L'employeur peut-il épier l'utilisation des outils numériques par ses salariés ?

Introduction

Aujourd'hui, nous avons évolué depuis nos inquiétudes d'être écoutés dans nos conversations, que cela soit au téléphone, ou via microphones cachés, ou encore que les lettres soient lues, etc. ; vers dans notre aire actuelle de la révolution numérique ; où la majorité de nos informations et activités flottent dans ce qu'on appelle le "cloud", nous avons donc à nous poser la question suivante : Comment pouvons-nous être surveillés, traqués, quelles sont les limites et comment protéger nos informations. Aujourd'hui, l'un des grands risques d'atteinte sur la vie privée des gens est leur lieu de travail, où la grande majorité du temps est passé.

Notre entreprise peut nous espionner via des enregistreurs de frappe et de mot de passes (keyloggers), via des enregistreurs d'écran (screenloggers) ou encore via des serveurs de relais, mais aussi via des détournements de réseaux, etc. [1]

Nous allons donc étudier ce qu'un employeur, peut et ne peut pas faire avec les outils numériques de ses employés. Donc, de tout appareil et logiciel informatique, comme les téléphones, les ordinateurs, navigateurs web, etc. Que cela soit la propriété ou non de l'entreprise.

1 Les droits d'accès de l'employeur

Tout d'abord, l'employeur est tenu d'informer, et d'obtenir l'accord des salariés de tout dispositif de surveillance, sérieusement justifié, et mis en place ; ainsi que les modalités de contrôle, en incluant toute durée de stockage, le cas échéant. Que cela soit par le moyen d'une charte, ou d'une note [2].

Les contrôles doivent avoir pour objectif, seul :

- D'assurer la sécurité des réseaux contre des attaques (virus, intrusions, ...) ;
- De limiter les risques d'abus de l'accès internet ou des ressources mises à disposition (achats de produits, discussions sur les réseaux sociaux, utilisation intensive du processeur, du disque dur, etc.).

2 Les garanties pour la vie privée

L'employeur ne peut pas excessivement recevoir toutes les données en copie automatique (messages envoyés ou reçus, touches appuyés, etc.).

Même si l'employeur a interdit tout usage des outils de l'entreprise à des fins personnelles, toute donnée personnelle doit être identifiée comme telle ; par exemple en intitulant le nom du fichier, l'objet du courriel, etc. avec la mention « Personnel » ou « Privé » [3]. L'employeur sera donc en obligation de demander le consentement et la présence du salarié.

À défaut d'une telle mention, l'employeur est libre d'accéder aux données, car elle sont considérées comme ayant un caractère professionnel [5].

3 Les limites de la vie privée

L'employeur est en droit d'accéder aux données (documents, courriels, ...) identifiés comme privées sur les appareils mis à sa disposition sans accord préalable [4], s'il y a atteinte aux droits des personnes [6].

Références

[1] What Types of Spyware are Out There ? (toptenreviews.com) [24 Nov 2018].

[2] La cybersurveillance sur les lieux de travail : les droits et devoirs du salarié et de l'employeur (assistance.orange.fr) [24 Nov 2018].

[3] La cybersurveillance des salariés : Les enjeux, les limites, les droits et devoirs des employeurs (ldsconseil.fr) [24 Nov 2018].

[4] Article L2313-2 du code du travail, *« L'employeur procède sans délai à prendre les dispositions nécessaires pour remédier à cette situation. »* (legifrance.gouv.fr) [22 Nov 2018].

[5] Cass. Soc 18 octobre 2006 n°04-48.025, *« les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence. »*.

[6] Article L1121-1 du code du travail, *« Nul ne peut apporter aux droits des personnes et aux libertés individuelles [...]. »* (legifrance.gouv.fr) [22 Nov 2018].