridiques de qualité.

Par « renseignements confidentiels », on entend des informations faisant l'objet de contraintes contractuelles ou légales (qui n'ont donc pas vocation à circuler librement) et dont le responsable (débiteur de l'obligation de confidentialité) doit veiller à la protection. Cela inclut, entre autres, les renseignements personnels, les secrets commerciaux ou industriels, l'information protégée par le secret professionnel et le privilège relatif au litige.

Outre la législation protégeant la confidentialité de ces renseignements[4], la Cour suprême du Canada a érigé le secret professionnel des avocats en règle de fond et principe fondamental de notre système de justice[5].

---

[3] Il s'agit d'ailleurs là d'un critère fondamental pour décider de l'opportunité de constituer un ordre professionnel – *Code des professions*, art. 25(5).

[4] *Charte des droits et libertés de la personne*, art. 9, *Code des professions*, art. 60.4, *Loi sur le Barreau*, art. 131(1), *Code de déontologie des avocats*, art. 60 et ss. et *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, art.17.

[5] Voir notamment *Lavallée, Rackel & Heintz* c. *Canada (Procureur général); White, Ottenheimer & Baker* c. *Canada (Procureur général)*; *R.* c. *Fink*, [2002] 3 R.C.S. 209. *R.* c. *Brown*, [2002] 2 R.C.S. 185; *Maranda* c. *Richer*, [2003] 3

L'utilisation des TI par les avocats commande donc que ceux-ci prennent toutes les précautions nécessaires afin qu'aucun accroc au respect du secret professionnel ne survienne. À ce sujet[6], l'article 34 de la *Loi concernant le cadre juridique des technologies de l'information*[7] (la « LCCJTI ») se lit comme suit :

> « 34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication.
>
> La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant. »

Pour ce faire, les avocats ont la responsabilité d'agir de façon prudente et diligente. Cela n'est possible que dans la mesure où ils prennent le temps de s'informer adéquatement quant aux TI utilisées, aux risques inhérents à leur utilisation ainsi qu'aux méthodes ou aux solutions assurant la prévention ou la réduction de ces risques.

L'article 61 du *Code de déontologie* prévoit que l'avocat doit prendre « les moyens raisonnables pour assurer la protection des renseignements confidentiels par toute personne qui coopère avec lui dans l'exerce de ses activités professionnelles, de même que, le cas échéant, par le cabinet au sein duquel il exerce de telles activités. L'article 61 précise aussi que lorsqu'il exerce ses activités au sein d'une organisation, l'avocat doit prendre « les moyens raisonnables pour que celle-ci mette à sa disposition les moyens nécessaires pour lui permettre d'assurer la protection des renseignements confidentiels »[8]. Ces moyens raisonnables devraient s'étendre aux équipements, systèmes et programmes informatiques que l'avocat et les membres de son équipe utilisent.

R.C.S. 193; *Société d'énergie Foster Wheeler ltée* c. *Société intermunicipale de gestion et d'élimination des déchets (SIGED) inc.*, [2004] 1 R.C.S. 456.

[6] De plus, l'article 60.4 du *Code des professions* prévoit ceci : « ***Renseignement confidentiel***. Le professionnel doit respecter le secret de tout renseignement de nature confidentielle qui vient à sa connaissance dans l'exercice de sa profession. […] »

[7] *Loi concernant le cadre juridique des technologies de l'information*.

[8] Voir aussi à cet égard les articles 5, 6 et 60 du *Code de déontologie des avocats*.

Le devoir de compétence

Outre la question de la protection des renseignements confidentiels, connaître et savoir comment utiliser les TI constitue aujourd'hui une des composantes importantes de la notion de compétence[9] que l'avocat doit démontrer en tout temps dans la prestation de services juridiques[10]. Qui pourrait aujourd'hui imaginer qu'un avocat puisse pratiquer le droit sans ordinateur, logiciel de traitement de texte, courriel, accès à Internet, ou sans connaître et savoir utiliser les ressources documentaires électroniques – législation, doctrine et jurisprudence[11]?

Aussi, selon le type de pratique d'un avocat ou en regard d'un dossier en particulier, la connaissance des médias sociaux peut aussi être perçue comme une des facettes de l'obligation de compétence[12].

[9] Le Service de l'inspection professionnelle du Barreau du Québec : « Définir la compétence : Un avocat compétent se reconnaît à : (...) sa maîtrise des moyens et des techniques disponibles lui permettant d'appliquer ses connaissances avec pertinence, habileté et efficacité; sa capacité de mettre en œuvre ces connaissances, ces moyens et ces techniques en constituant des dossiers qui documentent la cueillette de l'information importante, les avenues disponibles, la justification des choix professionnels, leur conformité avec les objectifs et décisions du client et les étapes de réalisation des objectifs (dépliant du Service de l'inspection professionnelle « *Faites-vous une loi de viser l'excellence* »).

[10] *Code de déontologie des avocats*, art. 10, 20, 21 et 29.

[11] Voir D. Jaar et F. Sénécal, *Les obligations de l'avocat face aux technologies de l'information*, Développements récents en déontologie, droit professionnel et disciplinaire, Barreau du Québec, 2010. www.caij.qc.ca/doctrine/developpements_recents/323/1770/index.html.

[12] Sur ce sujet voir notamment : *Social Media and the Lawyer's Evolving Duty of Technological Competence*, Benjamin P Cooper, *Legal Ethics*, 2014, Volume 17, Part 3, http://dx.doi.org/10.5235/1460728X.17.3.463). Le nouveau *Code de déontologie des avocats* fait d'ailleurs maintenant référence explicite à l'utilisation des médias sociaux à l'article 1.

SECTION 1 SÉCURITÉ DES COMMUNICATIONS

Un aspect important de la gestion des affaires de l'avocat réside dans la sécurité de l'information qu'il manipule. La circulation de cette information doit être bien encadrée. Dans un monde de papier, le contrôle de l'information s'opère par un contrôle physique des documents et des lieux. Dans un monde électronique, de nouvelles formes de sécurité doivent également être prises en compte.

La première section de ce guide vise la sécurité des réseaux informatiques, de la téléphonie et des communications électroniques.

Réseautique

Principe

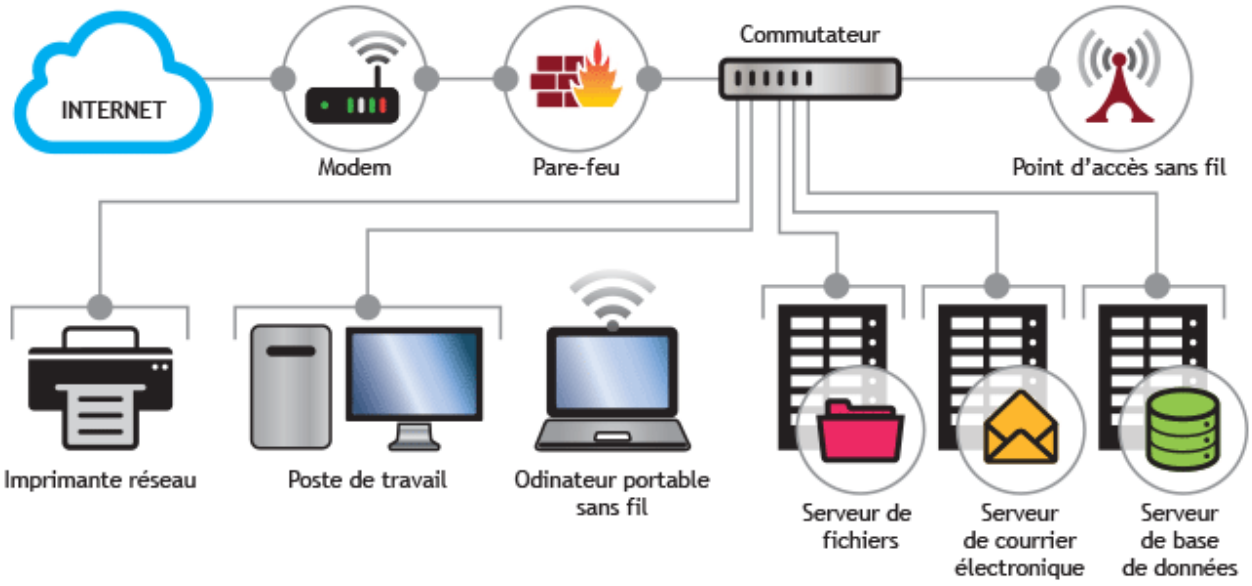
L'avocat doit mettre en place une politique encadrant l'utilisation de son réseau informatique ainsi que des mesures de sécurité pour en assurer la protection. Cette politique doit permettre à l'avocat de s'assurer que son réseau informatique est conforme à ses obligations déontologiques (secret professionnel, secrets commerciaux et industriels, renseignements personnels, etc.).

Définition

La réseautique vise l'ensemble des techniques relatives à la création, au maintien et à l'utilisation d'un réseau informatique. Ce dernier est formé d'ordinateurs et de périphériques, comme des imprimantes, des numériseurs, des téléphones intelligents, des tablettes, des serveurs, des commutateurs, des routeurs et des modems, reliés au moyen de matériel – avec ou sans fil – et de logiciels.

Les réseaux informatiques reliant plusieurs ordinateurs permettent aux utilisateurs de partager des données. Leur avantage réside dans la rapidité d'accès à l'information et l'amélioration de la productivité et de la collaboration. Les données contenues dans les réseaux informatiques sont souvent de nature confidentielle et doivent par conséquent être protégées. De plus, une même donnée placée sur un serveur partagé par plusieurs utilisateurs peut ne pas être destinée à être consultée par tous. Dans ces cas, la consultation de ces données devrait être subordonnée à l'octroi de droits d'accès préétablis. Cela peut s'avérer important lorsque la mise en place d'une « muraille de Chine » est nécessaire pour éviter des conflits d'intérêts apparents ou potentiels, ou pour éviter la dissémination d'information à des catégories d'utilisateurs qui n'ont pas à en prendre connaissance (principe du « besoin de savoir »).

Voici un graphique représentant un réseau comprenant un serveur, des postes de travail, un commutateur et un pare-feu.



Utilité

La mise en réseau d'ordinateurs permet :

a. Le partage de ressources (fichiers, applications, matériel, connexion à Internet, etc.);
b. La communication entre utilisateurs (courriel, messagerie instantanée, etc.);
c. La communication entre divers processus (p. ex., entre une application comptable et une application de facturation du temps passé sur un appel téléphonique), ce qui automatise les tâches et réduit le risque d'erreurs d'écriture;
d. La possibilité de trouver la bonne information à jour (utilisation de bases de données);
e. L'enregistrement centralisé de données.

Risques

Chaque ordinateur connecté à un réseau peut être exposé au monde extérieur et ainsi être victime d'une intrusion, d'une tentative de piratage ou, plus généralement, d'une atteinte à l'intégrité du système informatique et des données qu'il comporte.

Cette menace est d'autant plus grande lorsque l'ordinateur est connecté en permanence à Internet, ce qui est de plus en plus souvent le cas. Pour savoir si votre ordinateur est connecté en permanence à Internet, sur un PC, vous devez regarder en bas à droite de votre écran et repérer les petites lignes réseau ou un symbole de câble. Sur un Mac, regardez plutôt en haut à droite.

De nos jours, avec la mise en place de réseaux sans fil, l'utilisation de téléphones intelligents (p. ex., iPhone, Android, BlackBerry,etc.), l'établissement de connexions à distance ou l'usage d'appareils à connexion sans fil Bluetooth, les données sensibles sont de plus en plus exposées et vulnérables à des risques d'accès et de divulgation non autorisés qui sont externes au bureau physique.

Il est important de s'assurer que les données conservées sur votre réseau informatique sont sécurisées. Voici quelques points à vérifier :

L'utilisation d'un mot de passe et la déconnexion des sessions inactives

Afin de protéger l'information contenue sur un réseau informatique, il est important de protéger l'accès à tous les postes de travail qui sont connectés au réseau. Ainsi, il est recommandé d'utiliser une méthode d'authentification de l'utilisateur (code d'utilisateur et mot de passe) lorsqu'il se connecte sur son poste de travail. La plupart des systèmes d'exploitation réseau permettent ce genre d'authentification. Le mot de passe devrait être modifié périodiquement (aux 30 jours) et être composé d'un code contenant un minimum de dix caractères (ou plus, selon les possibilités du système). Ce mot de passe devrait inclure au moins une majuscule, une minuscule, un chiffre et un symbole.

Il est également important de déconnecter ou de verrouiller un poste de travail ou une session inactive afin d'éviter la prise de contrôle de ce poste de travail par un tiers et ainsi donner accès aux données confidentielles. La configuration d'un mot de passe sur l'écran de veille après une période maximale de trois minutes d'inactivité peut remplir cette fonction. Une configuration permettant un blocage du système pendant 15 à 30 minutes après cinq tentatives d'identification est aussi une bonne mesure de sécurité.

L'utilisation d'un antivirus polyvalent mis à jour régulièrement

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer les logiciels malveillants. Selon le produit utilisé, l'outil pourra également reconnaître un pourriel (*spam*) ou encore un logiciel espion (vers, témoins – communément appelés cookies –, etc.), et ainsi empêcher l'installation de logiciels de type Cheval de Troie, qui peuvent ouvrir une brèche donnant accès à un ordinateur faisant partie de votre réseau. La protection conférée par ces logiciels devrait s'accompagner de pratiques responsables, notamment quant à l'ouverture de pièces jointes provenant d'un courriel non sollicité ou de source non sûre.

L'utilisation d'un pare-feu

Un pare-feu (aussi nommé coupe-feu ou *firewall* en anglais) est un élément du réseau informatique, logiciel et/ou matériel, qui permet de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment Internet). L'objectif est de fournir une connexion sécuritaire et de contrôler les échanges de flux entre les différentes zones de confiance afin de laisser passer les données tout en respectant les règles de sécurité établies. Ainsi, une requête d'accès à un document provenant d'Internet sera refusée alors que cette même requête, provenant d'un utilisateur du même réseau, sera acceptée. Il est donc très important d'installer un pare-feu sur le réseau de votre organisation. À noter que certaines méthodes permettent d'authentifier des requêtes provenant d'Internet, ce qui facilite le télétravail sécuritaire.

Attention, bien que certains routeurs puissent contenir un pare-feu, le routeur n'en est pas un! Son rôle est de permettre à plusieurs équipements informatiques (ordinateurs, téléphones intelligents, téléphones IP, etc.) de partager un lien Internet. S'il peut être configuré pour laisser passer ou pour bloquer le trafic en provenance d'Internet, ce n'est pas son rôle premier. À la différence du pare-feu, il ne peut gérer le trafic entre des zones de confiance différentes.

Mise à jour des logiciels et des systèmes d'exploitation

Un logiciel ou un système d'exploitation, même après sa commercialisation, peut comporter des failles permettant à des programmeurs malveillants de les utiliser et de compromettre votre système.

La plupart des logiciels et des systèmes d'exploitation récents sont livrés avec des options de mises à jour[13]. Si votre poste de travail vous indique qu'une mise à jour est disponible, il est généralement recommandé de procéder à cette mise à jour. Avant d'installer celle-ci, assurez-vous qu'elle ne cause pas de faille informatique.

La connaissance de l'existence de ces failles se propage rapidement; c'est pourquoi il est recommandé de suivre les configurations par défaut et de choisir les options de mises à jour courantes ou périodiques prescrites par le fabricant (excluant les versions bêta ou en développement d'un logiciel qui pourraient engendrer des risques).

