LEPETITJOURNAL.COM
L'ACTUALITÉ LOCALE ET INTERNATIONALE POUR LES EXPATRIÉS FRANÇAIS ET LES FRANCOPHONES

Le "Smart Working" et la protection des données à la lumière du RGPD

Par Lablaw | Publié le 26/06/2018 à 00:15 | Mis à jour le 26/06/2018 à 09:31

Si le Smart Working (travail agile) ne cesse de progresser ces dernières années, le Règlement Général sur la Protection des Données (RGPD) apporte de nouvelles règles à ce mode de fonctionnement.

Le *Smart Working* se caractérise par une extrême flexibilité quant au temps et au lieu de travail, selon l'accord établi entre le salarié et l'employeur. Si d'une part, ce mode de travail permet au salarié de mieux concilier vie privée et vie professionnelle en lui permettant d'effectuer son travail à la maison

ou dans les lieux qu'il a choisi, il augmente d'autre part, le risque concernant le traitement et la sécurité des données personnelles et de l'entreprise, parfois réservées, que le travailleur doit utiliser pour rendre sa prestation.

Le Règlement de l'Union européenne entré en vigueur le 25 mai dernier est venu harmoniser les réglementations des États membres en matière de protection de la vie privée et introduit de nouvelles protections des données à caractères personnelles et professionnelles.

Et à la lumière du RGPD, le travail agile peut créer, pour les entreprises qui choisissent de l'adopter, certains problèmes concernant le traitement des données. Il appartient désormais à l'employeur de connaître les mesures à prendre s'il décide d'utiliser le *smart working* en respectant la législation sur la protection des données afin d'éviter toute sanction éventuelle. Ainsi, le RGPD prévoit qu'en cas de violation des données à caractère personnel, il appartient à l'employeur de notifier la violation en question à l'autorité de contrôle compétente, dans les 72 heures où il a pris connaissance du fait. En outre, lorsque la violation provient d'un *smart worker*, l'employeur pourra être sanctionné d'une amende allant jusqu'à dix millions d'euros pour ne pas avoir pris les mesures adéquates.

Travail à distance : les mesures à adopter par les entreprises

Dans un premier temps, comme prévu par le RGPD, un rôle fondamental sera joué par le Délégué à la protection des données (DPD). Le DPD a la responsabilité de préparer et de mettre en œuvre un système de gestion des données de l'entreprise. Il devra aussi tenir compte de l'existence de travailleurs à distance. Ce dernier devra former correctement les employés qui exercent leurs fonctions dans un régime de *smart working* en ce qui concerne les risques associés à cette méthode de travail et à l'utilisation correcte des instruments de l'entreprise.
Dans un second temps, des règlements d'entreprises devront être adoptés de manière à organiser l'utilisation des équipements électroniques accordés aux travailleurs (ordinateurs personnels, e-mail, portables professionnels, connexions internet, etc.…). En conséquence, les entreprises concernées devront garantir la sécurité des outils de travail mis à la disposition de l'employé, en procédant à un listage des normes de sécurité fixées. L'employeur devra également assurer la protection des outils informatiques de l'entreprise (ordinateurs portables, tablettes, smartphones) et la sécurité des données qu'ils contiennent, par la mise à jour continue des logiciels antivirus. Il est aussi conseillé de mettre en place un mécanisme de sauvegarde automatique des données et un système de communication directe avec le serveur principal de l'entreprise.
Il est également opportun d'établir des règles appropriées concernant les méthodes d'authentification

des systèmes d'information, ainsi que la désinstallation des informations d'identification, si l'employé n'a plus besoin de les utiliser.

Il serait donc adéquat pour les entreprises d'adopter un système d'authentification à deux facteurs, un mécanisme permettant au travailleur d'accéder aux données non seulement en tapant un mot de passe, mais aussi en procédant à une étape d'identification supplémentaire (texto, appel vocal, courriel, application pour les codes d'accès généraux). Ce système permet d'empêcher l'accès par des tiers aux données contenues dans l'appareil électronique fourni à l'employé, même en cas de vol ou de perte. Il permet également à l'employeur d'identifier l'employé qui s'est connecté.

Avv. Angelo Quarto - Studio Legale Lablaw
Corso Europa, 22 - 20122 Milano
Tel. +39 02 30 31 11
info.milano@lablaw.com
www.lablaw.com