



# PRÆVENTIO

© « Les années folles », Claude Théberge

Décembre 2019 | Volume 20 | n° 6

## SOMMAIRE

Le site Internet du Fonds d'assurance fait peau neuve	1
Noël est à nos portes, mais l'heure est à la prévention	1
Nos formations – La tournée se poursuit!	2
La cybercriminalité : L'affaire de tous!	2
Parce qu'on a parfois besoin d'aide!	4

## *Nos Meilleurs Vœux pour l'année 2020*

*La période des fêtes est un bon moment pour prendre une pause bien méritée et refaire le plein d'énergie. Nous en profitons pour renouer avec notre famille et nos amis. Afin de maximiser ce temps précieux, fermons nos ordinateurs et nos téléphones intelligents et profitons de cette occasion unique pour passer de bons moments avec ceux et celles qui nous sont chers.*

*L'équipe du Fonds d'assurance souhaite à tous ses assurés et partenaires tout ce qu'il y a de meilleur. Que l'année 2020 apporte bonheur, prospérité, santé et satisfaction professionnelle et que la vigilance soit au rendez-vous!*

## LE SITE INTERNET DU FONDS D'ASSURANCE FAIT PEAU NEUVE

Le site Internet du Fonds d'assurance a subi une cure de rajeunissement et le nouveau site sera prochainement mis en ligne. Sa conception et son apparence ont été enrichies afin d'en faciliter l'utilisation et son contenu a été mis à jour. De nouvelles ressources en prévention y seront également disponibles, dont les péripéties de Marika et des capsules vidéos en gestion des risques.

**Restez à l'affût, c'est pour bientôt!** ☂

## NOËL EST À NOS PORTES, MAIS L'HEURE EST À LA PRÉVENTION

Noël arrive à grands pas avec quelques jours à peine... Plusieurs d'entre nous prendront un repos bien mérité. Certains en profiteront pour passer quelques jours à la campagne ou pratiquer leur sport d'hiver préféré. Légitimement, on se dit, après tout, c'est la période des fêtes et il est normal que le bureau soit fermé!

Toutefois, des dispositions doivent être prises pendant cette période afin d'éviter que nos clients n'en subissent un préjudice.

L'article 6 du *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, RLRQ, c. B-1, r. 5, impose ce qui suit :

*« 6. L'avocat qui s'absente de son domicile professionnel pendant les heures normales d'affaires doit, selon la durée de cette absence, prendre des dispositions pour que toute procédure puisse lui être signifiée et prévoir un mécanisme pour traiter ses appels, ses messages, son courrier, ses courriers électroniques et les urgences. »*

Cet article impose à l'avocat de maintenir son télécopieur en état de recevoir des messages pendant les heures normales de bureau,

puisque des procédures peuvent lui être signifiées ou notifiées par ce moyen de communication. Sans oublier que les urgences, la correspondance, les appels téléphoniques et les courriers électroniques doivent être traités sans délai.

Cette période est sujette aux erreurs chaque année. Prenons les mesures nécessaires pour s'assurer que nous et nos clients passions une bonne et heureuse nouvelle année.

**Une once de prévention pour cette période des fêtes vaut bien un livre de guérison!** ☂

## NOS FORMATIONS – LA TOURNÉE SE POURSUIT!

Le Fonds d'assurance poursuit sa tournée de formations. Ces formations constituent un excellent moyen de compléter les trois (3) heures de formation obligatoire en éthique et déontologie ou en pratique professionnelle. Voici notre calendrier hiver-printemps 2020 :

### COMMUNICATIONS ENTRE L'AVOCAT ET SON CLIENT : Y A-T-IL QUELQU'UN QUI ÉCOUTE?

Date	Lieu	Heure	Durée reconnue
24 janvier 2020	Montréal (Holiday Inn Montréal Centre-Ville)	9h – 11h	2 h
20 mars 2020	Sherbrooke (salle à déterminer)	9h – 11h	2 h
26 mars 2020	Trois-Rivières (salle à déterminer)	9h – 11h	2 h
17 avril 2020 (pm)	Saint-Jérôme (salle à déterminer)	13h30 – 15h30	2 h
23 avril 2020	Laval (salle à déterminer)	9h – 11h	2 h
30 avril 2020	Longueuil (salle à déterminer)	9h – 11h	2 h