Sécuriser les réseaux sans fil (WiFi)

L'utilisation de réseaux sans fil donne l'avantage de connecter un ordinateur, un téléphone intelligent ou une tablette à un réseau, sans avoir besoin de connexion physique (câble). Les connexions diffusent un signal qui permet d'accéder au réseau. Ce signal peut être capté par toute personne ayant une carte réseau sans fil (WiFi). Les règles de sécurité de base dans l'utilisation de tels réseaux sont :

a. Modifier le code administrateur et le mot de passe du point d'accès (l'endroit où l'on se connecte) ou du routeur sans fil. Les paramètres par défaut sont les premiers testés lors de tentatives d'intrusion, et la plupart des utilisateurs ne les modifient pas. Voir la section 2 du guide dédiée aux mots de passe.

b. Mettre en place le chiffrement des données transitant sur le lien sans fil. L'utilisation du protocole WPA2 est recommandée, car le protocole WEP peut être piraté facilement et rapidement et devrait être évité.

c. Filtrer les adresses MAC (Media Access Control – adresse physique unique d'une carte réseau). Le point d'accès ou le routeur sans fil communiquera seulement avec les adresses préconfigurées par l'administrateur du réseau.

d. Bloquer la diffusion publique du signal du nom de réseau sans fil (SSID Broadcasting) afin de « cacher » l'équipement sans fil aux yeux des utilisateurs non autorisés.

Si vous offrez l'accès à votre réseau WiFi dans la salle d'attente de votre bureau : Prévoir un accès invité, distinct de celui que vous utilisez pour accéder à votre réseau, afin de minimiser les risques de sécurité et limiter les droits d'accès des personnes accédant à ce réseau. Outre les passerelles qui donnent l'accès à vos invités, vos mots de passe ne devraient pas être partagés.

[13] Dans la majorité des cas, seules les licences légales comportent ces mises à jour.

L'utilisation de l'informatique mobile

Les clés USB et les disques durs externes ont rapidement remplacé les CD, DVD, disquettes et autres médias amovibles. Il y a aussi l'utilisation des téléphones intelligents (iPhone, Android, BlackBerry, etc.) qui contiennent courriels, agendas, liste de contacts et documents, et qui peuvent donner accès à votre réseau. Les connexions au réseau interne à partir d'un lien Internet (extérieur à l'entreprise) sont aussi de plus en plus répandues. Pour assurer une bonne sécurité sur cette masse de données, facile à oublier sur la table d'un restaurant ou sur le siège arrière d'un taxi, il faut chiffrer les données s'y trouvant.

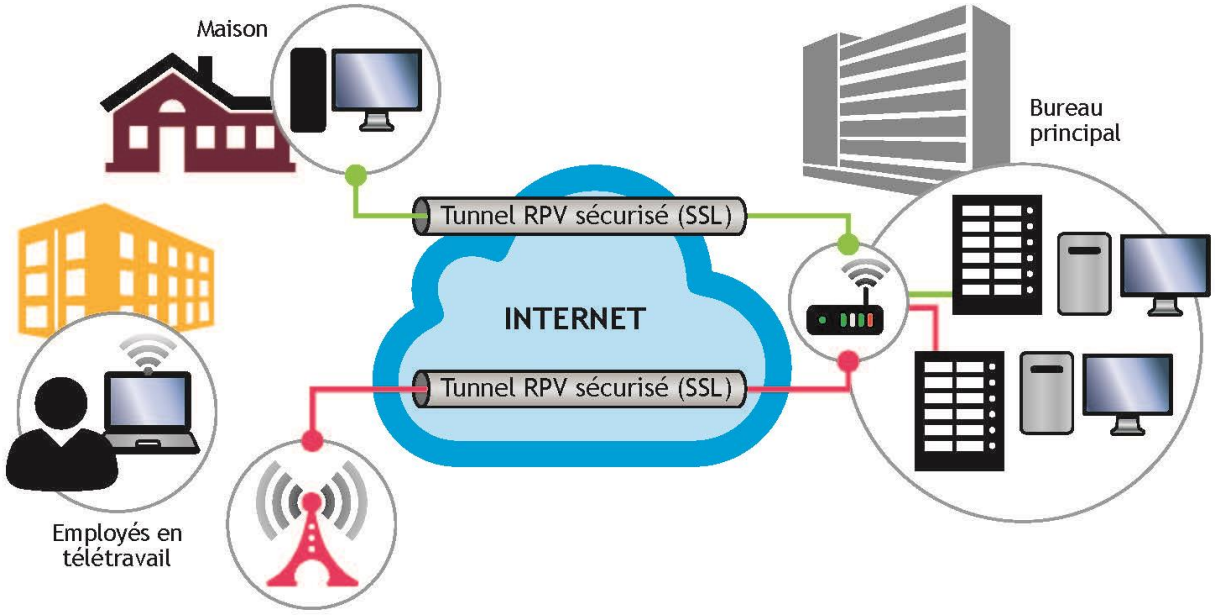
Pour ce qui est des téléphones intelligents, la mise en place d'une authentification par mot de passe est impérative ainsi que le chiffrement des documents que l'appareil contient[14]. Il faut aussi s'assurer que les connexions Bluetooth (connexions à faible portée permettant la connexion d'appareils comme des casques mains libres ou le transfert d'information entre deux appareils) sont non disponibles par défaut et sécurisées lorsqu'utilisées.

Pour ce qui est de l'utilisation de l'informatique mobile, dans la mesure où un réseau WiFi est public, il faut s'assurer d'utiliser une connexion RPV sécurisée (réseau privé virtuel; plus souvent appelé VPN ou *Virtual Private Network*). Pour ce qui est du télétravail, la même prudence s'impose : si vous branchez votre ordinateur professionnel à la maison à partir de votre réseau personnel, utilisez également une connexion RPV (VPN).

Une telle connexion permet d'avoir accès au réseau local de votre entreprise à travers une connexion Internet sécurisée et d'accéder aux ressources de votre réseau local (p. ex., fichiers, intranet, extranet) comme si vous étiez sur votre lieu de travail.

Une connexion RVP procure le niveau de sécurité le plus élevé possible, grâce à des tunnels chiffrés et à des technologies d'authentification. Les données traversant le RPV sont ainsi protégées contre tout accès non autorisé. Voir le schéma à la page suivante.

[14] Pour plus de détails, voir la sous-section intitulée *Cellulaire*.



Ressources (certaines de ces ressources n'existent qu'en anglais)

Antivirus

- McAfee
- Symantec Norton
- ESET
- Avast
- Microsoft Security Essentials (gratuit pour les entreprises de 10 employés et moins)
- The best free antivirus for 2015
- Kapersky

Pare-feu

- Zone Alarm
- Cisco
- Sonicwall
- WatchGuard

Mise à jour des logiciels et des systèmes d'exploitation

- Microsoft Windows 10
- Microsoft Windows Update
- Apple MAC OS X
- Mac App Store
- MacUpdate Desktop 5

Ajout d'une minuterie et d'un mot de passe à l'écran de mise en veille

- Pour Windows 7
- Pour Windows Vista
- Pour Mac OS X

Sécurité réseau sans-fil

- Microsoft Technet
- Setting up wireless security on a Linksys router
- How to secure a D-Link Wireless Router

BYOD (Bring Your Own Device) ou AVEC (Apportez Votre Équipement personnel de Communication)

Principe

L'avocat doit mettre en place une politique encadrant l'utilisation des équipements personnels qui se connectent à une partie ou à l'ensemble de son réseau informatique ainsi que des mesures de sécurité pour en assurer la protection. Cette politique doit permettre à l'avocat de s'assurer que l'utilisation d'un réseau informatique est conforme à ses obligations déontologiques (secret professionnel, secrets commerciaux et industriels, renseignements personnels, etc.).

Définition

L'acronyme BYOD est apparu vers la fin 2011 dans les publications informatiques. Cependant, c'est depuis le début des années 2000 que les firmes permettent à leurs employés d'utiliser leurs ordinateurs personnels pour se brancher au réseau d'entreprise par l'intermédiaire d'un réseau privé virtuel (RPV). Les firmes réalisent progressivement les bénéfices de laisser les avocats et le personnel de soutien avoir accès à leurs dossiers et courriels à partir de la maison, élargissant ainsi la disponibilité et la productivité des employés.

L'arrivée des téléphones intelligents ainsi que des tablettes sur le marché a fortement contribué à déplacer vers le consommateur l'achat de ses propres équipements selon ses goûts et ses besoins.

Un équipement BYOD est donc un équipement fourni par l'employé ayant accès à une partie ou à la totalité des données du réseau informatique de l'entreprise.

Utilité

L'utilisation d'équipements fournis par l'employé permet :

a) L'accès en tout temps aux données (en tout ou en partie) de la firme;
b) La mobilité de l'employé;
c) Une diminution des coûts d'acquisition d'équipements par la firme;
d) À l'employé de choisir un équipement avec lequel il se sent à l'aise et qu'il a choisi avec soin.

Risques

Les équipements personnels n'étant pas gérés par le département des TI de la firme, il est difficile de contrôler la sécurité de ces appareils. De plus, la plupart de ces équipements utilisent les liens sans-fil (WiFi) ce qui risque de congestionner et de ralentir les connexions de la firme. Voici une liste des risques inhérents à utilisation des BYOD :

a) Accès non contrôlé aux données de l'entreprise;
b) Plusieurs comptes de courriel sur le même appareil, augmentant le risque d'infection par un virus;
c) Plusieurs comptes de courriel sur le même appareil, augmentant le risque de fuite de données;
d) Aucun contrôle sur les mises à jour et vulnérabilités inhérentes aux différents systèmes d'exploitation utilisés;
e) Besoin d'expertise sur plusieurs plateformes pour soutenir les usagers;
f) Aucun contrôle sur l'installation d'applications pouvant entrer en conflit avec les applications critiques de la firme.

Meilleures pratiques

Il est pratiquement impensable aujourd'hui d'empêcher un employé d'utiliser son propre équipement et de lui donner accès, au minimum, à ses courriels. Afin de garder un certain contrôle sur le flux d'information transitant par ces équipements mobiles, la mise en place d'outils permettant une utilisation sécuritaire des BYOD est suggérée. Voici une liste des outils pouvant être mis en place, ainsi que leur utilité :

a) **Politique d'utilisation des équipements personnels**

   Cette politique devrait établir la propriété de l'appareil mobile (dans le cas où la firme fournit l'équipement) et ce qu'il est permis de faire ou non du côté personnel. Cette politique devrait également établir la propriété des données transitant sur l'appareil dans le cas où ce dernier est la propriété de l'employé. Elle devrait aussi déterminer à qui, de l'employé, de la firme ou au prorata de l'utilisation personnelle/affaires, doivent être attribués les coûts mensuels d'utilisation et de bande passante. La politique devrait finalement établir clairement les paramètres de sécurité (accès et restriction) vis-à-vis les données de l'entreprise.

b) **Mise en place d'outils de gestion des équipements personnels**

   Il existe deux outils pour la gestion des BYOD, soit l'EMM (Enterprise Mobility Management tools) et le MDM (Mobile Device Management tools).

L'EMM est en fait un mélange de technologies, de procédures et de personnel ayant la capacité de gérer l'utilisation des BYOD et des services dans un contexte d'entreprise.

Le MDM est une application permettant la gestion des BYOD au niveau des services informatiques de l'entreprise. L'application permet de mettre à jour les systèmes d'exploitation à distance, de surveiller et de contrôler les erreurs des appareils, de prendre contrôle à distance afin de supporter les usagers, de garder un inventaire des terminaux actifs et de consulter les communications en temps réel. Du point de vue de la sécurité, l'application permet la gestion des sauvegardes et des restaurations en cas de perte ou de remplacement des équipements, de bloquer ou d'effacer les données à distance en cas de perte ou de vol des équipements et d'installer des applications à distance.

Ressources

- The New BYOD : Best Practices for a Productive BYOD Program – Air Watch by VMWare
- Wikipedia MDM
- Wikipedia EMM

Cellulaire

Principe

Tout appareil téléphonique mobile (cellulaire ou intelligent) ou assistant numérique personnel doit être protégé par un mot de passe après une veille de trois minutes. Son contenu doit être chiffré, et son nom par défaut modifié. Les fonctions de réseautage (Bluetooth, WiFi ou autres) de même que la détectabilité de l'appareil doivent être désactivées lorsqu'elles ne sont pas utilisées. Lorsqu'elles sont activées, elles doivent être chiffrées.

Définition

Les téléphones intelligents sont des téléphones mobiles couplés à des assistants numériques personnels. Ils offrent des fonctionnalités telles que l'agenda, la navigation Web, le courriel et la messagerie instantanée. Plusieurs modèles permettent aussi d'installer des applications additionnelles. Les plus connus utilisent les plateformes suivantes : iOS, Android et BlackBerry.

En ce qui a trait au Bluetooth, il s'agit d'une technologie radio couvrant une courte distance qui vise à simplifier les connexions entre appareils électroniques en remplaçant les câbles autrement nécessaires. Le réseau Bluetooth permet d'interconnecter ordinateurs, imprimantes, numériseurs, claviers, téléphones portables, souris, assistants numériques personnels, écouteurs, micros mains libres, etc.

Risques

Plus les jours passent et plus les téléphones intelligents s'apparentent à des ordinateurs en raison des fonctionnalités et des capacités qu'ils offrent. Ils contiennent de plus en plus d'informations confidentielles telles que des renseignements personnels et des secrets commerciaux ou industriels, mais surtout des renseignements couverts par le secret professionnel des avocats ou le privilège relatif au litige. C'est pourquoi il est primordial d'en assurer la protection en toute circonstance.

Leurs petites dimensions les rendant particulièrement vulnérables à la perte et au vol, il faut redoubler de précautions. Ainsi, il faut s'assurer que si un appareil est égaré, la personne qui fera main basse dessus ne pourra accéder à son contenu. La seule façon de l'en empêcher est de protéger l'appareil par un mot de passe et par chiffrement. Le mot de passe devrait respecter les normes minimales applicables à celui-ci.

Quant à la technologie Bluetooth, elle est particulièrement courante pour la téléphonie cellulaire puisque les écouteurs et les micros sont obligatoires au Québec pendant la conduite automobile. Bien que très utile, elle constitue un maillon faible de plus dans la sécurité de l'information. En effet, les divers outils Bluetooth ouvrent un canal de communication, potentiellement non sécurisé, avec le téléphone intelligent.

Par l'entremise de cette technologie, la majorité des téléphones mobiles permettent l'échange de données telles que les cartes de visite, les événements inscrits au calendrier, les documents et, surtout, la voix. Dans bien des cas, la synchronisation entre l'outil Bluetooth et le téléphone intelligent se fait par l'octroi de permissions par ce dernier à l'outil qui accède ensuite à son contenu. La connexion s'effectue en deux temps : d'abord, le téléphone et l'outil doivent pouvoir se détecter l'un l'autre afin d'entamer la communication; ensuite, les deux équipements communiquent ensemble afin de requérir leur

identification respective, après quoi l'échange d'information est autorisé. Dans le cadre de ce processus, il est possible pour un tiers de s'immiscer dans l'échange ou même de l'initier.

Meilleures pratiques

La protection par mot de passe doit être activée dans le téléphone. Cette fonctionnalité se trouve généralement dans la section « sécurité » des paramètres du téléphone. À titre indicatif, le mot de passe s'active de la façon suivante :

→ **Sur un iPhone** : Réglages > Code (sur un iPhone 5s et plus, vous pouvez aussi activer le lecteur d'empreinte digitale : Réglages > Touch ID et Code)

→ **Sur un appareil Android** : Paramètres -> Lieu et sécurité -> Verrouillage de l'écran (vous pourrez alors entrer un code, un schéma ou un mot de passe, à votre choix.)

