

## THÈME D5 SÉCURITÉ DES SI

## D 5.2 L'obligation d'informer

## D 5.2

Mots clés : cybersurveillance, charte informatique

Fiche synthèse

<b>Idée clé</b> →	La loi protège la vie privée du salarié et encadre l'usage des outils numériques sur le lieu de travail
<b>Donner du sens</b> →	Les usages (privés) d'outils professionnels mis à la disposition des salariés sont à l'origine de nombreux litiges portés devant les tribunaux

L'employeur a légitimement un droit de regard sur les activités de ses salariés. Si les outils numériques utilisés sur le lieu du travail améliorent la performance de l'activité ils peuvent également être utilisés de façon personnelle par le salarié. De son côté l'employeur peut renforcer son pouvoir de contrôle grâce à ces outils...

**1. La cybersurveillance des salariés**

La cybersurveillance regroupe tous les moyens techniques permettant de contrôler un individu. Elle se fait au moyen de logiciels de surveillance permettant d'enregistrer tous les événements ou messages survenus pendant un temps donné et à un endroit déterminé. Les écoutes téléphoniques font partie intégrante de la cybersurveillance, tout comme le traçage d'internautes sur le web ou sur un réseau Intranet ou encore des dispositifs de vidéosurveillance (*voir infra*). La surveillance et l'interception de courriers électroniques sont considérées comme de la cybersurveillance.

La loi impose un principe de proportionnalité : la surveillance des salariés doit s'effectuer de façon adaptée, pertinente, non excessive et en adéquation avec l'objectif poursuivi « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché » article L 1121-1 du code du travail. Une surveillance générale et permanente serait contraire à ce principe.

La loi impose des obligations de loyauté et de transparence

- l'article L 1221-9 du code « aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié et du candidat à un emploi ». Sur ce fondement, la Cour de cassation a refusé de reconnaître la validité de la preuve, dans le cadre d'une procédure de licenciement, qui avait été rapportée par des caméras de vidéosurveillance installées à l'insu du salarié (Cour de cassation, chambre sociale, 20 novembre 1991)
- Le comité d'entreprise doit être informé et consulté avant l'introduction d'un dispositif de contrôle des salariés articles L.2327 et L.2323-32 du code du travail. Cette consultation est obligatoire, comme le démontre un jugement du TGI de Paris du 4 avril 2006 : « doit être suspendue la mise en œuvre d'un dispositif d'écoute téléphonique des salariés en raison de l'absence de consultation du Comité d'établissement [...] et de la non-déclaration à la Commission nationale de l'informatique et des libertés (CNIL) du traitement de données à caractère personnel [...] ».
- Les employés doivent donc toujours être individuellement informés de la mise en œuvre de dispositifs permettant de contrôler leur activité au sein de l'entreprise.
- La cybersurveillance recourt à des technologies collectant et stockant des données à caractère personnel. Dans ce cadre, une déclaration auprès de la CNIL s'impose. Ceci va concerner notamment les outils de gestion du travail de groupe (*workflows*) ou encore les outils techniques de surveillance du réseau téléphonique (autocommutateurs, systèmes d'enregistrement des communications...) ou électronique (stockage des logs de messagerie, firewall, programmes de télémaintenance, serveur proxy...).

Concernant les DCP collectées par l'employeur sur les salariés :

- Elles doivent avoir un usage déterminé et légitime,
- L'employeur ne doit pas porter de commentaires excessifs dans les fichiers personnels
  - Le salarié doit pouvoir exercer son droit d'accès, de rectification, de suppression de ses DCP comme le prévoit la LIL de 1978

- La durée de conservation des données doit être précisée pour chaque fichier et en fonction de la finalité

*Remarque : le cas de la vidéosurveillance : Interdiction en certains lieux (vestiaires, douches...) Limitations pour d'autres lieux (enregistrement systématique son et vidéo pour les locaux syndicaux) Déclaration Cnil : déclaration normale pour un lieu privé (sans accès du public comme dans un supermarché) Limitation de la vidéo lecture aux seules personnes habilitées ; Conservation limitée dans le temps (quelques jours à un mois maximum)*

## **2. Consultation des dossiers et fichiers des salariés, usage de la messagerie privée par les salariés**

Par principe, les dossiers, fichiers et tous les écrits, créés, reçus et stockés sur le poste de travail du salarié sont présumés professionnels (Cour de cassation, chambre sociale 15 décembre 2010). Les fichiers et dossiers figurant sur le poste informatique professionnel peuvent être consultés par l'employeur. