COMJUR CCBF

Bulletin Juridique
Spécial Covid-19
Mai 2020 – Article n° 19

Garder secrets les secrets professionnels – Des mesures raisonnables à une époque irrationnelle

Quand il s'agit de protéger des informations de secret professionnel, le propriétaire doit user d'efforts « raisonnables » pour les maintenir en secret.

Les secrets professionnels font partie des actifs les plus précieux d'une entreprise. Cependant, la présence de haut-parleurs intelligents dans les espaces de travail domestiques, l'utilisation de services non sécurisés pour le transfert d'archives, les boîtes mail personnelles, entre autres, amoindrissent les efforts faits par les entreprises pour protéger le secret de leurs informations confidentielles et peuvent représenter de possibles violations de confidentialité ou de secret professionnel.

Cette alerte passe en revue les principaux risques pour les entreprises forcées à pratiquer le télétravail pendant la crise provoquée par le COVID-19 et fournit des recommandations grâce auxquelles elles peuvent renforcer la protection de leurs secrets professionnels.

Les mesures que les entreprises peuvent adopter pour protéger leurs secrets professionnels pendant la crise du COVID-19

Quand il s'agit de protéger des informations de secret professionnel, le propriétaire doit user d'efforts « raisonnables » pour les maintenir en secret. Ce critère souple apporte une flexibilité, de façon que ce qui est "raisonnable" dépend de la nature et de la quantité des secrets professionnels et encore davantage de la nature de l'affaire.

Pour protéger leurs secrets professionnels pendant la pandémie, **l**e premier pas pour les entreprises est d'établir une politique de télétravail qui prenne en compte les risques et défis provoqués par cette crise, en employant les protocoles suivants :

1. **Distribuer, Rappeler, Répéter**

   Distribuer régulièrement des rappels et des bulletins de confidentialité incitant les destinataires à la vigilance pendant le télétravail. Inclure dans ces rappels et bulletins, les informations de contact d'une (ou plusieurs) personne(s) désignée(s) qui répondra constamment aux questions et aux inquiétudes de ceux qui travaillent à la maison sur des secrets professionnels de l'entreprise et autres informations confidentielles

2. **Limiter ou interdire l'utilisation de dispositifs**

   Insister sur les interdictions et/ou limitations de l'utilisation de dispositifs personnels par les employés pour conduire les affaires de l'entreprise. Même si des employés ont accès et sauvegardent provisoirement ces informations dans des dispositifs personnels et les excluent après leur retour à l'entreprise, les backups de ces informations pourront rester indéfiniment dans des archives de données personnelles ou des unités de backup externes.

Garder secrets les secrets professionnels – Des mesures raisonnables à une époque irrationnelle

Quand il s'agit de protéger des informations de secret professionnel, le propriétaire doit user d'efforts « raisonnables » pour les maintenir en secret.

3. Maintenir des lieux de travail sécurisés

Recommander que les employés maintiennent isolés leur lieu de travail. Par ailleurs, demander au secteur de TI de l'entreprise d'habiliter le blocage automatique d'écran sur tous les dispositifs de l'entreprise après de courtes périodes d'inactivité. Enfin, dire aux employés de retirer ou déconnecter des appels confidentiels les haut-parleurs intelligents localisés près des mains ; et de répondre aux appels dans un espace séparé des lieux communs de leur maison.

4. Restreindre le transport et l'impression de documents

Restreindre la possibilité pour les employés d'imprimer des documents ou désactiver complètement la possibilité d'impression. Dire aux employés de ranger les copies imprimées de documents confidentiels dans un lieu sûr jusqu'à ce qu'elles puissent être rendues à l'entreprise. De la même façon, exiger que les copies des documents destinées à être jetées soient rangées dans une armoire ou un tiroir fermé à clé jusqu'à ce qu'elles soient détruites au moment de la réouverture de l'entreprise.

Pour les documents retirés de l'entreprise, instaurer un registre d'entrées et sorties pour les documents à rendre, et s'assurer qu'ils soient réellement rendus au moment de la réouverture de l'entreprise. De la même façon, instaurer un système de notification pour alerter le secteur de TI à chaque fois que quelqu'un télécharge, copie, imprime, transfère ou exclut des données confidentielles ou des documents importants liés à un secret professionnel.

5. Réseaux et dispositifs sécurisés

Dire aux employés d'ajouter une protection par mot de passe à leurs réseaux Wi-Fi personnels. Pour une protection supplémentaire, exiger que les dispositifs de l'entreprise soient toujours connectés au Réseau Virtuel Privé (VPN) de l'entreprise et instaurer l'authentification de deux facteurs. Par ailleurs, demander au TI de désactiver USB et autres entrées externes sur les ordinateurs portables de l'entreprise pour empêcher l'envoi non autorisé de secrets professionnels et autres informations confidentielles.

6. Limiter la transmission de documents et inclure des protections

Idéalement, les entreprises interdiraient la transmission de secrets professionnels ou autres informations ou documents confidentiels par e-mail ou autres moyens de transfert d'archives en dehors de leurs locaux. Toutefois, cette interdiction n'est sans doute pas réaliste dans les circonstances actuelles.

Garder secrets les secrets professionnels – Des mesures raisonnables à une époque irrationnelle

Quand il s'agit de protéger des informations de secret professionnel, le propriétaire doit user d'efforts « raisonnables » pour les maintenir en secret.

En effet, implanter des protections supplémentaires, (i) exigeant qu'un destinataire d'email ait une adresse IP spécifique ou une signature numérique exclusive pour réviser des messages et (ii) permettant l'accès au secret commercial ou à d'autres informations confidentielles qu'à travers des documents de collaboration archivés dans des unités de réseau interne sécurisées, empêchera qu'emails et pièces jointes ne soient envoyés au mauvais destinataire et que les secrets professionnels qu'ils contiennent soient compromis.

7. **Restreindre l'installation de logiciels non essentiels et de tiers**

   Il est crucial que les entreprises surveillent constamment d'éventuelles nouvelles menaces et diffusent les menaces déjà connues.

   Pour obtenir une protection supplémentaire, prévoir l'adoption de procédures telles que le blocage à distance d'individus compromettant des secrets professionnels et la destruction à distance de dispositifs installés dans des ordinateurs ou des téléphones égarés.

8. **Avoir un plan de retour à l'entreprise**

   Même si plusieurs des mesures recommandées ci-dessus facilitent la transition du retour, il est important d'avoir des procédures en vigueur pour s'assurer que toute information de secret commercial obtenue en dehors de l'entreprise sera effectivement rendue ou détruite.

Avant même la pandémie du COVID-19, la définition de ce qui constituait des mesures raisonnables pour protéger les secrets professionnels d'une entreprise dépendait de plusieurs facteurs.

La pandémie et les directives de confinement, qui obligent toute la force de travail à migrer vers le télétravail, sont des facteurs supplémentaires déterminants pour définir le caractère raisonnable des efforts de protection des entreprises. Définir ce qui est approprié pour la protection des secrets professionnels des entreprises et s'assurer que les mesures et protocoles actuels satisfont ces critères, est aujourd'hui plus important que jamais.

Auteur: Antonella Carminatti
Antonella.Carminatti@bmapi.com.br
FrenchDesk@bmalaw.com.br