→ **Sur un BlackBerry** : Paramètres > Sécurité et confidentialité > Mot de passe simple ou Mot de passe du terminal

Quant à la veille, elle permet de diminuer la période de vulnérabilité de l'appareil lorsqu'il échappe au contrôle de son titulaire. Elle devrait être établie à trois minutes et moins. À titre indicatif, voici comment régler vos options de veille :

→ **Sur un iPhone** avec iOS 8.x et plus : Réglages > Général > Verrouillage auto
→ **Sur un appareil Android** : Paramètres > Personnel > Sécurité > Verrouillage de l'écran
→ **Sur un BlackBerry** : Paramètres > Sécurité et confidentialité > Mot de passe du terminal. Dans la liste déroulante choisir « Verrouiller le terminal après » et indiquer un intervalle.

Il est également recommandé de désactiver l'option « partage de connexion » lorsqu'elle n'est pas utilisée. Cette fonction permet à un ordinateur d'utiliser la connexion Internet d'un téléphone cellulaire, soit par branchement câblé, par connexion WiFi ou par l'entremise d'une connexion Bluetooth. À titre indicatif, l'option « partage de connexion » se désactive de la façon suivante :

- **Sur iPhone avec iOS 8.x et plus** : Réglages > Partage de connexion

Généralement, le chiffrement se trouve aussi à cet endroit et devrait être activé. Il est parfois possible d'en établir la force et il est suggéré de retenir le plus haut niveau. Cela étant, la protection de base sera parfois suffisante si elle est de 128 bits ou plus.

En ce qui concerne la technologie Bluetooth, afin de protéger l'information contenue dans le téléphone, il faut s'assurer que, hors communication, la détectabilité soit désactivée et que pour toute communication, celle-ci soit chiffrée et protégée par un mot de passe. Ce dernier est généralement le même que le mot de passe mentionné plus tôt afin d'accéder « physiquement » au contenu du téléphone. À titre indicatif, les paramètres Bluetooth sont accessibles de la façon suivante :

- **Sur un BlackBerry :**

  Détectabilité : Options > Bluetooth > Bouton Menu > Options > Détectabilité > Non. Chiffrement : Options > Bluetooth > Bouton Menu > Options > Niveau de sécurité > Élevé et Chiffré.

- **Sur un iPhone avec iOS 8.x et plus :**

Détectabilité : Réglages > Général > Bluetooth > (désactiver)
Chiffrement : Il n'est pas possible pour le moment de procéder au chiffrement de l'information à même les applications du iPhone. Il est cependant possible de recourir au service Hushmail pour effectuer un tel chiffrement des informations contenues sur ce type d'appareil.

Il est aussi nécessaire de modifier les noms par défaut du téléphone et de l'outil Bluetooth. Autrement, il est possible pour quiconque d'identifier le code d'accès de l'équipement et d'y accéder à distance. À titre indicatif, ce changement s'effectue de la façon suivante :

- **Sur un iPhone :** Le meilleur moyen de prévenir l'accès à distance aux informations contenues sur le iPhone est de désactiver la fonctionnalité Bluetooth lorsque non requise. Pour ce faire, vous devez procéder ainsi : Réglages > Général > Bluetooth > Fermez l'application. Pour changer le nom de l'appareil : Réglages > Général > Informations > Nom.

- **Sur un appareil Android** : Paramètres > A propos (tout en bas) > appuyez sur « Nom de l'appareil » > Tapez le nom souhaité > « OK ». Pour changer le nom du bluethooth : Paramètres > Bluetooth, affichez le Menu et sélectionnez « Renommer l'appareil » puis tapez le nom souhaité et validez avec « OK ».
- **Sur un BlackBerry** : Options > Bluetooth > Sélectionner l'outil > Bouton Menu > Propriétés

En cas de perte de votre appareil cellulaire, il est possible pour la plupart des modèles de localiser, de verrouiller ou de déverrouiller l'appareil, de même que d'en effacer le contenu à distance.

Pour plus d'informations sur cette option :

- **Sur un iPhone** : Avant de pouvoir procéder à l'une de ces actions, il faut cependant s'assurer d'avoir activé l'option au préalable alors que vous avez l'appareil en main.
- **Sur un appareil Android**, votre appareil doit être associé à un compte Google (disponible gratuitement) :
- **Sur un BlackBerry** : BlackBerry Protect est une application gratuite conçue pour retrouver un appareil perdu et protéger les informations qu'il contient.

Éthique et déontologie

Il est nécessaire pour l'avocat de respecter ces pratiques afin de satisfaire à l'obligation de protéger le secret professionnel[15].

Aussi, rappelons qu'il est illégal pour un avocat de tenir une conversation téléphonique en public avec un client qui lui confie une information confidentielle, à moins que celui-ci ne l'ait relevé de son obligation. L'obligation relative à cette situation est prévue à l'article 5 du *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, lequel se lit comme suit :

[15] *Code des professions*, art. 60.4., *Code de déontologie des avocats*, art. 60 et 61, *Loi concernant le cadre juridique des technologies de l'information*, art. 34., *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, art. 17.

« L'avocat doit utiliser un cabinet de consultation ou un autre local lui permettant de rencontrer des clients ou de tenir des conversations assujetties au secret professionnel. Ce cabinet ou ce local doit être fermé et aménagé de façon à ce que les conversations des personnes qui s'y trouvent ne puissent être entendues de l'extérieur. Pendant toute la durée de ces rencontres ou conversations, aucune autre personne ne doit avoir accès à ce local, sauf avec l'autorisation de l'avocat. »

Ressources

Sécurité et téléphones intelligents

- Ten dangerous claims about smart phone security
- Mobile Security

Sécurité Bluetooth

- Site officiel de l'organisation Bluetooth
- Guide to Bluetooth Security
- Bluecasting
- Bluejacking
- Bluesnarfing

Communications électroniques

Principe

L'avocat qui communique de l'information confidentielle doit protéger celle-ci par un moyen approprié en fonction du mode de communication et de la nature de l'information. Il doit aussi convenir avec ses clients des modes de communication et des moyens de protection qu'il utilisera pour chacun d'eux selon l'information en question. Cette convention doit être documentée, généralement par écrit.

Exemple

Par exemple, un avis juridique concernant la privatisation d'une entreprise publique communiqué par courriel devrait être chiffré afin d'en assurer la protection entre son émission et sa réception. Par opposition, un avis transmis à une adolescente désirant se faire avorter pourrait l'être sans chiffrement, mais devrait être autrement protégé et être contenu dans une pièce jointe protégée par un mot de passe, ou être acheminé à une adresse de courrier électronique convenue pour éviter que ses parents n'en prennent connaissance.

Risques

Les avocats n'hésitent pas à communiquer par courriel des renseignements ou des documents hautement confidentiels, comme beaucoup de gens. Par contre, seul l'avocat a l'obligation de maintenir le secret absolu des renseignements qu'il détient pour autrui et qu'il a reçu en sa qualité d'avocat.

L'utilisation de moyens de communication électronique sans mesure de protection comporte plusieurs risques : destinataire erroné, utilisation à mauvais escient, interception, altération du message, etc. De plus, il est important de prendre conscience qu'entre votre boîte d'envoi et la boîte de réception du destinataire, un courriel transite par de nombreux serveurs, potentiellement situés dans d'autres juridictions ou pays, dont certains peuvent en conserver une copie. La réalité est la même pour la plupart des moyens de communication électronique, c'est-à-dire qu'ils laissent des traces en de nombreux lieux. Ces risques sont inhérents à l'utilisation des technologies de l'information, mais peuvent faire l'objet de mesures permettant de remplir les obligations auxquelles sont soumis les avocats.

Réception accidentelle d'information possiblement protégée par le secret professionnel

La transmission accidentelle de documents ou de renseignements protégés par le secret professionnel[16] à une personne autre que le client est une problématique qui a tendance à s'accentuer avec le développement des nouvelles technologies.

Alors que les erreurs impliquant la poste régulière étaient plutôt rarissimes (erreur d'adresse ou interversion d'enveloppes), celles-ci se sont multipliées avec l'usage de moyens de communication plus instantanés tels le télécopieur (erreur dans le numéro) puis le courrier électronique (erreur dans l'adresse, c.c./c.c.b.c. accidentels, etc.). De plus, les versions électroniques des documents transmis peuvent contenir des renseignements, notamment sous forme de métadonnées[17], dont la divulgation n'est pas voulue[18] par l'expéditeur.

Bien que la jurisprudence et la doctrine indiquaient le contraire dans un passé pas si lointain, et que la question demeurerait controversée en common law, il est maintenant reconnu en droit civil que la divulgation par inadvertance ne peut équivaloir à une renonciation à la protection du secret

[16] À ce sujet généralement, voir : M^e^ Michel TÉTRAULT, *Le litige familial, la déontologie et l'éthique*, Cowansville, Éditions Yvon Blais, 2006, p. 19-26 et M. JAMAL et S. LUSSIER, *Le secret professionnel de l'avocat*, Développements récents en déontologie, droit professionnel et disciplinaire, Formation permanente du Barreau, Colloque 2008, p. 216-217.

[17] Sur les implications déontologiques de la réception accidentelle de métadonnées aux États-Unis, voir : « Formal Opinion 2009-100 – Ethical obligations on the transmission and receipt of metadata », (July/August 2009) The Pensylvania Lawyer.

[18] Sur la possible interdiction d'effacer les métadonnées dans le contexte du « discovery » aux États-Unis, voir : « Technology traps/Ethical considerations for litigations in a 24/7 online world », (Winter 2010) 36 Litigation, p. 34, 37-38 (n °2).

professionnel[19], et ceci plus particulièrement depuis l'adoption en 1994 de l'article 2858 du *Code civil du Québec*[20].

> « [25] En l'espèce, considérant d'une part les représentations du Procureur général selon lesquelles le document a été divulgué à la partie demanderesse par inadvertance, et, d'autre part, l'absence de preuve d'une divulgation volontaire et autorisée par le client, ce dévoilement ne saurait lui être imputé et constituer une renonciation de sa part à son droit au secret professionnel[21]. »

D'un point de vue plus procédural, et quoique découlant de l'exécution d'une ordonnance de type Anton Pillar, le jugement de la Cour suprême du Canada dans l'affaire Celanese[22] a établi toute une série de balises applicables à la problématique examinée en l'espèce, dont le fait que la partie ayant ainsi transmis par erreur des documents contenant de l'information protégée devrait, sans délai :

1. en être avisée;
2. se voir restituer les documents transmis par erreur[23];
3. être informée de la mesure dans laquelle les documents ont été examinés.

---

[19] Voir notamment : *Spieser* c. *Canada (Procureur général)* 2010 QCCS 3248; *Guillemette* c. *Smith*, 2009 QCCA 2190; *GeneOhm Sciences Canada Inc.* c. *Biomérieux Inc.*, 2007 QCCA 290; *Lavallée, Rackel & Heintz* c. *Canada (Procureur général)*; *White, Ottenheimer & Baker* c. *Canada (Procureur général)*; *R.* c. *Fink*, [2002] 3 R.C.S. 209, par. 49; *Poulin* c. *Pratt*, [1994] R.D.J. 301 (C.A.); *G.(A.)* c. *W.(D.)*, REJB 2002-32223 (C.S.); M. JAMAL et S. LUSSIER, *Le secret professionnel de l'avocat*, Développements récents en déontologie, droit professionnel et disciplinaire, Formation permanente du Barreau, Colloque 2008, p. 216-217; ROYER et LAVALLÉE, *La preuve civile*, 4e éd., Cowansville, Éditions Yvon Blais, 2008, par. 1222, note 478 et Léo DUCHARME, *L'administration de la preuve*, 3e éd., Montréal, Wilson et Lafleur, 2001, p. 117-118.

[20] *Guillemette* c. *Smith*, 2009 QCCA 2190, par. 19; *Code civil du Québec*, art. 2858 : « Le tribunal doit, même d'office, rejeter tout élément de preuve obtenu dans des conditions qui portent atteinte aux droits et libertés fondamentaux et dont l'utilisation est susceptible de déconsidérer l'administration de la justice.

[21] *Spieser* c. *Canada (Procureur général)*, 2010 QCCS 3248.

[22] *Celanese Canada Inc.* c. *Murray Demolition Corp.*, [2006] 2 R.C.S. 189.

[23] À défaut de cela, un tribunal pourra l'ordonner; voir à ce sujet : *Smith* c. *Bélanger et al.*, 2009 QCCS 4277 confirmé par *Guillemette* c. *Smith*, 2009 QCCA 2190.

À défaut de cela, il y aura présomption de préjudice[24], et un tribunal pourra émettre des ordonnances visant réparation et même prononcer une déclaration d'inhabileté[25] à l'endroit du procureur qui aurait pris connaissance des renseignements protégés, quoique telle inhabileté ne soit cependant pas automatique[26].

Les ordonnances visant réparation peuvent notamment enjoindre le retrait d'un document accidentellement produit au dossier de la Cour[27] ou inclus dans les documents transmis à la partie adverse[28], ou la remise, par la partie adverse ou ses procureurs, des documents en question à l'expéditeur[29]; les ordonnances peuvent également interdire de référer à ces documents ou de les utiliser[30], de poser des questions relativement à ceux-ci[31], de requérir la production de quoi que ce soit

[24] À cet égard, la Cour Suprême du Canada, dans son arrêt *Celanese*, applique ce qu'elle a déjà établi dans son arrêt *Succession Macdonald* : « L'arrêt de notre Cour *Succession MacDonald* c. *Martin*, [1990] 3 R.C.S. 1235, établit clairement qu'il y a présomption de préjudice lorsqu'une partie adverse a accès à des communications pertinentes effectuées à titre confidentiel entre un avocat et son client.», *Celanese Canada Inc.* c. *Murray Demolition Corp.*, [2006] 2 R.C.S. 189.

[25] « Il faut tenir pour acquis que le droit d'être représenté par un avocat ayant eu accès à des communications pertinentes effectuées à titre confidentiel entre un avocat et son client n'existe pas dans le cas où cet accès aurait dû être prévu et sans trop de peine évité et où la partie ayant sollicité la perquisition n'a pas réfuté la présomption de risque de préjudice […] », *Celanese Canada Inc.* c. *Murray Demolition Corp.*, [2006] 2 R.C.S. 189– voir aussi les par. 56-59; *Darco Archery* c. *Topo Production*, EYB 1991, 04-10-1991; *Hull* c. *Chellecourt*, 2006 QCCS 1364; sur ce sujet, aux États-Unis voir : Etan MARK, « Inadvertant document productions and the threat of attorney disqualification », (November 2009) 83 Florida Bar Journal (nº 10).

[26] *Celanese Canada Inc.* c. *Murray Demolition Corp.*, [2006] 2 R.C.S. 189, par. 56; *D.L.* c. *J.G.*, AZ-50141353 (C.S.), 01-08-2002; *Chouinard* c. *Robbins*, REJB 1996-86859 (C.S.).

[27] *G.(A.)* c. *W.(D.)*, REJB 2002-32223 (C.S.); *Bombardier Inc.* c. *Union Carbide Canada Inc.*, 2010 QCCS 6780.

[28] *Smith* c. *Bélanger et al.*, 2009 QCCS 4277 , conclusions.

