# Droits des salariés en matière de cybersurveillance

publié le **05/06/2015**, vu **8523 fois**, Auteur : Yaya MENDY

**Tout salarié a droit au respect de sa vie privée même dans son lieu de travail.**

Selon la définition donnée par la Commission nationale de l'informatique et des libertés (CNIL), la cybersurveillance est « *un dispositif mis en place par un employeur pour contrôler l'usage des technologies de l'information et de la communication fait par les salariés* ».

Ce contrôle concerne au premier chef :

- les ordinateurs mis à la disposition des salariés,
- les téléphones portables professionnels,
- le réseau de l'entreprise…

Les enjeux de la cybersurveillance sont fondamentalement liés à la question du bon fonctionnement de l'entreprise et sa sécurité mais aussi et surtout au respect de la délicate frontière entre la vie professionnelle et la vie privée des salariés sur le lieu de travail.

En effet, il ressort de l'article 8 de la Convention européenne des droits de l'Homme et de l'article 9 du Code civil que tout individu a droit au respect de la vie privée.

En se fondant sur ces dispositions, la jurisprudence a consacré la notion de « vie personnelle » du salarié et a posé le principe selon lequel tout salarié a droit au respect de l'intimité de sa vie privée même dans son lieu de travail.

Cependant, étant donné que les outils fournis par l'employeur aux salariés sont des outils professionnels et à des fins professionnelles, l'employeur a parfaitement le droit de les contrôler et de contrôler l'usage que peuvent en faire les salariés.

Concrètement, l'employeur peut contrôler l'utilisation des outils professionnels mis à la disposition de ses salariés par le biais :

- de la consultation des fichiers ou des e-mails des salariés,
- du contrôle des connexions internet et de la durée des connexions,
- de la consultation de l'historique de la navigation des sites,
- le contrôle des SMS passés depuis les téléphones portables professionnels des salariés.

Toutefois, si l'employeur a évidemment le droit de contrôler les outils mis à la disposition des salariés, en revanche, ce contrôle doit s'opérer sous réserve du respect de trois principes fondamentaux, à savoir :

- le **principe de finalité**,
- le **principe de proportionnalité**, et
- le **principe de transparence**.

Le principe de finalité signifie que les données qui peuvent être collectées par l'employeur par le biais d'un de ces dispositifs ne peuvent être recueillies et traitées que pour un usage déterminé et légitime pour l'entreprise. (Exemple, la sécurité de l'entreprise, lutter contre des vols, le piratage de données confidentielles, la concurrence déloyale…)

Le principe de proportionnalité signifie que la surveillance des salariés ne doit pas conduire à apporter aux droits et aux libertés des personnes des restrictions qui ne seraient pas proportionnelles aux buts recherchés. Dès lors, les restrictions apportées par l'employeur aux droits et aux libertés individuelles des salariés non justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché sont illicites. (Article L. 1121-1 du code du travail)

Quant au principe de transparence, il implique trois obligations pour les employeurs :

- Tout d'abord, l'information préalable des salariés de tout dispositif de contrôle mis en place dans l'entreprise.
- Ensuite, l'information et la consultation préalable des institutions représentatives du personnel,
- Et enfin, la déclaration préalable à la CNIL.

Concernant l'information préalable des salariés, elle doit porter sur :

- les finalités poursuivies par le contrôle,
- le destinataire des données,
- le droit d'accès, d'opposition et de rectification des salariés.

Le non respect de ces obligations entraine l'irrecevabilité des preuves obtenues par le biais de ces dispositifs pour fonder un licenciement.

Ainsi, selon la Cour de cassation, les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la CNIL constituent un moyen de preuve illicite. (Cass. Soc. 8 octobre 2014, n° 13-14991)

De même, l'employeur ne peut pas prendre connaissance des messages identifiés comme personnels émis et reçus par le salarié grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. (Cass. Soc., 2 octobre 2001, n°99-42942)

Ce principe souffre néanmoins de quelques exceptions. En effet, la consultation de mails personnels est permise dans 3 cas:

- Consultation en présence du salarié ou dûment appelé,
- En cas de danger menaçant l'entreprise (ex : acte de terrorisme, piratage de données, concurrence déloyale),
- Autorisation du juge dans le cadre d'une enquête judiciaire ou une mesure d'instruction in futurum (article 145 du Code de Procédure Civile)

En tout état de cause, l’employeur ne peut pas, en raison de son pouvoir de contrôle, contrôler la correspondance du salarié comportant la mention « personnel » ou « privée »  même dans son lieu de travail.

De même, l’employeur ne peut apporter aux libertés individuelles et collectives des salariés de restrictions que si elles sont justifiées par la nature de la tâche à accomplir et proportionnées au but recherché.

L’employeur ne peut pas non plus faire de copie automatique de tous les messages écrits ou reçus par les salariés ni conserver des logs de connexion au-delà de six mois.

Il convient enfin de noter pour finir que l’employeur a légitimement accès au contenu des mails non identifiés comme personnels, mais il ne peut ensuite les utiliser que si le contenu est en rapport avec l’activité professionnelle (ex : dénigrement d’un supérieur).

De toute manière, le juge veille au respect par l’employeur de ces principes et de la vie privée des salariés sur le lieu de travail.

Je reste à votre disposition pour toutes questions supplémentaires.

**Yaya MENDY**