# Intelligence artificielle et télétravail : des mesures de sécurité à prendre

18 septembre 2020

## Auteur

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

De manière générale, la cybersécurité sera un enjeu important pour les entreprises dans les années à venir. Le télétravail, l'infonuagique et l'arrivée de l'intelligence artificielle font en sorte que d'immenses quantités de données sont susceptibles de devenir la proie de pirates informatiques, attirés par les renseignements personnels ou les secrets commerciaux hébergés qu'elles recèlent.

D'un point de vue juridique, les entreprises ont l'obligation de prendre des mesures raisonnables pour protéger les renseignements personnels qu'elles détiennent[1]. Bien que le cadre juridique ne spécifie pas toujours quels sont ces moyens raisonnables d'un point de vue technologique, il faut néanmoins adopter des mesures qui sont appropriées eu égard à la nature des renseignements personnels. Ces mesures doivent aussi être évaluées en tenant compte de l'évolution des menaces qui pèsent sur les systèmes informatiques.

Certaines juridictions vont plus loin, par exemple l'Europe où on demande que la conception même d'une solution informatique intègre des mesures de sécurité[2]. Aux États-Unis, pour les renseignements médicaux, de nombreuses balises guident les moyens techniques à adopter pour s'assurer de la sécurité des renseignements[3].

Outre les renseignements personnels qu'elle détient, une entreprise peut aussi vouloir protéger ses secrets commerciaux. Ceux-ci ont souvent une valeur inestimable et leur divulgation à des concurrents pourrait causer un préjudice irréparable à l'entreprise.

Aucune technologie n'est à l'abri. Dans un bulletin récent[4], la réputée firme Kaspersky nous met en garde contre les risques grandissants posés par certains groupes de pirates organisés qui pourraient vouloir exploiter les faiblesses des systèmes d'exploitation Linux, pourtant réputés très sécuritaires. Kaspersky énumère un certain nombre de failles connues, pouvant servir à mener des attaques visant à obtenir des rançons ou à accéder à de l'information privilégiée. Ce bulletin fait écho aux avertissements émis par le FBI aux États-Unis relativement à la découverte d'un nouveau logiciel malfaisant ciblant Linux[5].

*Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.*

**Les mesures à prendre pour gérer le risque**

C’est pourquoi il est important de prendre des mesures appropriées pour diminuer ces risques. Pour les administrateurs et dirigeants d’entreprise, il est notamment recommandé :

D’adopter des politiques d’entreprise empêchant l’installation de logiciels non sécuritaires par les usagers;
D’adopter des politiques de révision et de mises à jour régulières des mesures de sécurité informatiques;
De faire effectuer des tests d’intrusion et des audits pour vérifier la sécurité des systèmes;
De s’assurer qu’au moins une personne en autorité est responsable de la sécurité informatique.

En cas d’intrusion ou, de manière préventive, lorsqu’une entreprise collige et héberge des renseignements personnels sensibles, il est recommandé de consulter un avocat agissant en matière de renseignements personnels ou de secrets commerciaux afin de bien cerner les enjeux juridiques associés à ces questions.

---

1. Voir notamment : *Loi sur la protection des renseignements personnels dans le secteur privé* (Québec), art. 10, *Loi sur la protection des renseignements personnels et les documents électroniques* (Canada), art. 3.
2. *Règlement général sur la protection des données*, art. 25.
3. *Security Rule, sous le Health Insurance Portability and Accountability Act*, 45 CFR Part 160, 164.
4. https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
5. https://www.fbi.gov/news/pressrel/press-releases/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecurity-advisory

*Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.*