[29] *Smith* c. *Bélanger et al.*, 2009 QCCS 4277 , conclusions; *Spieser* c. *Canada (Procureur général)* 2010 QCCS 3248, conclusions; *Bombardier Inc.* c. *Union Carbide Canada Inc.*, 2010 QCCS 6780.

[30] *Smith* c. *Bélanger et al.*, 2009 QCCS 4277 , par.24; *Bombardier Inc.* c. *Union Carbide Canada Inc.*, 2010 QCCS 6780.

[31] *Smith* c. *Bélanger et al.*, 2009 QCCS 4277 , par. 26.

découlant du contenu desdits documents[32], de se servir de ce qu'on a pu en retenir pour interroger (au préalable ou à procès)[33], et d'en révéler le contenu à qui que ce soit[34].

Enfin, sur un plan plus déontologique, la Cour supérieure a déjà énoncé que le devoir de confidentialité s'appliquerait à l'avocat qui reçoit ou voudrait utiliser de l'information privilégiée émanant d'un tiers qui n'est pas ou n'a jamais été son client[35].

---

[32] *Smith* c. *Bélanger et al.*, 2009 QCCS 4277 , par. 24.

[33] *Smith* c. *Bélanger et al.*, 2009 QCCS 4277 , par. 24 et 26.

[34] *Spieser* c. *Canada (Procureur général)* 2010 QCCS 3248, conclusions.

[35] *G.(A.)* c. *W.(D.)*, REJB 2002-32223 (C.S.). Dans cette affaire, le procureur d'une partie avait, comme c'est souvent le cas dans de telles situations, transmis par erreur aux procureurs adverses des documents échangés entre lui et son client; contra : *D.L.* c *J.G.*, AZ-50141353 (C.S.); Il serait possiblement plus approprié, en droit disciplinaire, de se reporter à l'article 59.2 du *Code des professions*, en s'inspirant notamment de l'esprit des articles 63 et 64 du *Code de déontologie des avocats*, du principe fondamental de notre système de justice qu'est le secret professionnel (voir les notes de bas de page 2 et 3 de l'introduction du présent guide) et du rôle d'officier de justice de l'avocat, pour éventuellement conclure à la perpétration d'un acte dérogatoire.

Voici ce que le *Code de déontologie des avocats* prévoit :

> 63. L'avocat ne doit pas faire usage d'un renseignement confidentiel en vue d'obtenir un avantage pour lui-même ou pour un tiers.
>
> 64. L'avocat ne doit pas accepter un mandat s'il a des raisons de croire que cela comporte ou pourrait vraisemblablement comporter la communication ou l'utilisation d'un renseignement confidentiel relatif à un autre client.

L'avocat qui reçoit, particulièrement de l'avocat de la partie adverse, communication d'un document qui apparaît ne pas lui être destiné ou contenir de l'information possiblement protégée par le secret professionnel, devrait[36] :

1. Ne pas en prendre plus amplement connaissance;
2. Aviser immédiatement le collègue (et ce, malgré l'absence d'une disposition déontologique spécifique à cet effet[37]) et requérir les commentaires quant à savoir si ce document lui était vraiment destiné et, le cas échéant, s'il est ou non couvert par le secret professionnel ou un autre privilège;
3. Sur demande, détruire le document ou le remettre à l'expéditeur, sans en prendre copie.

---

[36] Pour une revue des règles applicables aux États-Unis, selon les codes de déontologie en vigueur dans différents États, laquelle étudie les obligations de l'avocat « receveur » aux stades de la pré-notification, de la notification et de la post-notification, voir : « What's yours is ours : Making sense of inadvertant disclosure », (2009) 22 The Georgetown Journal of Legal Ethics, p. 1095-1113.

[37] *Code de déontologie des avocats*, art. 132.

Par ailleurs, vu ses devoirs envers son propre client, notamment ceux de loyauté[38], de transparence[39] et de dévouement à la cause de celui-ci[40], nous croyons que l'avocat « receveur » devrait aviser son client de l'incident et, particulièrement si la question peut raisonnablement faire l'objet d'un débat, lui faire part du secret ou du privilège invoqué, de la nature des informations prétendument privilégiées et de son droit de s'adresser à la Cour pour contester le privilège invoqué, le tout, en gardant à l'esprit qu'il ne doit aucunement révéler ainsi, même en partie, des détails de ces informations en question dont il aurait pu prendre connaissance. Dans ce même esprit, l'avocat qui aurait, du fait des circonstances de l'espèce, pris grandement ou même intégralement connaissance des renseignements protégés devrait s'interroger sur l'à-propos de lui-même conseiller ou représenter son client qui voudrait contester le privilège invoqué.

Enfin, il y aurait probablement lieu pour l'avocat du client dont des renseignements protégés ont été transmis par erreur à des tiers, d'aviser son client de cet incident. Cette obligation découlerait premièrement du fait que le secret appartient au client et que l'avocat, qui en est le fiduciaire, se doit de l'informer de toute atteinte, ou atteinte potentielle, audit secret[41]. Tel qu'énoncé au paragraphe précédent, les avocats ont toujours des devoirs généraux de loyauté et de transparence à l'égard de leurs clients, de même qu'un devoir d'information[42].

Meilleures pratiques

Dans les cas où le client y consent, l'application de la loi du nombre pourra convenir pour communiquer des renseignements confidentiels. Selon ce principe, l'information sera communiquée sans protection, en présumant que tout se passera bien, vu le nombre élevé de courriels qui circulent à tout moment sur Internet et le nombre relativement restreint de personnes susceptibles d'en intercepter un en particulier. Bien que cette approche ne soit pas farfelue, il faut s'assurer que le client y consente en toute connaissance des risques que cette pratique comporte et des conséquences pouvant en découler. Le client

[38] *Code de déontologie des avocats*, art. 20, 72 al. 1 par. 2° et 134 par. 6.

[39] Voir notamment *Fortin* c. *Lord*, 2008 QCCDBQ 140.

[40] Qu'on appelle aussi parfois la « représentation zélée »; voir notamment sur ce sujet *R.* c. *Neil*, [2002] 3 R.C.S. 631, par. 19 et le *Code de déontologie professionnelle de l'Association du Barreau Canadien*, chapitre IX, section 1.

[41] On peut certainement ici tracer un parallèle avec l'obligation qu'a un avocat d'informer son client dont le dossier est visé par un mandat de perquisition (voir *Lavallée, Rackel & Heintz* c. *Canada (Procureur général); White, Ottenheimer & Baker* c. *Canada (Procureur général)*; *R.* c. *Fink*, [2002] 3 R.C.S. 209, par. 49) afin que celui puisse ensuite décider s'il entend invoquer la protection du secret professionnel.

[42] À titre illustratif voir : *Thibault* c. *Bilodeau*, 2003 CanLII 54678 (QC C.D.B.Q.); *Montbriand* c. *Desmarais*, 2009 CanLII 110 (QC C.D.B.Q.).

qui convient avec son avocat d'appliquer la loi du nombre dans le cadre de leurs communications ne renonce pas pour autant au secret professionnel.

Par ailleurs, dans un tel cas, l'objet du courriel devrait contenir un avertissement très clair du caractère privilégié de son contenu. Ainsi, des expressions comme « Confidentiel » ou « Protégé par le secret professionnel » devraient être utilisées dans le champ « Objet » du courriel ou, à la rigueur, au début du corps du texte.

Les déclarations de confidentialité ajoutées automatiquement à la fin du corps du texte ne sont d'aucun secours. D'abord, elles sont situées après les renseignements confidentiels, ce qui ne peut empêcher le destinataire accidentel d'en prendre plus ample connaissance. Ensuite, elles sont généralement apposées indistinctement du contenu du courriel (mêmes aux messages personnels), de sorte que leur pertinence est sérieusement amoindrie et qu'enfin, personne ne les lit ou ne les prend au sérieux.

Dans la majorité des cas, les documents contenant des renseignements confidentiels devraient être acheminés dans un fichier joint, protégé par un mot de passe. Ce dernier devrait être communiqué au destinataire par un moyen de communication autre ou par un envoi chiffré.

La méthode de protection idéale est sans doute le chiffrement. Par l'emploi d'algorithmes mathématiques complexes, le chiffrement modifie en profondeur le contenu d'une communication ou le conduit qu'elle emprunte. L'information devient alors incompréhensible et est à toutes fins utiles indéchiffrable. Seul le destinataire en possession de la « clé » appropriée (généralement, un mot de passe) pourra déchiffrer le message original et en prendre connaissance. Différents logiciels de chiffrement sont disponibles sur le marché. De telles mesures de chiffrement, conformes aux standards actuels (algorithme à 256 bits, etc.), sont probablement suffisantes pour satisfaire le critère de l'article 34 de la LCCJTI.

L'établissement d'un réseau fermé et sécurisé avec le client est évidemment une solution coûteuse qui ne peut être envisagée que pour des clients importants avec lesquels le volume de courriels échangés justifie une telle dépense. Il satisfait clairement lui aussi au critère de l'article 34 de la LCCJTI.

Obligation de convenir du mode de transmission avec le client et de documenter cette convention

Selon les termes du second alinéa de l'article 34, la seule protection de la confidentialité de l'information n'est pas suffisante. Il faut, au surplus, que « la documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis [soit] disponible pour production en preuve, le cas échéant ». Cela implique les obligations suivantes pour l'avocat qui prévoit transmettre de l'information confidentielle par courriel :

- Convenir avec son client du mode de transmission qu'il entend utiliser (ici, le courriel) ainsi que des moyens qu'il prendra pour en assurer la confidentialité (p. ex., le chiffrement). Nous recommandons de prévoir ces modalités dans la lettre de confirmation du mandat;
- Documenter cette convention (sur support papier ou technologique). Le législateur impose le formalisme dans l'élaboration de cette convention. Le recours à la lettre de confirmation du mandat permet de respecter cette obligation;
- Conserver, aux fins de preuve, la documentation ainsi générée. Dès lors, si un jour le client entreprenait un recours contre l'avocat au motif qu'il n'a pas protégé adéquatement la confidentialité des renseignements transmis par courriel, l'avocat devra être en mesure de produire la documentation établissant le consentement du client à utiliser ce moyen de communication et la méthode de protection de la confidentialité utilisée.

Exceptions aux obligations imposées par l'article 34

L'article 34 de la LCCJTI n'impose pas en soi la confidentialité : il pose seulement certaines exigences à la transmission d'un document qui contient par ailleurs des renseignements que la loi déclare

confidentiels. La disposition législative qui impose cette confidentialité peut aussi y prévoir des exceptions.

Dans le cas qui nous occupe, l'article 9 de la *Charte québécoise des droits et libertés de la personne* ainsi que l'article 131(2) de la *Loi sur le Barreau*, prévoient que l'avocat peut être relevé, même implicitement, de son obligation de respecter le secret professionnel envers son client. Ainsi, le client peut autoriser son avocat à utiliser le courriel non sécurisé pour communiquer avec lui, même pour des renseignements couverts par le secret professionnel. Il est cependant préférable, et potentiellement plus approprié, d'y voir une autorisation implicite à l'utilisation du courriel non sécurisé plutôt qu'une renonciation au secret professionnel de la part du client.

Cette autorisation peut être implicite. Par exemple, si le client communique lui-même des renseignements confidentiels à son avocat par l'entremise de courriels non sécurisés, il est possible de conclure, selon les circonstances, qu'il s'agit d'une autorisation implicite pour que celui-ci procède de cette façon. Il s'agirait alors, autrement dit, d'une renonciation à l'utilisation de moyens de protection, tel le chiffrement.

Évidemment, une autorisation ou une renonciation expresse demeure préférable, et il est recommandé d'inclure une mention spécifique en ce sens dans la lettre de confirmation du mandat.

Conservation des courriels

Étant donné qu'un courriel constitue un document, il faut s'assurer de sa conservation et de sa gestion d'une manière appropriée (voir à cet effet la section 3 intitulée Gestion des documents électroniques). On devra, entre autres, s'assurer que l'accès au document électronique est protégé et réservé aux personnes concernées seulement (voir la section 1 intitulée Sécurité des communications et la sous-section concernant les mots de passe). Les courriels, comme toute forme de correspondance, font partie du dossier de l'avocat et doivent, à cet égard, être conservés (sur support papier ou électronique) conformément aux exigences du *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats* et de la *Loi concernant le cadre juridique des technologies de l'information*.

Ressources

Gestion des documents technologiques

- *Afin d'y voir clair, Guide relatif à la gestion des documents technologiques*, Fondation du Barreau du Québec

Acheminement du courriel

- Acheminement du courriel

SECTION 2 PROTECTION DE L'ACCÈS AUX DONNÉES

La protection de l'accès aux données peut faire l'objet de nombreuses méthodes opérant à divers niveaux. Ainsi, la section « Sécurité des communications » traitait de la protection des systèmes et de la configuration de ceux-ci afin de réduire la circulation des informations à ce qui est nécessaire pour opérer convenablement.

La protection de l'accès aux données peut aussi se faire par un processus d'authentification, qui consiste, pour un système informatique, à vérifier qu'un utilisateur est bien la personne qu'il prétend être avant de lui accorder l'accès à des systèmes ou à des services. On dit souvent qu'il y a trois façons d'identifier une personne : par ce qu'elle sait, par ce qu'elle est et par ce qu'elle a[43].

Les mots de passe étant la méthode d'authentification la plus répandue, avec le chiffrement, la prochaine section s'attardera plus spécifiquement à ces deux méthodes.

Mot de passe

Principe

L'accès à tout document ou information de nature juridique utilisé dans le cadre de l'exercice de la profession doit être limité à l'aide d'un mot de passe sécuritaire et modifié aux 30 jours. Cette protection peut viser le matériel informatique et/ou les logiciels utilisés.

Définition

Lors de la connexion à un système informatique, celui-ci demande la plupart du temps un nom d'utilisateur (*login* ou *username* en anglais) et un mot de passe (*password* en anglais) pour y accéder. Ce couple nom d'utilisateur/mot de passe forme ainsi la clé permettant d'obtenir un accès au système.

Risques

La plupart des utilisateurs, estimant qu'ils n'ont rien de vraiment secret à protéger ou qu'ils ne sont pas susceptibles de se faire voler de l'information, se contentent d'utiliser un mot de passe facile à retenir comme leur identifiant, le prénom de leur conjoint ou leur date de naissance.

[43] Article 41 de la LCCJTI.

À l'aide d'outils de génération de mots de passe, disponibles gratuitement sur le Web, n'importe qui peut essayer un grand nombre de mots de passe générés à l'aide de banques, aléatoirement ou par une combinaison des deux, jusqu'à ce que le mot de passe soit obtenu.

Chaque fois que des mots de passe pour des comptes chez de grands opérateurs Web sont compromis, les dictionnaires de mots de passe, disponibles aux pirates informatiques, s'enrichissent de millions de mots de passe. Il devient facile pour eux d'identifier les plus communs, ils seront les premiers à être testés lors d'attaques informatiques.

Plus un mot de passe est long, plus il est difficile à trouver, c'est-à-dire à « casser » en jargon informatique. Par ailleurs, un mot de passe constitué uniquement de chiffres sera beaucoup plus simple à casser qu'un mot de passe contenant des lettres et encore davantage qu'un mot de passe alphanumérique, c'est-à-dire qui contient des chiffres et des lettres.

Par exemple, un mot de passe de dix chiffres correspond à 100 millions de possibilités. Si ce nombre paraît élevé, un ordinateur doté d'une configuration modeste est capable de le casser en quelques secondes. À titre comparatif, on lui préférera un mot de passe de dix lettres, pour lequel il existe 200 milliards de possibilités. Malgré tout, un tel mot de passe peut être cassé en quelques minutes[44].

