QUELLE CYBERSURVEILLANCE SUR LE LIEU DE TRAVAIL

Dans le cadre de l'exercice de leur activité professionnelle, les salariés disposent d'un ordinateur qui, le plus souvent, est connecté à Internet et doté d'une adresse de messagerie électronique.

L'employeur tolère généralement l'utilisation des différents outils informatiques à des fins autres que professionnelles. En tout état de cause cette utilisation doit rester raisonnable et ne pas affecter la bonne marche de l'entreprise.

Quels sont les intérêts en présence?

Le **salarié** a droit au respect de sa vie privée sur son lieu de travail. Le respect de la vie privée comprend notamment le secret des correspondances. Mais le salarié doit exécuter son contrat de travail et a aussi un devoir de loyauté vis-à-vis de son employeur: il ne doit pas porter préjudice au bon fonctionnement de l'entreprise.

L'**employeur** a le droit de protéger ses biens : les données confidentielles ne doivent pas être divulguées ou communiquées, son système informatique doit pouvoir fonctionner normalement (éviter les virus, les phénomènes de saturation ou d'engorgement,…).

Obligation d'informer les salariés sur l'utilisation des outils informatiques

L'employeur doit informer des limites et de l'usage à des fins personnelles qu'il tolère des outils informatiques ainsi que des dispositifs mis en place et des modalités de contrôle de ces outils : il doit ainsi dire s'il autorise les salariés à utiliser une messagerie électronique et/ou à surfer sur Internet et/ou à créer et à disposer de fichiers personnels.

Sans être exhaustif, il peut s'agir des informations suivantes :

- l'utilisation de ces outils à des fins privées (les périodes et les durées d'utilisation, le mode de stockage des informations sur le disque dur,...);
- les raisons et les objectifs du contrôle, la nature des données collectées, étendue et circonstances des contrôles, les destinataires des données ;
- la mise en place d'outils bloquant des sites Internet et/ou des messages en chaîne ou des fichiers trop lourds ;
- le mode de collecte et l'utilisation des données issues de la surveillance ;
- qui est autorisé à utiliser les données issues de la surveillance et dans quelles circonstances ;
- la durée de conservation des données issues de la surveillance;
- les décisions pouvant être prises par l'employeur lors d'un contrôle ;
- le rôle des représentants des salariés dans la mise en œuvre de la politique de surveillance ;
- les modalités du droit d'accès des salariés à leurs données.

Dans un souci de transparence et de loyauté dans les relations de travail, la Commission nationale recommande que l'employeur adopte une charte, un règlement interne ou tout autre document relatif à l'utilisation des outils informatiques ainsi qu'aux modalités de contrôle.

Quand et comment l'employeur peut-il contrôler les outils informatiques?

Même en cas d'interdiction totale de l'utilisation des outils informatiques à titre privé, l'employeur n'a pas le droit de contrôler l'usage de manière continue, sauf exception légale.

Quel que soit l'outil informatique, la surveillance doit toujours être **graduée** (« progressive Kontrollverdichtung »): l'employeur doit d'abord procéder à une surveillance ponctuelle pendant laquelle les salariés ne sont pas identifiés. Si des indices et soupçons sont détectés, alors l'employeur peut intensifier sa surveillance et faire des analyses individualisées où les salariés sont identifiés.

Contrôle de l'utilisation de la messagerie

L'employeur doit respecter le secret des correspondances:

Tout courriel entrant ou sortant depuis un poste de travail mis à la disposition par l'employeur est présumé être reçu ou envoyé dans le cadre de la relation professionnelle, c'est-à-dire que le destinataire ou l'expéditeur est réputé être l'employeur.

Mais, il s'agit d'une présomption simple : le message peut avoir le caractère d'une correspondance privée.

Dans ce cas, l'employeur ne peut pas ouvrir les courriers électroniques personnels de ses salariés, sous peine de violer le secret des correspondances, ce qui constitue une infraction pénale. La jurisprudence retient aussi que cette interdiction de lire les messages privés s'applique même dans le cas où l'employeur aurait interdit une utilisation non professionnelle des outils informatiques.Le principe du secret des correspondances peut cependant être levé dans le cadre d'une instruction pénale ou par une décision de justice.

Contrôle des messages professionnels:

Tout ce qui n'est pas identifié comme « personnel » est réputé être professionnel, de sorte que l'employeur peut y accéder.

Ce dernier peut tout à fait obtenir des données de trafic et de journalisation comme le volume, la fréquence, la taille, le format de leurs pièces jointes. Ces informations sont contrôlées sans identifier la personne concernée.