### LE DÉFI DE L'AVOCAT FACE AUX PERSONNALITÉS DIFFICILES

Date	Lieu	Heure	Durée reconnue
6 février 2020	Gatineau (Sheraton Four Points)	9h – 12h	3 h
20 février 2020	Bromont (salle à déterminer)	9h – 12h	3 h
20 mars 2020	Valleyfield (salle à déterminer)	9h – 12h	3 h
26 mars 2020	Québec (Hôtel Château Laurier)	9h – 12h	3 h

### NON-RESPECT DES DÉLAIS : SURVIE PRATIQUE POUR LIMITER LES RISQUES!

Date	Lieu	Heure	Durée reconnue
17 avril 2020 (am)	Saint-Jérôme (salle à déterminer)	9h – 12h	3 h
14 mai 2020	Valleyfield (salle à déterminer)	9h – 12h	3 h

Pour vous inscrire à la formation en salle, rendez-vous sur le site Web du Barreau du Québec à [www.barreau.qc.ca](http://www.barreau.qc.ca) à Formation continue / Les formations du Barreau / Accédez au catalogue complet / et choisissez la formation désirée, la date et le lieu appropriés.

Vous désirez suivre nos formations dans le confort de votre bureau ou de la maison? Aucun problème! Trois formations du Fonds d'assurance sont désormais en ligne et disponibles sur Web-Pro. Rendez-vous à <https://webpro.barreau.qc.ca/formations-farpbq.html>.

Pour toute question, vous pouvez contacter M<sup>e</sup> Guylaine LeBrun ou M<sup>e</sup> Judith Guérin au 514 954-3452.

**Réservez du temps à votre agenda et venez bénéficier de ces formations afin de satisfaire vos obligations de formation continue!** ☂

## LA CYBERCRIMINALITÉ : L'AFFAIRE DE TOUS!

Récemment, les médias ont révélé au grand jour des cas d'entreprises ayant été victimes de cybercriminalité mettant ainsi en lumière les failles qui peuvent exister en matière de protection des données personnelles. Ces cas nous enseignent également que le cybercrime n'est pas qu'une affaire de pirates informatiques n'ayant aucun lien avec l'entreprise « victime », mais qu'au contraire, la menace peut parfois venir de l'intérieur.

Les avocats ne sont pas en reste! Ils demeurent des cibles de choix pour les cybercriminels pour les raisons suivantes :

- Ils possèdent des informations confidentielles de grande valeur;

- Ils détiennent un compte en fidéicomis où y sont déposées d'importantes sommes d'argent;
- Leurs systèmes de sécurité pourraient comporter des faiblesses pouvant être exploitées.

Au Canada, la cybercriminalité entraînerait des pertes économiques de plus de 3 milliards de dollars et la cybermenace ne cesse de croître. L'ordinateur, l'Internet, les courriels et les téléphones intelligents font partie des outils de travail quotidien de tout avocat. Dans de telles circonstances, comment faire pour diminuer les risques d'être victime de cybercriminalité? Voici quelques suggestions :