En cas de perte ou de vol de matériel informatique (clé USB, téléphone, ordinateur portable, etc.), ce sera plutôt le chiffrement qui viendra protéger l'information (voir la prochaine section à ce sujet).

Meilleures pratiques

Hormis la protection que les mots de passe offrent contre les attaques informatiques, ceux-ci protègent l'accès à différents systèmes ou ressources informationnelles.

Il convient de définir une politique en matière de mots de passe afin d'imposer aux utilisateurs le choix d'un mot de passe suffisamment sécuritaire.

Un mot de passe devrait être composé d'au moins dix caractères alphanumériques, c'est-à-dire de chiffres et de lettres, en plus d'être composé de minuscules, de majuscules et de caractères spéciaux.

Mots de passe à éviter

- Votre nom d'utilisateur
- Votre nom
- Votre prénom ou celui d'un proche (conjoint, enfant, etc.)
- Un mot du dictionnaire (qu'importe la langue), ou pire, un terme commun comme « mot de passe »
- Un mot à l'envers (les outils de cassage de mots de passe prennent en compte cette possibilité)
- Un mot suivi d'un chiffre, de l'année en cours ou d'une année de naissance (par exemple « password1999 »)
- Le même mot de passe pour plusieurs systèmes (qui augmente les risques si un des systèmes est effectivement compromis)

[44] Pour connaître la vitesse à laquelle un mot de passe peut être trouvé en fonction de sa complexité (longueur, composition, etc.) : www.lockdown.co.uk/?pg=combi

- Tout mot de passe utilisé ailleurs, surtout sur les réseaux sociaux

Surtout, gardez vos mots de passe confidentiels. Si vous les notez, ne les placez pas à des endroits où d'autres peuvent les consulter.

Les mots de passe cèdent la place aux phrases de passe

Un bon système pour choisir un mot de passe et pour vous en rappeler consiste à imaginer une « phrase secrète » par exemple : « J'aime le mois de septembre, c'est ton anniversaire mon amour! », et de le transformer par des chiffres et des lettres : **jlm09ctAma**!

Vous avez ainsi un mot de passe d'au moins dix caractères alphanumériques qui ne correspond absolument à aucun mot du dictionnaire et dont vous pourrez vous rappeler facilement : **jlm09ctAma!**

Inventez une phrase qui vous convient et suivez ces quelques règles pour utiliser un mot de passe sécuritaire. Ce genre de phrase secrète est plus sécuritaire qu'un mot de passe ordinaire, car il est plus long, plus complexe et moins prévisible (et donc plus difficile à « casser »).

Attention de ne pas remplacer une lettre ou un chiffre par des caractères assimilables (exemple, le chiffre 1 par un !). En effet, les outils permettant de craquer les mots de passe prennent en compte les possibles substitutions de caractères dans les mots de son dictionnaire (4 et A; I, L et le 1; le 5 et S; 7 et T, etc.).

Question de récupération de mots de passe

Plusieurs applications et logiciels permettent de récupérer le mot de passe à l'aide d'une question secrète. Les réponses fournies à cette question ne devraient pas être un élément facile à trouver (par exemple, le nom de votre conjoint(e)) que vous pourriez divulguer sur les réseaux sociaux.

Des alternatives aux mots de passe

De plus en plus d'outils permettent l'utilisation de la biométrie (par exemple, les empreintes digitales ou la reconnaissance faciale) comme solution de rechange aux mots de passe. Cette solution procure un niveau de sécurité très intéressant.

Considérer l'authentification multi-facteur

L'authentification multi-facteur est une pratique qui permet de rendre le système d'une entreprise encore plus sécuritaire et il est recommandé d'installer de tels systèmes d'authentification lorsqu'il est possible de le faire.

Par exemple, un système d'authentification pourrait obliger les utilisateurs à se connecter en saisissant un code de validation (généré sur un téléphone intelligent par exemple) en complément de leur nom d'utilisateur et de leur mot de passe.

Utiliser un gestionnaire de mots de passe

Un gestionnaire de mots de passe est un outil permettant de protéger une base de données de mots de passe. Ceci est particulièrement utile dans les cas où plusieurs mots de passe sont à retenir : le mot de passe de la base de données devient le seul à mémoriser. Ces outils peuvent également comporter un module de génération aléatoire de mots de passe, dont il n'est pas nécessaire de se rappeler. Les gestionnaires de mot de passe peuvent être sous forme de services infonuagiques (par exemple Passwordsafe) ou sous forme de logiciel installé sur un ordinateur, voire sur une clé USB.

Le mot de passe protégeant cet outil devrait cependant être choisi selon les plus hauts standards de sécurité, celui-ci donnant accès à tous les autres mots de passe.

Considérations éthiques

Enfin, notons qu'il est nécessaire pour l'avocat de se conformer aux pratiques susdites afin de respecter l'obligation de prudence envers son client[45] et de protéger le secret professionnel[46]. Vu les délais requis pour casser un mot de passe, il est primordial que celui-ci soit remplacé au moins mensuellement, par un mot de passe n'ayant pas été utilisé au cours des 12 mois précédents.

[45] *Code de déontologie des avocats*, art. 20

[46] *Code des professions*, art. 60.4.

Ressources

- Site de Microsoft sur les méthodes de création d'un mot de passe sécuritaire
- Site analysant le niveau de sécurité d'un mot de passe
- Force des mots de passe
- Générateur de mots de passe
- Gestionnaire de mots de passe
- Temps requis pour casser un mot de passe en fonction de sa longueur et de son contenu
- Logiciel de cassage de mots de passe Password Recovery Toolkit d'AccessData (200 000 essais par seconde)
- How to Make Two-Factor Authentication Work for You

Chiffrement

Principe

L'avocat devrait prendre les moyens raisonnables pour s'assurer que les renseignements confidentiels de ses clients ne puissent être consultés ou interceptés par un tiers non autorisé.

Définition

Le mot chiffrement (ou cryptage) est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre incompréhensibles sans une action spécifique.

Meilleures pratiques

Les données enregistrées sur des supports amovibles, tels une clé USB, un disque dur externe ou un iPod, peuvent être interceptées (trouvées ou volées) et devraient par conséquent être chiffrées. De plus, les messages transmis par courrier électronique et les données enregistrées sur les téléphones intelligents devraient également faire l'objet de chiffrement.

Dans certaines circonstances, le chiffrement permet non seulement de préserver la confidentialité des données, mais aussi d'en garantir l'intégrité et l'authenticité.

De façon générale, plus l'information est exposée et/ou confidentielle, plus elle doit être protégée par chiffrement.

Ressources

Logiciels de chiffrement

- Stormshield Endpoint Security (fonctionne sous Windows XP, Windows Vista, Windows 7)
- PGP – Whole Disk Encryption
- Microsoft Virtual Private Network

- GNU Private Guard
- BitLocker (Microsoft)
- FileVault 2 (pour Mac)

Le chiffrement, vu par quelques barreaux américains :

- Encryption conniption

Processus de sécurité informatique pour gérer le départ d'un employé

1. Désactiver temporairement (de deux à quatre semaines) le compte utilisateur de l'ex-employé qui a quitté le cabinet, puis le supprimer définitivement.

2. Désactiver le compte de téléphonie cellulaire, la boîte vocale et le poste téléphonique de l'ex-employé.

3. Désactiver les accès au réseau privé virtuel (RVP ou *Virtual Private Network*, VPN en anglais).

4. Remplacer tous les mots de passe des comptes que l'ex-employé aurait pu utiliser : site Web, transaction bancaire (PayPal), système téléphonique, code du système d'alarme, etc.

5. Archiver les documents, courriels, contacts, tâches et calendrier de l'ex-employé.

6. Rediriger temporairement l'adresse courriel de l'ex-employé vers la boîte de courriel du superviseur afin de récolter la correspondance et aviser les correspondants du départ de l'employé.

7. Récupérer tout matériel informatique ordinateur, portable, tablette appartenant au cabinet.

8. Retirer toute page ou tout profil de l'ex-employé sur le site Web du cabinet.

9. Le cas échéant, retirer tout droit que l'ex-employé pourrait avoir comme administrateur du site Web du cabinet ou de sa page corporative sur les réseaux sociaux.

10. Le cas échéant, retirer tout droit de gestion que l'ex-employé pourrait détenir sur le (ou les) nom(s) de domaine(s) du cabinet.

Lors d'un congédiement, les accès de l'employé devraient être coupés immédiatement, à moins que l'employé continue de travailler pendant la période du délai de congé que la loi vous oblige à lui donner. Si tel est le cas, il est prudent de limiter l'accès en écriture de l'employé dans les semaines précédant son départ.

Entente avec les fournisseurs

À l'extérieur d'un contexte informatique, l'avocat qui choisit un emplacement pour y déposer des documents qui concernent sa pratique se sera enquit des mesures de sécurité disponibles. On ne peut imaginer un cabinet d'avocat(s) sans mur, sans porte, sans serrure, et où n'importe qui pourrait entrer en tout temps. De la même façon, on n'imagine pas les documents de l'avocat sans dossiers ni classeurs pour éviter que le premier venu les voie, et qu'un étranger cherchant une information la trouve. De plus, l'avocat qui retient les services d'un fournisseur pour effectuer des recherches juridiques ou factuelles aura tôt fait d'exiger la confidentialité de ces recherches.

Dans un contexte informatique, les mêmes principes s'appliquent.

Il est de plus en plus fréquent que les avocats aient recours à un fournisseur afin d'obtenir différents services informatiques (hébergement, accès Internet, technicien informatique, communications, etc.). Le fournisseur a alors accès aux données informatiques de l'avocat, ce qui représente un problème majeur quant aux obligations déontologiques auxquelles est soumis l'avocat. Certaines mesures devraient être prises afin de préserver la confidentialité de l'information relayée par le fournisseur, transmise ou accessible au fournisseur ou hébergé par celui-ci.

Voici ces mesures :

- Il est nécessaire de conclure une entente de confidentialité[47]avec le fournisseur afin de protéger adéquatement l'information confidentielle. Cette entente devrait notamment prévoir les conditions de manipulation, de transfert des données, d'utilisation, de stockage et de disponibilité de l'information, ainsi que les droits d'accès et de propriété de données.

- Hormis cette entente de confidentialité, le contrat de service devrait inclure des dispositions relatives à la fin du contrat ou des activités (volontairement ou par la faillite ou la fin des activités du fournisseur) et au transfert des données, au droit d'audit ou de vérification.

- Les fournisseurs en matière informatique peuvent avoir des attitudes variées devant les demandes de leurs clients avocats. Un technicien chargé d'une réparation pourrait bien accepter de signer une entente de confidentialité sans négocier, alors qu'un installateur de système informatique voudra en revoir les termes en vue d'éviter toutes formes d'obligation de résultat, et que le fournisseur d'un service de recherche sur Internet imposera des conditions en ligne qui sont non-négociables et prévoient la réutilisation des données saisies par l'utilisateur, et ce, dans toutes les entreprises et filiales de l'entreprise offrant ce service. Il est d'une grande importance pour l'avocat de veiller, dans la négociation ou l'acceptation de ces ententes, au respect de ses obligations déontologiques. En particulier, en ce qui a trait à l'hébergement des données, l'avocat doit vérifier le contrat de service afin de s'assurer que tout est conforme à ses obligations déontologiques. Il s'agit après tout, dans la plupart des cas, de l'endroit où seront entreposés les dossiers!

- Attention aux contrats d'adhésion : l'avocat doit se demander si l'entente de confidentialité répond à ses obligations déontologiques.

[47] Art.26, *Loi concernant le cadre juridique des technologies de l'information.*

L'infonuagique (*cloud computing*)

Principe

L'avocat doit prendre les moyens raisonnables pour s'assurer que les renseignements confidentiels qui transitent ou sont hébergés dans le nuage ne puissent être consultés ou interceptés par un tiers non autorisé.

Définition

L'infonuagique ou *cloud computing* est un : « modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation[48] ». L'infonuagique peut être envisagée selon différents modèles de déploiement (privé interne, privé externe, public, communautaire et hybride) et de services (logiciel-service, plateforme-service, infrastructure-service, etc.) possédant chacun leurs avantages et leurs inconvénients.

Modèles de déploiement :

- **Infonuage privé interne** : Modèle d'infonuagique selon lequel les ressources demandées sont installées à l'intérieur de l'organisation cliente (exemple : avoir ses propres serveurs)
- **Infonuage privé externe** : Modèle d'infonuagique selon lequel les ressources sont gérées à l'extérieur de l'organisation cliente, mais dans un nuage qui est réservé à celle-ci (exemple : un contrat d'hébergement)
- **Infonuage public** : Modèle d'infonuagique selon lequel les ressources sont offertes publiquement par une entreprise (exemple : iCloud, Gmail, Google Docs, Dropbox, Outlook, Hotmail, Yahoo Mail, Microsoft Office 365, etc.)
- **Infonuage communautaire** : Modèle d'infonuagique apparenté au modèle privé qui servira à combler les besoins des organismes voulant mettre en commun leurs ressources. (Les gouvernements australien et britannique disposent de tels modèles.)
- **Infonuage hybride** : Modèle d'infonuagique qui implique généralement une combinaison de deux ou plusieurs modèles (privé, public et/ou communautaire), selon les besoins de l'organisation

[48] Office de la langue française, *Grand dictionnaire terminologique*, en ligne : www.granddictionnaire.com.

Modèles de service :

- **Logiciel-service (*Software as a Service* ou SaaS)** : « Logiciel[49] prêt à l'emploi, loué à la demande chez un fournisseur de services, accessible par Internet ou par le réseau d'une organisation, ou par les deux à la fois. Le logiciel-service est accessible par Internet dans le cas d'un nuage public, par le réseau d'une organisation dans celui d'un nuage privé ou par les deux à la fois dans le cas d'un nuage hybride » (exemple : Google docs)[50].

- **Plateforme-service (*Platform as a Service* ou PaaS)** : « Plateforme[51] prête à l'emploi, louée à la demande chez un fournisseur de services, accessible par Internet ou par le réseau d'une organisation, ou par les deux à la fois. La plateforme-service est accessible par Internet dans le cas d'un nuage public, par le réseau d'une organisation dans celui d'un nuage privé ou par les deux à la fois dans le cas d'un nuage hybride. La plateforme-service met à la disposition des développeurs un environnement d'exécution (système d'exploitation, matériel, réseau) qui leur permet d'installer ou de créer leurs propres logiciels » (exemple : les outils de développement de Facebook)[52].

- **Infrastructure-service (*Infrastructure as a service* ou Iaas)** : « Infrastructure[53] prête à l'emploi, louée à la demande chez un fournisseur de services, accessible par Internet ou par le réseau d'une organisation, ou par les deux à la fois[54] » (exemple : Azure de Microsoft)

Exemples

[49] Le terme « logiciel » peut être défini comme étant l'« ensemble des programmes destinés à effectuer un traitement particulier sur un ordinateur ». Office de la langue française, *Grand dictionnaire terminologique*, en ligne : www.granddictionnaire.com.
[50] Définition : Office de la langue française, *Grand dictionnaire terminologique,* en ligne : www.granddictionnaire.com.
[51] Le terme « plateforme » peut être défini comme étant une « Structure matérielle d'un système informatique, principalement basée sur le type de système d'exploitation utilisé ». Office de la langue française, *Grand dictionnaire terminologique*, en ligne : www.granddictionnaire.com.
[52] Office de la langue française, *Grand dictionnaire terminologique,* en ligne : www.granddictionnaire.com.
[53] Le terme « infrastructure » peut être défini comme étant l'« ensemble des éléments de configuration utilisés dans la prestation des services des TI, qui comprend le matériel informatique, les logiciels, les installations, les ressources humaines, la documentation et les données ». Office de la langue française, *Grand dictionnaire terminologique*, en ligne : www.granddictionnaire.com.
[54] Office de la langue française, *Grand dictionnaire terminologique,* en ligne : www.granddictionnaire.com.