Dans l'hypothèse où des irrégularités sont constatées, il peut dans une seconde phase passer à l'identification des personnes concernées et contrôler le contenu des courriels professionnels.

Recommandations sur l'utilisation de la messagerie:

- Distinguer les courriels privés des courriels professionnels
  Pour éviter que l'employeur ne porte atteinte à la confidentialité des messages personnels, la Commission nationale propose:
  - l'installation d'une double boîte de messagerie séparant les messages personnels et les messages professionnels;
  - l'archivage des messages personnels dans un dossier appelé « personnel »;
  - les salariés indiquent la nature privée et personnelle dans l'objet des messages et incitent leurs correspondants à faire de même.
- L'employeur peut-il avoir accès à la messagerie en cas d'absence du salarié pour assurer la continuité des affaires ?
  Après en avoir informé les salariés et les organes représentatifs, il est suggéré de:
  - mettre en place d'une réponse automatique d'absence du bureau à l'expéditeur avec indication des personnes à contacter en cas d'urgence;
  - désigner un suppléant qui dispose d'un droit d'accès personnalisé à la messagerie de son collègue : il peut lire et traiter les messages professionnels, mais il ne peut pas lire les messages identifiés comme personnels;
  - transférer à un suppléant tous les messages entrants.

Chaque salarié doit connaître l'identité de son suppléant.

- En cas de départ définitif du salarié, il est recommandé que:
  - l'employé qui quitte l'entreprise transfère tous les documents professionnels en cours à une personne prédéfinie (par exemple, son supérieur hiérarchique) ;
  - il certifie avoir remis à son employeur tous les documents professionnels ;
  - il peut copier les messages électroniques et autres documents de nature privée sur un support privé, puis les effacer des serveurs de l'entreprise ;
  - l'employeur s'engage à bloquer tous les comptes informatiques et à effacer la/les boîte/s aux lettres du salarié dès son départ ;
  - les personnes qui enverront un message à l'adresse bloquée sont automatiquement informées de la suppression de l'adresse électronique et reçoivent une adresse alternative.

Contrôle de l'utilisation de l'internet

L'accès à Internet est donné pour des raisons professionnelles.

L'employeur peut fixer les conditions et limites de l'utilisation d'internet pour des besoins privés. Il doit informer clairement et préalablement les salariés sur les dispositifs et les modalités de contrôle.

Il ne peut pas surveiller individuellement un salarié sans avoir, au préalable, procéder à une surveillance globale et non personnelle. Ainsi, il peut faire dresser une liste d'adresses de sites consultés de façon globale sur une certaine période, sans identifier les auteurs des consultations. S'il a des indices sur une utilisation d'Internet préjudiciable pour l'entreprise en repérant une durée anormalement élevée de consultation d'internet ou la mention d'adresses de sites suspects, il pourra alors prendre les mesures de contrôle appropriées et passer, alors, dans un second stade à une surveillance individualisée.

La Commission nationale recommande la mise en place de moyens de protection préventifs compte tenu des risques de virus que présentent ces accès, comme par exemple, des filtrages de sites non autorisés, l'interdiction de téléchargements de logiciels ou l'interdiction de se connecter à des forums de discussion (« chat »).

Contrôle des supports informatiques et des fichiers de journalisation

De façon générale, tous les documents et fichiers créés par un salarié sont censés être de nature professionnelle. Mais le salarié peut, dans les limites du raisonnable, créer des documents ou fichiers qu'il identifie comme étant personnels, ceci en vertu du principe de la sphère privée sur le lieu de travail.

La surveillance des supports informatiques et des fichiers de journalisation ne doit pas se faire sous forme d'analyse individualisée mais doit être graduée dans le rythme et l'envergure des données contrôlées.

En ce qui concerne les fichiers ou documents identifiés comme privés, l'employeur ne peut pas y accéder sans la présence du salarié concerné. Ce dernier doit avoir la possibilité de s'opposer à l'ouverture d'un fichier privé et doit être informé de cette possibilité au moment du contrôle.

La Commission nationale recommande donc que l'employeur prenne des mesures destinées à assurer que les documents électroniques de l'entreprise soient accessibles pendant l'absence du salarié sans qu'il soit nécessaire d'ouvrir les dossiers « personnels » du salarié.

Enfin, il est recommandé qu'à la fin de son emploi, le salarié soit habilité à obtenir une copie des documents conservés dans son fichier privé et qu'il ait la possibilité d'effacer ses dossiers personnel, le cas échéant, en présence d'un représentant de l'employeur.

Dernière mise à jour 05/09/2019

Commission nationale
pour la protection des données

15, Boulevard du Jazz
L-4370 Belvaux

Tél. : (+352) 26 10 60 -1