- ☑ Évaluez le niveau de cybermenace auquel vous êtes exposé;
- ☑ Établissez un budget pour investir dans la cybersécurité;
- ☑ Élaborez un plan d'intervention en cas d'incidents de cybersécurité et nommez une personne responsable de l'application de ce plan. Une version papier de ce plan devrait être conservée si l'accès à la version numérique s'avérait impossible;
- ☑ Effectuez les mises à jour des programmes installés sur votre ordinateur. Veuillez noter que Windows et Apple possèdent un système de notification des mises à jour qui pourront par la suite être facilement téléchargées. Toutefois, la prise en charge de Windows 7 prendra fin le 14 janvier 2020 faisant en sorte que ce logiciel sera plus vulnérable au piratage ou aux logiciels malveillants;
- ☑ Activez ou installez des logiciels antivirus ou anti-maliciels sur vos ordinateurs;
- ☑ Installez un logiciel coupe-feu (qui surveille le flux de trafic) afin de protéger votre réseau interne contre les intrusions;
- ☑ Changez les configurations par défaut qui sont installées sur votre ordinateur, notamment quant aux paramètres de sécurité. Ajoutez toutes les fonctions de sécurité pertinentes;
- ☑ Sauvegardez vos données sur un serveur externe et chiffrez (cryptez) les informations confidentielles et plus sensibles;
- ☑ Mettez en place un système d'authentification fort. À cet égard, il pourrait s'avérer souhaitable de se doter d'une politique de bureau sur la longueur du mot de passe, l'utilisation d'un gestionnaire de mots de passe et la façon de conserver ces derniers;
- ☑ Sensibilisez et offrez de la formation aux employés, notamment sur l'utilisation efficace des mots de passe, la détection de courriels malveillants, l'utilisation adéquate d'Internet et des médias sociaux ainsi que l'utilisation de logiciels sécurisés et approuvés;
- ☑ Portez une attention sur l'usage du cellulaire et mettez en place une politique à cet effet, notamment quant aux applications téléchargées et aux adresses courriel personnelles qui peuvent être l'objet de virus ou de cybercrime. Ceci dit, le cellulaire devrait comporter minimalement un mot de passe pour être déverrouillé;
- ☑ Utilisez une connexion à des réseaux privés plutôt qu'à des réseaux Wi-Fi publics (bibliothèque, café internet, aéroport, hôtel, etc.) autant pour les ordinateurs que pour les téléphones cellulaires. Lorsqu'il n'est pas possible d'utiliser un réseau privé, l'usage du Bluetooth ou autres protocoles de communication en champs proche devrait être limité;
- ☑ Dans le cas du télétravail, assurez-vous que l'accès au réseau soit sécurisé. Cela peut notamment se faire avec une clé VPN (réseau privé virtuel);
- ☑ Lorsque vous utilisez les services infonuagiques par le biais d'un fournisseur externe, assurez-vous qu'il peut protéger les données et leur confidentialité et vérifiez à quel endroit les données sont entreposées. En fait, toute information confidentielle emmagasinée à l'extérieur du bureau devrait être chiffrée;
- ☑ Mettez en œuvre des contrôles d'accès et des autorisations. Cela implique de donner accès uniquement aux fonctionnalités dont les employés ont besoin pour effectuer leurs tâches. Ainsi, les comptes partagés devraient être limités. Il en va de même des comptes administrateur qui devraient être restreints. Les comptes individuels des employés qui ne sont plus à l'emploi du cabinet doivent être annulés;
- ☑ Ayez des supports amovibles (clés USB) sécurisés;
- ☑ Protégez vos appareils mobiles et ne les laissez pas sans surveillance (exemple : dans une voiture);
- ☑ Souscrivez à une police d'assurance couvrant les cyberrisques;

Bien qu'il soit impossible de prédire à l'avance si vous serez victime de cybercriminalité, les suggestions précédentes devraient à tout le moins limiter les risques

d'être la prochaine victime! Par ailleurs, il va de soi que ces suggestions doivent être adaptées à votre pratique. Vous désirez en savoir plus sur les contrôles de cybersécurité qui pourraient être mis en place par votre cabinet? Voici certaines suggestions de documentation pertinente dont nous nous sommes inspirés pour cet article :

- **Guide afin d'y voir plus clair** : Il s'agit d'un guide préparé par la *Fondation du Barreau* sur la gestion des documents technologiques.  
[https://www.fondationdubarreau.qc.ca/wp-content/uploads/2016/10/Guidetech\\_allège\\_FR.pdf](https://www.fondationdubarreau.qc.ca/wp-content/uploads/2016/10/Guidetech_allège_FR.pdf)
- **Guide des TI** : Il s'agit d'un document préparé par le *Barreau du Québec* pour évaluer votre utilisation des technologies de l'information.  
<http://guideti.barreau.qc.ca/>
- **Contrôles de cybersécurité de base pour les petites et moyennes organisations V1.1** : Le centre canadien pour la cybersécurité a mis un guide à la disposition des petites et moyennes entreprises qui veulent améliorer leur résilience en matière de cybersécurité.  
<https://cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations>
- **Protecting yourself from cybercrime dangers: The steps you need to take**: *Lawpro* a publié cet article destiné aux avocats afin de limiter les risques d'être victime de cybercriminalité.  
<https://www.practicepro.ca/2013/12/protecting-yourself-from-cybercrime-dangers-the-steps-you-need-to-take/>