Pour l'instant, les types d'infonuagique les plus utilisés par les avocats sont les services gratuits de courriel Web tels Gmail ou Hotmail et les services gratuits de stockage ou de partage de copies tels Dropbox ou iCloud. (Un tableau comparatif des divers services de stockage et de partage des fichiers locaux en ligne est disponible ici : http://en.wikipedia.org/wiki/Comparison_of_file_hosting_services.)

Ces derniers services permettent de sauvegarder des documents dans le nuage et d'accéder à ceux-ci de n'importe quel poste de travail, voire même d'une tablette ou d'un téléphone intelligent (dès lors que l'on possède les autorisations requises). L'utilisation de ce type de services gratuits n'est pas recommandée pour les raisons énoncées dans la section ci-dessous portant sur les risques.

Comme avocat, vous devez prendre les moyens raisonnables pour assurer la sécurité des données de vos clients et effectuer vos propres vérifications au moment de choisir votre fournisseur. Pour vous aider, consulter la liste de contrôle en matière d'infonuagique en annexe de ce guide.

Risques

Malgré ses avantages notoires (notamment au niveau des coûts et de l'accessibilité), l'infonuagique présente d'importants inconvénients en raison des risques au niveau de la sécurité des données hébergées dans le nuage ou transitant par celui-ci. D'abord, quant à la disponibilité des données, il est possible pour l'information hébergée dans le nuage de devenir inaccessible parce que les serveurs deviennent eux-mêmes indisponibles (panne de courant, entretien, etc.).

Notons toutefois que ce risque est généralement inversement proportionnel à la taille du nuage, puisque les nuages les plus importants auront en place des mesures de redondance pour contrer de telles situations.

Une problématique plus importante est toutefois liée à l'inaccessibilité des données due au fait que celles-ci sont en quelque sorte prises en otage par le fournisseur de service d'infonuagique – par exemple parce que les frais d'hébergement n'ont pas été payés. Il importe également de porter attention à la question de la disposition des données afin d'éviter le transfert de propriété de celles-ci à l'hébergeur, soit au moment de la signature du contrat, soit en cas de non-paiement, ou tout simplement à la fin du contrat. Il est finalement important d'examiner les délais dans lesquels les données seront remises à la fin du contrat.

Bien que de telles clauses d'appropriation des données soient plus rares, plusieurs prestataires de services d'infonuagique (principalement les services « gratuits ») s'accordent une licence d'exploitation quant aux données hébergées. Il existe donc un risque au niveau de la confidentialité de ces données, notamment en ce qui a trait aux données protégées par le secret professionnel. Ce risque est par ailleurs accentué par le fait que les données situées « dans le nuage » se retrouvent en fait sur un serveur, lequel peut être situé à l'extérieur du Québec, notamment dans des juridictions qui ne comportent pas les mêmes garanties au niveau de la protection des données confidentielles et du privilège avocat-client. Par exemple, aux États-Unis, d'où une majorité de services d'infonuagique sont contrôlés, il est possible pour l'État d'avoir accès aux données hébergées dans le nuage nonobstant les droits des clients. Le privilège avocat-client n'est en effet pas un droit comportant les mêmes protections qu'au Canada et, dans certaines causes, ce type de données ont fait l'objet de perquisitions.

Finalement, comme tout autre service accessible via Internet, les services d'infonuagique sont vulnérables aux tentatives d'accès par des tiers non autorisés, notamment si le compte d'un utilisateur n'est pas protégé par un mot de passe suffisamment sophistiqué.

Meilleures pratiques

L'avocat qui désire héberger des données confidentielles dans un nuage – notamment des données visées par le secret professionnel – devrait privilégier les nuages composés de serveurs situés uniquement en sol canadien et sous le contrôle d'entités canadiennes.

Si une telle option s'avère indisponible vu, par exemple, le modèle d'infonuagique désiré, le chiffrement des données, à la source, est fortement recommandé. À cet égard, il importe de préciser que des documents préparés par le gouvernement américain et rendus publics par Edward Snowden indiquent que certains prestataires de services infonuagiques américains fourniraient les clés de chiffrement aux autorités. Il serait donc préférable de recourir à un système de chiffrement distinct de celui offert par le service d'infonuagique, bien que certains communiqués également rendus publics par Edward Snowden suggèrent que cette pratique n'est pas sans risque pour les mêmes raisons (la capacité pour le gouvernement américain d'avoir accès aux clés). Ainsi, nous sommes d'avis que, peu importe les mesures de sécurité mises en place, l'hébergement à l'étranger est très risqué d'un point de vue déontologique.

Il s'avère par ailleurs plus prudent d'adopter une solution proposée par une entreprise reconnue et de s'abstenir d'utiliser les services d'entrée de gamme ou dits « à l'essai » comportant généralement l'attrait d'espace de stockage gratuit (en échange, bien souvent, de licences d'exploitation des données hébergées). Le choix de solutions payantes qui offrent des garanties de protection des données confidentielles est donc souvent incontournable pour s'acquitter de ses obligations déontologiques.

Quant à l'accès aux données, il importe de respecter les conseils du présent guide quant à l'utilisation des mots de passe et du chiffrement des données.

Dans tous les cas, il est important d'informer les clients des risques liés au modèle d'infonuagique sélectionné et d'obtenir leur accord lorsque ce modèle ne permet pas de garantir la protection des informations confidentielles, dont les renseignements personnels et ceux couverts par le secret professionnel. D'ailleurs, dès que les données des clients sont hébergées ailleurs qu'au bureau ou sont répliquées à l'externe, il est préférable d'en aviser le client.

Finalement, il est fortement recommandé de garder une copie de sauvegarde de toute information hébergée dans le nuage afin d'assurer la disponibilité de cette information en cas de panne ou de différend avec le prestataire de services infonuagiques.

Ressources

Jean-François DE RICO, « L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements », (2014) nº 6 *Technologies de l'information en bref*.

Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », étude présentée au Conseil du Trésor du Québec, 2014, en ligne : http://www.cyberjustice.ca/publications/etude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-pour-le-gouvernement-du-quebec/

Articles pertinents sur le sujet

- Guide de l'infonuagique, Volume 3 — Considérations de contrôle et de sécurité, Architecture d'entreprise gouvernementale 3.0
- Les services infonuagiques Microsoft arrivent au Canada.
- HIPAA-Compliant Cloud File Services
- Comparison of files hosting services
- Cloud Storage and Client Confidentiality: A Perfect Match or Perfect Storm?
- Best free encryption utility for cloud storage
- Top 6 free encryption tools to protect your data stored in the cloud.

Avis juridiques de divers barreaux concernant l'Infonuagique

- Cloud Ethics Opinions Around the U.S.

Sécurisation des bureaux, des salles et des équipements

1. Verrouiller les portes.

2. Verrouiller les classeurs.

3. S'assurer que le ou les serveurs sont installés dans un environnement verrouillé, bien ventilé, branché sur une batterie de secours (UPS) et ayant une température constante entre 15° C et 20° C.

4. Éteindre les postes de travail ou activer l'écran de veille sécurisé.

5. Conserver dans un endroit protégé et verrouillé tous les médias contenant des données confidentielles (CD-ROM, DVD, disque dur externe, clé USB, cassettes de sauvegarde, etc.).

6. Chiffrer les données confidentielles sur les ordinateurs portables et les médias amovibles (CD-ROM, DVD, disque dur externe, clé USB, etc.).

7. Activer la sécurité des agendas personnels ou des téléphones intelligents par la mise en place d'un code de déverrouillage de l'équipement (écran de veille avec mot de passe) et le chiffrement de l'information.

Mise au rebut ou recyclage du matériel informatique

Serveurs, ordinateurs et ordinateurs portables

- Supprimez les données enregistrées sur les disques durs par l'exécution d'un script en plusieurs passes (pour plus de détails, contactez votre consultant informatique ou faites l'acquisition d'un logiciel se conformant à la norme canadienne CSEC ITSEG-06);

  OU

- Les détruire physiquement par déchiquetage (pour plus de détails, contacter votre consultant informatique ou une firme spécialisée dans la destruction physique ayant la certification internationale (National Association for Information Destruction ou NAID).

Téléphones intelligents

1. Réinitialisez le téléphone portable en sélectionnant l'option de suppression de toutes les données;

2. Retirez la carte mémoire additionnelle ou supprimez les données pouvant s'y retrouver.

Photocopieur et appareils d'imagerie

1. Videz les mémoires de vos photocopieurs ou appareils d'imagerie. Ces appareils utilisent un disque dur branché sur le réseau du cabinet, qui est donc accessible par Internet.

Truc écolo

Les compagnies de recyclage de vieux ordinateurs

Il existe deux types de compagnies de recyclage d'ordinateurs : celles qui récupèrent les pièces pour fournir des équipements aux plus démunis (pays du tiers monde, secteurs défavorisés, pièces de rechange) et celles qui récupèrent les matières premières (plastique, plomb, silicium). Dans les deux cas, il est grandement préférable de retrouver nos vieux ordinateurs, imprimantes et écrans sur leurs tablettes que dans les déchets. Toutefois, vous devez vous assurer de suivre la procédure prévue dans le présent guide quant au recyclage, préalablement à la remise de votre matériel informatique.

Voici quelques compagnies de recyclage que vous pouvez contacter :

- RecyPro
- Reboot Canada (en anglais seulement)
- MultiRecycle
- Insertech

Voici un répertoire pour trouver un **point de dépôt officiel près de chez vous** :

- Recycler mes électroniques (ARPE)

SECTION 3 GESTION DES DOCUMENTS ÉLECTRONIQUES

Il serait impensable de prétendre à une gestion efficace de documents papier sans agrafes, chemises, dossiers et autres classeurs. Il en est de même pour la gestion des documents électroniques. Nous considérerons donc le classement et la sauvegarde des documents électroniques, ainsi que les « métadonnées », qui permettent une gestion encore plus précise des documents.

Classement des documents

Principe

Un classement judicieux des fichiers électroniques contenant les documents faisant partie des dossiers de l'avocat est important pour épargner du temps, éviter la perte de documents et faciliter la conformité aux règles encadrant la tenue des dossiers des avocats et la démonstration de celle-ci.

Définition

Les documents électroniques créés par l'avocat sont enregistrés dans des fichiers. L'avocat peut décider du nom de chaque fichier. Ces fichiers peuvent être classés dans des répertoires et des sous-répertoires (ou « dossiers électroniques ») afin qu'ils soient repérables et accessibles facilement de la même façon que les documents sur support papier.

Exemple

Lorsque l'avocat enregistre un document informatique pour la première fois, il se fait habituellement demander, par le logiciel qu'il utilise, quel nom portera le fichier informatique dans lequel le document devra être enregistré.

L'avocat a aussi le choix du répertoire ou du sous-répertoire dans lequel ce fichier sera enregistré. L'avocat peut créer autant de répertoires et de sous-répertoires qu'il le juge nécessaire pour organiser ses documents de façon utile.

Utilité

Quant au nom du fichier

Il apparaît efficace que le nom d'un fichier décrive son contenu, ce qui aura pour effet de classer les divers éléments du dossier selon leur nature, comme le prévoit la réglementation concernant les normes

de tenue des dossiers. Le tout a pour but que puisse être retrouvé efficacement tout élément contenu au dossier, qu'il s'agisse d'une lettre, d'une décision ou d'une procédure.

Une convention de nommage des documents devrait être mise en place afin de standardiser leur présentation et ainsi faciliter leur recherche. Une telle convention pourrait prévoir que tous les noms des fichiers comportent certains éléments clés, par exemple :

Date du document_son objet_nom de l'émetteur_ la version du document
2015-04-13_Ltr dossier_Me Untel_V1

Quant au répertoire

Il peut être souhaitable pour l'avocat de créer des dossiers informatiques, tout comme il créait auparavant des dossiers papier, pour chacun des mandats qu'on lui confie.

Risques

Il est parfaitement possible de perdre un fichier sur son ordinateur! Quand l'ordinateur contient un grand volume de fichiers de tous genres, il est relativement facile de perdre un fichier s'il n'est pas nommé, classé ou indexé de façon utile ou suite à une erreur de classement.

Un autre risque non négligeable lié à un classement déficient des documents concerne la gestion des droits d'accès de ces documents (voir la section sur la protection de l'accès aux données à ce sujet.)

Meilleures pratiques

L'Inspection professionnelle rappelle souvent aux membres du Barreau lors de ses visites que les documents papier devraient idéalement être classés dans le dossier papier de façon à ce que :

- La correspondance soit regroupée par ordre chronologique;
- Les procédures soient aussi regroupées par ordre chronologique;
- Les notes au dossier et la recherche soient regroupées à part; et
- Une fiche-client, comprenant les données du client et du dossier ainsi qu'un calendrier des dates importantes du dossier, soit incluse.

Il est recommandé de créer un système de sous-répertoires informatiques distincts pour chaque client, ou pour chaque dossier si chaque client a accordé plusieurs mandats à l'avocat. On pourrait même suggérer de créer un dossier nommé « Latronche » et un sous-dossier nommé « 3e mandat ».

Un chemin d'accès et un nom de fichier évocateurs, décrivant bien ce qu'ils contiennent, épargneront, dans la plupart des cas, du temps passé à chercher des documents, tout en laissant davantage pour le travail dans le dossier.

Il est également suggéré que le nom de chaque document commence par sa date. Ainsi, les documents se classent automatiquement à l'écran en ordre chronologique, ce qui facilite la recherche.

Il est possible d'améliorer encore l'efficacité de la gestion des documents. Si le nom du fichier, le nom du répertoire qui le contient et sa date de création permettent un certain classement des documents, il est possible d'ajouter encore plus d'information concernant les documents afin d'en permettre le classement selon différents critères. Pour ce faire, les logiciels de gestion documentaire plus sophistiqués utilisent les métadonnées des documents pour affiner les recherches et l'indexation. Il sera ainsi possible d'indiquer, pour un document, quels avocats y ont travaillé, la date de la fermeture du dossier, des mots clés, les coordonnées des personnes responsables ou tout autre renseignement pertinent. Il est possible de saisir ces métadonnées dans la même fenêtre que celle où elles peuvent être consultées. Par exemple, dans le logiciel MS Word 2003 et les versions plus récentes, la consultation des propriétés (menu Fichier/Propriétés) du document donne accès aux métadonnées et permet de remplir plusieurs champs.

Quant à la correspondance par courriel, selon le logiciel utilisé, elle peut être agrégée dans une base de données unique pour tous les courriels. Nous suggérons dans ce cas de créer, dans le logiciel de messagerie, un répertoire portant le nom du dossier visé. Lors de la fermeture du dossier, les courriels peuvent être archivés et exportés, de sorte qu'ils sont contenus dans un seul fichier distinct qui pourra être placé dans le répertoire « physique » du dossier.

Copie de sauvegarde des documents/plan de reprise

Principe

En plus de l'enregistrement normalement effectué pour ne pas perdre un fichier à la suite de la fermeture d'un document ou d'un logiciel, une copie de sauvegarde de l'ensemble des fichiers devrait être effectuée quotidiennement sur un support indépendant conservé dans un lieu autre afin de pouvoir être récupérée en cas de désastre. Les copies de sauvegarde devraient être testées régulièrement.

Définition

En informatique, la copie de sauvegarde (*backup* en anglais) est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.

Ce terme est proche de deux notions :

- L'enregistrement des données, qui est l'opération d'écriture des données sur un outil de stockage d'information, tel qu'un disque dur, une clé USB, des bandes magnétiques, etc.

- L'archivage, qui consiste à enregistrer des données sur un support à des fins légales ou historiques.

La sauvegarde passe nécessairement par un enregistrement des données, mais n'a pas une finalité d'archivage. En fait, les copies de sauvegarde ne devraient jamais être utilisées comme mécanisme d'archivage ou de conservation.

Exemple

Dans le passé, on pouvait lire de temps à autre dans le *Journal du Barreau* un appel aux confrères et aux consœurs dans le but de reconstituer des dossiers détruits par un incendie. Une copie de sauvegarde permettra de remplacer sans délai les documents électroniques détruits au moyen d'une copie de ces documents, que l'avocat aurait par exemple conservée à sa résidence. Dans ce cas, il est à noter que la copie des dossiers est soumise aux mêmes règles concernant le maintien du secret professionnel. Le support de stockage d'information conservé à domicile pourra, par exemple, être chiffré pour satisfaire à ces exigences.

Utilité

Les copies de sauvegarde sont utiles surtout pour permettre de restaurer un système informatique suite à un incident (bris ou perte d'un support de stockage comme un disque dur, ou de la totalité ou d'une partie des données qu'il contient).

De telles copies de sauvegarde peuvent être utiles devant la menace de rançongiciels (aussi appelés *ransomware*). Ce type de logiciels malveillants a pour objet de permettre à un pirate de bloquer l'accès à des données, de verrouiller un ordinateur ou de chiffrer des données. Pour rétablir l'accès aux données, la victime est « invitée » à verser une somme d'argent au pirate.

Risques

Même la technologie la plus perfectionnée peut cesser de fonctionner. Un accès informatique bien protégé peut faire l'objet d'une intrusion. Un ordinateur peut être volé même dans un bureau bien verrouillé. Un immeuble de bureaux peut être la proie des flammes ou être sujet à un autre sinistre, tel un dégât d'eau.

Il est donc extrêmement important d'effectuer régulièrement une copie de sauvegarde de ses fichiers informatiques, laquelle pourra être utilisée pour assurer la continuité des affaires. Cette copie de sauvegarde devrait être conservée dans un endroit sûr, à l'extérieur du cabinet. Les causes les plus fréquentes sont notamment les cas de problème technique avec l'ordinateur dont on se sert tous les jours, de virus, de perte ou de vol d'un équipement informatique contenant des fichiers.

Meilleures pratiques

Avant de concevoir le système de sauvegarde des données de l'entreprise, on doit se poser plusieurs questions :

- Sur quoi sauvegarder?
- Quoi sauvegarder et quand?
- Comment s'assurer d'une sauvegarde optimale de mes données?

Sur quoi sauvegarder?

Voici quelques-unes des solutions disponibles pour sauvegarder vos données :

Disque dur externe

L'utilisation d'un disque dur externe est certainement des plus économiques et pratiques. Les disques durs externes peuvent atteindre des capacités de stockage importantes, et certains modèles disposent même de fonctions pour planifier des sauvegardes automatiquement.

Clé USB

Les clés USB sont abordables, faciles à transporter mais leur capacité de stockage limitée constitue leur principal inconvénient. Elles sont aussi fragiles et peuvent facilement être égarées. Pour toutes ces raisons, elles ne sont pas des supports à envisager.

Sauvegarde en ligne

L'utilisation de sites Web offrant le service de sauvegarde en ligne est une solution intéressante puisque la procédure se fait automatiquement et ne requiert aucune intervention de la part de l'utilisateur. Il importe cependant de s'assurer que le site d'hébergement des données soit situé au Québec ou au Canada afin d'éviter les problèmes de confidentialité, tels que ceux rencontrés avec, par exemple, le « Patriot Act » américain. À cet égard, il est recommandé de conclure une entente de confidentialité avec le fournisseur afin de protéger adéquatement l'information confidentielle. Pour plus de détails, veuillez consulter la section sur l'infonuagique.

Quoi sauvegarder?

La méthode la plus simple est la sauvegarde complète (*full backup* en anglais); elle consiste à copier toutes les données à sauvegarder, que celles-ci soient récentes, anciennes, modifiées ou non, en plus des fichiers, systèmes et logiciels.

Par contre, cette méthode est longue et coûteuse en termes d'espace disque. Afin de gagner du temps de sauvegarde, l'avocat peut effectuer une sauvegarde différentielle à chaque jour des données seulement. La sauvegarde différentielle effectue une copie des fichiers créés ou modifiés depuis la dernière sauvegarde complète.

Ces sauvegardes peuvent, entre autres, se faire sur une unité de « disque dur » externe relativement peu coûteuse. Certains de ces appareils contiennent un logiciel qui gère automatiquement la sauvegarde différentielle.

En matière de sauvegarde de données, nous vous recommandons d'utiliser un seul répertoire. Ainsi, la sauvegarde est simplifiée et cela évite de sauvegarder l'ensemble des fichiers des programmes lors d'une procédure de sauvegarde.

De façon mensuelle, une sauvegarde complète des données, y compris les programmes, sera utile.

Comment s'assurer d'une sauvegarde optimale de mes données?

Peu importe les moyens que vous prenez pour sauvegarder vos données, idéalement, vous devriez :

- Garder les données dans un lieu différent du lieu d'origine (par exemple, il ne faut pas conserver votre disque dur externe branché à votre ordinateur en permanence);
- Multiplier les outils de sauvegarde (principe LOCKSS : *Lots of copies keep stuff safe*);
- Automatiser les sauvegardes de façon à ce qu'elles soient quotidiennes;
- Vous assurer du chiffrement des données.

À titre indicatif, voici comment automatiser une sauvegarde de votre ordinateur sur un disque externe et vous assurer du chiffrement de vos données :

- Avec Windows : Démarrer > Panneau de configuration > Assistant de configuration BitLocker (outil de chiffrement inclus dans Windows 7 Pro Edition Entreprise et Ultimate, dans Windows 8.1 Pro et dans Windows 10 Pro), puis suivre les étapes de l'Assistant. Lorsque BitLocker est

activé sur l'ordinateur, il suffit de chiffrer le support contenant la copie de sauvegarde. Si la version de Windows utilisée n'inclut pas BitLocker, il est toujours possible d'utiliser un autre logiciel de chiffrement pour protéger le support contenant la copie de sauvegarde (voir la section chiffrement).

- Avec Mac : Dans le menu Application, choisir Time Machine et glisser le curseur en position activée. Dans la partie gauche de la fenêtre Utilitaire de disque, sélectionner le disque que vous souhaitez utiliser avec Time Machine. Choisir l'option « Chiffrer le disque de sauvegarde » si vous souhaitez chiffrer votre disque externe de sauvegarde Time Machine à l'aide de FileVault 2 (OS X Lion ou version ultérieure).

Métadonnées

Principe

À moins de bien maîtriser les métadonnées, les avocats devraient, par précaution, purger les métadonnées des documents qu'ils acheminent électroniquement à la partie adverse ou à des tiers, à moins que les documents ne soient des éléments de preuve, qui doivent impérativement demeurer intègres.

Définition

Le terme « métadonnée » signifie « donnée à propos d'une donnée ». Le *Grand dictionnaire terminologique* de l'Office québécois de la langue française propose la définition suivante : « Donnée qui renseigne sur la nature de certaines autres données et qui permet ainsi leur utilisation pertinente ». Bref, il s'agit d'information relative au contexte d'un document. Les métadonnées sont généralement enchâssées dans le document électronique et ne sont pas visibles à moins d'accéder aux propriétés du document, voire d'utiliser des logiciels spéciaux.

Exemple

Sans le savoir, les gens connaissent bien les métadonnées puisqu'ils les utilisent au quotidien dans plusieurs logiciels. Par exemple, dans le logiciel Microsoft Outlook, les champs suivants constituent des métadonnées : « de », « à », « cc », « cci », « date d'envoi », « date de réception » et même l'« objet » du courriel! En outre, un courriel contient généralement beaucoup d'informations retraçant, dans chaque serveur, le chemin parcouru de l'expéditeur au destinataire.

Un autre exemple est le logiciel Microsoft Word, qui permet d'accéder aux métadonnées à l'aide des propriétés du document (Office 2003 et précédents : Fichier > Propriétés; Office 2007 : Bouton Office > Préparer > Propriétés; Office 2013 : Fichier > Propriétés dans la colonne de droite). La majorité des champs se trouvant sous chacun des onglets constituent des métadonnées. Enfin, la date de l'enregistrement d'un texte n'apparaît pas dans le texte, mais peut être utilisée par un logiciel pour identifier la version la plus récente du texte.

Utilité

L'objectif premier des métadonnées est d'automatiser divers processus de traitement de l'information, tels que l'organisation, la recherche et la catégorisation. Certaines sont définies et inscrites

automatiquement alors que d'autres peuvent être ajoutées par l'usager ou par des systèmes de gestion de l'information lors de l'enregistrement des documents. Certaines métadonnées permettent de retracer l'historique d'un document et s'avèrent ainsi nécessaires lorsque vient le temps de démontrer l'intégrité de celui-ci.

Risques

Par contre, pour l'avocat et l'administration de la justice, ces métadonnées créent des risques importants dont les avocats doivent être conscients. En effet, les métadonnées peuvent comporter des renseignements confidentiels, dont certains sont couverts par le secret professionnel.

Par exemple, les avocats génèrent fréquemment des documents (p. ex., contrats, procédures, etc.) qu'ils acheminent à leurs clients par courriel pour obtenir leurs commentaires. Ces documents sont ensuite retournés à l'avocat avec certains changements, commentaires ou annotations à l'aide de la fonction de suivi des modifications (*Track Changes*[55]). Ces informations sont fréquemment couvertes par le secret professionnel ou le privilège relatif au litige. Or, après avoir seulement « masqué » les modifications susdites, ces documents sont fréquemment acheminés tels quels à la partie adverse, à ses procureurs ou à des tiers. Ainsi, dans la mesure où l'autre partie possède des connaissances informatiques minimales, il lui est possible de faire ressortir ces modifications, commentaires ou annotations et d'en prendre connaissance.

Meilleures pratiques

Il existe deux grandes façons d'éliminer ces informations, et du coup, les risques qui y sont associés : A) les supprimer à l'aide de certains outils ou B) convertir le fichier au standard PDF.

A. Microsoft a compris ces risques et a développé un outil d'inspection et d'élimination des métadonnées, qu'elle a d'ailleurs inclus par défaut dans sa suite Office 2007 (Bouton Office > Préparer > Inspecter le document). Cet outil permet d'éliminer de nombreuses métadonnées ainsi que d'autres informations pouvant être confidentielles.

B. Plusieurs logiciels (voir ressources) permettent d'imprimer[56] les documents en format PDF. Ce processus permet de supprimer l'information pouvant être confidentielle en transformant le document modifiable en un document statique.

[55] N.B. Techniquement, le suivi des modifications, les commentaires, etc., ne sont pas des métadonnées. Dans le cadre du présent document, ils sont malgré tout considérés comme tels par souci de simplification. Afin d'en apprendre davantage, nous vous invitons à consulter la section des Ressources.

[56] Attention! Il est important d'imprimer en format PDF et non d'« enregistrer sous », comme le permettent certains logiciels, dont Microsoft Office depuis son édition 2007 et Adobe Acrobat, puisque enregistrer un document de la sorte n'élimine pas les métadonnées.

Éthique et déontologie

Notons pour terminer qu'il est légitime, voire utile, pour un avocat de prendre connaissance des métadonnées contenues au sein d'un document émanant de son client. De plus, dans la mesure où de l'information potentiellement couverte par le secret professionnel est identifiée, l'avocat doit en informer le procureur de la partie adverse. Par ailleurs, il serait négligent de se baser sur ce principe pour éviter de supprimer les métadonnées des documents puisque ceux-ci pourraient tomber entre les mains de tiers n'ayant pas l'obligation déontologique susdite incombant à l'avocat. Nous renvoyons ici le lecteur à la section sur la réception accidentelle d'informations possiblement protégées par le secret professionnel.

Ressources

Explications relatives aux métadonnées

- Wikipédia

Outil d'inspection et d'élimination des métadonnées

- Microsoft
- Scrubber

Outils de conversion PDF

- CutePDF
- PrimoPDF

Avis juridiques de divers barreaux concernant les métadonnées

- Metadata Ethics Opinions Around the U.S.
- Le déontologie du droit à l'ère numérique (Comité de déontologie et de responsabilité professionnelle de l'Association du Barreau canadien)

Histoires d'horreurs relatives aux métadonnées

- Metadatarisk.org : Content Security in the news
- Shauna Kelly : How tracked changes have made businesses and government look foolish

Surveillance et gestion du parc informatique /gestion des alertes

Principe

Tout système informatique doit faire l'objet d'une surveillance afin d'identifier, de diagnostiquer et de résoudre les difficultés techniques avant que celles-ci ne mettent en péril la sécurité des données ou du système lui-même.

Définition

Une surveillance se fait notamment par la mise en place, le paramétrage et le suivi d'alertes. Ces alertes générées par votre système permettent d'être avertis et de réagir lorsqu'un risque potentiel ou réel se présente.

Utilité

Les logiciels ou les services de télésurveillance analysent, selon des paramètres donnés, les réponses des systèmes et équipements sondés. Ces systèmes peuvent être, par exemple, le serveur sur lequel est déposé le site Web, l'accès à Internet, les copies de sauvegarde, etc. Ces réponses sont comparées à des normes.

Lorsque les réponses des systèmes sont hors normes, des alertes sont générées.

Ces alertes peuvent prendre différentes formes :

- Message dans le bas de l'écran ou à l'ouverture des logiciels;
- Courriels d'alerte;
- Mise en garde;
- Etc.

Même si une situation est hors norme et qu'une alerte est générée, cela ne signifie pas automatiquement que l'équipement ou le service est défectueux. C'est ce que nous appelons des « faux positifs ».

Une gestion des alertes est donc nécessaire pour distinguer les faux positifs, c'est-à-dire les alertes mineures à garder en observation (p. ex., une alerte mentionnant qu'une prise de sauvegarde n'est pas complétée alors que seulement deux fichiers n'ont pas été copiés) et les alertes majeures (p. ex., manque imminent d'espace disque pouvant rendre le serveur principal inopérant).

Risques

Ignorer les alertes peut poser des risques importants. Il peut être tentant de désactiver les alertes, mais il faut éviter de le faire à moins que ce soit un faux positif confirmé.

Voici les éléments de l'environnement informatique devant être surveillés (notamment en cas de panne) :

1. Serveur principal
2. Routeur, pare-feu ou accès à Internet

3. Prise de sauvegarde
4. Antivirus

Éthique et déontologie

Il est nécessaire pour l'avocat de se conformer aux pratiques proposées afin de s'assurer de la sécurité des dossiers de ses clients et de protéger leur intégrité.

Lexique

Antipourriel

Logiciel qui, selon des règles de filtrage prédéfinies, analyse le contenu des courriels reçus, détecte les pourriels et les déplace automatiquement dans un dossier spécifique ou les supprime sur le serveur de messagerie avant réception.