En terminant, le gouvernement a récemment lancé CyberSécuritaire Canada, un programme de certification en cybersécurité. Ce programme est administré par Innovation, Sciences et Développement économique Canada et vise spécifiquement les petites et moyennes entreprises bien que toute organisation puisse formuler une demande de certification. Le programme en est présentement à sa phase pilote, mais peut-être voudrez-vous obtenir cette certification ou la suggérer à un client afin de créer pour votre cabinet ou l'entreprise de celui-ci une image distinctive par rapport aux concurrents. Vous pouvez retrouver toute l'information pertinente à cette adresse : <https://www.ic.gc.ca/eic/site/137.nsf/fra/accueil>. ☂

## PARCE QU'ON A PARFOIS BESOIN D'AIDE!

Le *Programme d'aide aux membres du Barreau du Québec (PAMBA)* est un service d'aide et de consultation offert à tous les membres du Barreau du Québec souffrant de stress, du syndrome d'épuisement professionnel (burn-out), de problèmes de santé mentale, d'alcoolisme et de toxicomanie.

Une poursuite en responsabilité professionnelle peut être source de remises en question et entraîner des répercussions autant dans la vie professionnelle que personnelle. Aussi, le Fonds d'assurance responsabilité professionnelle du Barreau du Québec offre aux assurés qui feront appel à PAMBA à la suite d'une réclamation assurée, en sus des heures d'entrevue sans frais assumées par le PAMBA, **trois (3) heures additionnelles de consultation** auprès d'un professionnel de la santé.

Vous désirez bénéficier de ces heures additionnelles? Vous n'avez qu'à autoriser le gestionnaire de PAMBA à communiquer directement avec le Fonds d'assurance pour demander l'autorisation de prolonger les paramètres actuels de la consultation. Pour ce faire, veuillez communiquer avec :

**PAMBA**    [aide@pamba.info](mailto:aide@pamba.info)  
Montréal : 514 286-0831  
Extérieur : 1 800 747-2622

Nous vous invitons également à consulter le site Internet du Barreau à l'adresse suivante : <https://www.barreau.qc.ca/fr/ressources-avocats/services-avocats-outils-pratique/pamba/> ☂

## Service de prévention

AVIS

M<sup>e</sup> Guylaine LeBrun  
Avocate et Coordonnateur  
aux activités de prévention

Fonds d'assurance responsabilité professionnelle du Barreau du Québec

445, boulevard Saint-Laurent, bureau 300

Montréal (Québec) H2Y 3T8

Téléphone : 514 954-3452

Télécopieur : 514 954-3454

Courriel : [guylaine.lebrun@farpbq.ca](mailto:guylaine.lebrun@farpbq.ca)

Courriel : [judith.guerin@farpbq.ca](mailto:judith.guerin@farpbq.ca)

Visitez notre site Internet : [www.farpbq.ca](http://www.farpbq.ca)

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

Tous les bulletins Praeventio antérieurs sont disponibles à l'adresse suivante : [www.farpbq.ca/fr/bulletin.html](http://www.farpbq.ca/fr/bulletin.html)

M<sup>e</sup> Judith Guérin  
Avocate analyste et aux  
activités de prévention

Assurance  
responsabilité  
professionnelle

Barreau 

Cette publication est un outil d'information dont certaines indications visent à réduire les risques de poursuite, même mal fondée, en responsabilité professionnelle. Son contenu ne saurait être interprété comme étant une étude exhaustive des sujets qui y sont traités, ni comme un avis juridique et encore moins comme suggérant des standards de conduite professionnelle. Le masculin désigne, lorsque le contexte s'y prête, aussi bien les femmes que les hommes.

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