Antivirus

Logiciel de sécurité qui procède, automatiquement ou sur demande, à l'analyse des fichiers et de la mémoire d'un ordinateur, soit pour empêcher toute introduction parasite, soit pour détecter et éradiquer tout virus dans un système informatique.

Archivage

Stockage de données qui doivent être conservées dans le but de pouvoir être utilisées ultérieurement.

Bêta

Version non encore commercialisée d'un logiciel, pouvant contenir quelques bogues, qui est distribuée à certains utilisateurs afin d'être testée et évaluée. La version bêta d'un logiciel est distribuée en avant-première à certains utilisateurs potentiels afin d'évaluer les fonctions du produit, de rechercher les erreurs de programmation, etc.

Bluetooth

Le réseau Bluetooth permet d'interconnecter, en utilisant une technique radio courte distance, des ordinateurs, imprimantes, numériseurs, téléphones portables, claviers, souris, assistants numériques personnels, écouteurs, micros mains libres, etc., le tout sans fil.

BYOD (Bring your own device)

Locution désignant le mode de travail selon lequel un employeur permet à son employé ou exige de lui qu'il utilise son matériel électronique personnel dans le cadre de son travail.

Commutateur

Équipement réseau permettant l'interconnexion d'équipements informatiques en réseau local.

Chiffrement / cryptographie

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre incompréhensibles sans une action spécifique. Elle permet également d'authentifier les messages (p. ex., signature numérique). Le verbe crypter est parfois utilisé, mais on lui préférera le verbe chiffrer.

Fichier

Un fichier est un lot d'informations portant un nom et conservé dans une mémoire, généralement dans une mémoire de masse, tel un disque dur.

Gestion des accès

La gestion des accès consiste à vérifier si une entité (p. ex., une personne ou un ordinateur) qui demande l'accès à une ressource a l'autorisation nécessaire pour le faire.

Infonuagique

Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services évolutifs, adaptables dynamiquement et facturés à l'utilisation.

Logiciel malveillant

Un logiciel malveillant (en anglais, *malware*) est développé dans le but de nuire à un système informatique. Les logiciels malveillants les plus connus s'appellent virus et vers, mais il en existe beaucoup d'autres.

Modem

Contraction des mots « modulateur » et « démodulateur ». Le modem sert à convertir les données numériques de l'ordinateur en signal modulé, dit « analogique », transmissible par une ligne de téléphone classique et réciproquement.

Pare-feu

Élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de sécuriser le réseau en permettant ou en interdisant l'accès à certains sites Web ou à certaines fonctions.
Le pare-feu, aussi nommé coupe-feu ou *firewall* en anglais, est un élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de contrôler, selon des règles de sécurité établies, les communications entre différentes zones de confiance (p. ex., Internet est une zone de confiance faible, et le réseau local d'entreprise est une zone de confiance élevée).

Politique de sécurité informatique

Une politique de sécurité informatique est un document qui établit des règles pour les accès au réseau informatique et pour les flux autorisés ou non, qui détermine ce qu'il est interdit de faire (p. ex., consulter des sites pornographiques, utiliser les imprimantes du cabinet à des fins personnelles), qui prévoit l'application de la politique et qui présente une partie de l'architecture de base de l'environnement de sécurité du réseau.

Répertoire (sous-répertoire)

Une table qui donne le nom, le lieu, la taille et la date de création et de révision de chaque fichier contenu dans une mémoire de masse.

Réseau informatique

Le réseau informatique est formé d'ordinateurs et de périphériques, comme des imprimantes, des numériseurs, des serveurs, des commutateurs, des routeurs et des modems, reliés au moyen de matériel – avec ou sans fil – et de logiciels informatiques.

Réseautique

La réseautique vise l'ensemble des techniques relatives à la création, au maintien et à l'utilisation d'un réseau informatique.

Routeur

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage ou la redirection des données. Sa fonction est de faire transiter des données d'une interface réseau (p. ex., le réseau interne de l'entreprise) vers une autre (p. ex., Internet).

Sauvegarde

Transfert sur un support distinct d'informations en mémoire en vue de les protéger ou de les mettre en sécurité.

Session (active/inactive)

Une session active est le moment pendant lequel un appareil informatique est en communication et réalise des opérations au service d'un utilisateur, d'un logiciel ou d'un autre appareil. Par opposition, l'appareil peut se mettre en état de veille (session inactive) suite à une période d'inactivité déterminée par l'utilisateur.

Support amovible

Média que l'on peut facilement transporter (p. ex., clé USB, disque dur externe, iPod, etc.).

Système d'exploitation

Le système d'exploitation, abrégé SE (en anglais, *operating system*, abrégé OS), est l'ensemble des programmes centraux d'un appareil informatique qui sert d'interface entre le matériel et les logiciels applicatifs (p. ex., Windows, Linux et iOSX sont des systèmes d'exploitation).

Serveur

Ordinateur dont le rôle est de répondre à des demandes transmises par des utilisateurs connectés en réseau sur ce serveur et permettant un partage de ressources informatiques.

Téléphone intelligent/smartphone

Un téléphone intelligent ou un smartphone est un téléphone mobile disposant aussi des fonctions d'un assistant numérique personnel. Il peut aussi fournir les fonctionnalités d'agenda, de calendrier, de navigation Web, de consultation, de courrier électronique, de messagerie instantanée, etc. Les plus connus utilisent les plateformes suivantes : iOS, Android et BlackBerry.

De nombreuses définitions de ce lexique sont tirées du grand dictionnaire terminologique, disponible sur le site Web de l'Office québécois de la langue française : www.granddictionnaire.com/

Réalisation et mise à jour du *Guide des TI*

Dernière mise à jour : janvier 2016

La mise à jour du *Guide des TI* a été rendue possible grâce à la collaboration des membres du Comité sur la sécurité des technologies de l'information :

- Me Jean L. Beauchamp
- Me Jean-François De Rico
- Me Maxime Fournier
- Me Annick Gariépy
- Me Patrick Gingras
- Me Dominic Jaar, Ad. E. président du Comité
- Me Geneviève Lefebvre
- Me Éric Lestage
- Me Jean-Michel Montbriand
- Me Dyane Perreault
- Me François Senécal
- Me Michel A. Solis
- Me Benoît Trotier
- Me Nicolas Vermeys
- M. Patrick Vicente

Annexe

Liste de contrôle en matière d'infonuagique

Comme avocat, vous devez prendre les moyens raisonnables pour vous assurer que les renseignements confidentiels qui transitent ou sont hébergés dans le nuage ne puissent être consultés ou interceptés par un tiers non autorisé. Ce document se veut un outil complémentaire au *Guide des TI* afin d'aider les avocats souhaitant intégrer l'infonuagique à leur pratique à le faire de façon sécuritaire.

Avant de faire le saut vers un hébergement de données ou l'utilisation d'applications utilisant l'infonuagique, quelques précisions importantes s'imposent :

1. Si les données que vous comptez transférer dans un nuage sont de **nature sensible**, vos exigences en matière de sécurité devraient être plus élevées et les garanties de votre fournisseur plus grandes (par exemple, si vos dossiers sont des dossiers en lien avec la propriété intellectuelle, d'intérêt national ou international, etc.).
2. Assurez-vous que votre **assurance responsabilité civile** est adéquate, c'est-à-dire qu'elle couvre vos dommages et les dommages de vos clients qui découlent de l'utilisation de l'infonuagique.
3. Assurez-vous que les applications (par exemple, un logiciel de gestion ou de comptabilité) qui se retrouvent sur le nuage **s'intègrent bien** dans les autres systèmes de votre bureau.
4. Remplissez la **liste de contrôle** (p. 2 et suivantes) avec le fournisseur envisagé et conservez l'information pour référence ultérieure. Dans le cadre des négociations avec votre fournisseur d'infonuagique, soyez aussi rigoureux que vous l'êtes pour vos clients.

Une fois dans le nuage, assurez-vous de bien intégrer l'infonuagique à vos pratiques de gestion :

1. Obtenez toujours **l'autorisation écrite** de vos clients (par exemple, à l'intérieur de votre mandat) avant de stocker leurs informations dans le nuage et voyez si des lois particulières ou des obligations contractuelles exigent que des précautions additionnelles soient prises ou vous empêchent de les transférer dans un nuage.
2. Mettez en place des **politiques d'utilisation** de l'infonuagique pour les utilisateurs du cabinet et formez les utilisateurs afin qu'ils puissent gérer vos données dans le nuage.
3. Pour plus de sécurité, **cryptez vos données** avant de les verser sur le nuage et bénéficiez d'un niveau supérieur de protection en plus du chiffrement effectué par votre fournisseur.
4. Informez l'avocat qui a accepté d'être **cessionnaire**, selon l'article 78 du *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats,* des **modalités** pour accéder à vos données ou applications sur le nuage.

Grille d'évaluation d'un fournisseur

Même si l'infonuagique comporte de nombreux avantages, ce type d'outil est tout de même récent. Comme c'est le cas pour bien des nouveaux produits et services, les fournisseurs tendent à imposer des conditions limitant leur risque et responsabilité. Vous pourriez avoir à insister auprès d'un fournisseur pour obtenir des conditions plus favorables que celles initialement offertes. Si cela peut

être ardu, cela demeure toutefois possible pour certaines clauses. Avant de signer un contrat avec un fournisseur, vous devriez vous assurer que celui-ci est en mesure de fournir certaines garanties vous permettant de respecter vos obligations déontologiques ainsi que de vous protéger en cas de perte de données, de violation ou de résiliation de contrat. Si le fournisseur ne peut répondre à ces exigences, vous aurez tout de même une meilleure idée des risques qui se posent et des moyens à prendre pour les atténuer. Par exemple, en prenant conscience de la responsabilité limitée du fournisseur, vous pourriez avoir à sauvegarder une copie sur votre serveur local, choisir de ne pas transférer certains dossiers sensibles sur le nuage ou prendre des mesures supplémentaires (p. ex. le chiffrement) pour assurer la sécurité des données confidentielles de vos clients.

Autres conseils

- Informez-vous de la feuille de route du fournisseur en ce qui a trait à la santé financière et au plan d'évolution de la compagnie.
- Informez-vous des coûts internes totaux (matériel, logiciels et coûts des accessoires) associés à votre passage à ce service infonuagique et analysez l'incidence de ce changement sur vos frais administratifs et frais de bande passante.
- Renseignez-vous sur les frais initiaux et les frais mensuels exigés par le fournisseur ainsi que sur la fréquence et le plafond des augmentations que le fournisseur peut exiger pour la durée du contrat.
- Informez-vous des limites de l'assurance responsabilité du fournisseur.

SÉCURITÉ DES DONNÉES
1. Le fournisseur est une compagnie canadienne détenue par des intérêts canadiens.
2. Les données demeureront au Canada en tout temps, y compris les copies de sauvegarde.
3. Le fournisseur informera l'avocat s'il sous-traite à d'autres fournisseurs l'hébergement ou la sauvegarde de données (nuage de nuages). Ceux-ci seront tenus aux mêmes obligations que le fournisseur principal et, en tout temps, ce dernier demeurera responsable de ses sous-traitants.
4. Les données seront chiffrées, tant lors de la transmission qu'au lieu de stockage.
5. Le fournisseur notifiera l'avocat sans délai lors de toute faille de sécurité.
6. Le fournisseur produit régulièrement des rapports de vérification menés par des experts indépendants et réputés (p. ex., certification SOC2) et les communique sans délai à l'avocat.
ACCÈS/PROPRIÉTÉ DES DONNÉES
7. L'avocat et ses clients demeurent les seuls propriétaires des données stockées dans le nuage.
8. L'avocat sera en mesure d'accéder à ses données en tout temps, 24 h sur 24, 7 jours sur 7 (le standard dans l'industrie étant d'environ 10 h en maintenance/panne par an).
9. Le fournisseur est doté d'un système d'authentification et de contrôle d'accès approprié et il dispose d'un registre d'accès aux informations stockées dans le nuage.

10. L'accès du fournisseur aux données est limité et l'utilisation qu'il peut en faire est restreinte. De plus, le fournisseur s'engage à préserver la confidentialité des informations qui lui sont confiées par l'avocat.
11. Le fournisseur avisera l'avocat de toute demande d'accès par un tiers à l'information stockée, et l'avocat disposera d'un délai raisonnable pour réagir.
12. Le fournisseur ne peut empêcher l'avocat d'accéder à ses données en cas de non-paiement des frais ou pour toute autre raison.
13. En cas de perte de données ou de fin des activités, le fournisseur donnera à l'avocat un accès facile et rapide aux données, et ce dernier sera capable d'importer celles-ci dans un format qu'il lui sera possible de lire et d'exploiter.
14. Le fournisseur indemnisera l'avocat en cas de perte de données résultant de l'utilisation de son service. Le fournisseur dispose d'une assurance responsabilité adéquate et accepte de fournir à l'avocat une copie de la police d'assurance.
15. Le fournisseur accordera à l'avocat le soutien nécessaire pour collaborer aux inspections et enquêtes du Barreau du Québec, notamment pour lui permettre d'accéder à tout dossier exigé par son ordre professionnel.
CONTRAT, MODIFICATION ET RÉSILIATION
16. L'avocat peut mettre fin au contrat en tout temps.
17. Aucune modification aux conditions ne sera effectuée pour la durée du contrat, sans qu'un avis écrit ne soit transmis à l'avocat avant ces modifications. Cet avis sera transmis dans un délai raisonnable, permettant ainsi à l'avocat de refuser cette modification ou de résilier le contrat, sans frais de pénalité ou indemnité.
18. Les données de l'avocat demeureront disponibles lorsque le service prendra fin, et le fournisseur garantit qu'il offrira un soutien de transition pour permettre à l'avocat de récupérer ses données. Dans un délai raisonnable suite à la fin du contrat, les données de l'avocat seront détruites et le fournisseur en produira une attestation.
19. En cas de cessation des activités, le fournisseur donnera accès à l'avocat à son code source (par contrat d'entiercement ou autre) afin de permettre le transfert des données vers un autre fournisseur.
20. En cas de conflit, la médiation ou l'arbitrage seront privilégiés pour le résoudre. Le contrat est régi et interprété selon les lois en vigueur dans la province de Québec, et les tribunaux du Québec sont les seuls tribunaux à avoir juridiction en cas de différend.

VOUS NE PASSEZ PAS LE TEST ?
PAS DE PANIQUE !

Le Barreau du Québec veut vous aider à mettre en place des pratiques sécuritaires en ce qui a trait aux TI.

Que faire si vous avez répondu *NON* ou *Ne sais pas* à certaines questions ? Agissez immédiatement !

1. Lisez sans tarder les sections pertinentes du ***Guide des TI*** mis à votre disposition au **guideTI.barreau.qc.ca**

2. Au besoin, consultez les ressources complémentaires fournies à chacune des sections du Guide.

3. Mettez en place les mesures facilement réalisables.

4. Consultez des professionnels pour mettre en place les mesures plus complexes. Un des objectifs du Guide est de faciliter l'élaboration de la liste de modifications à être effectuées par un technicien en informatique, ainsi que les coûts approximatifs à prévoir.

guideTI.barreau.qc.ca

Maison du Barreau

445, boulevard Saint-Laurent
Montréal (Québec) H2Y 3T8

T 514 954-3411
Sans frais 1 844 954-3411

infobarreau@barreau.qc.ca
www.barreau.qc.ca

Barreau du Québec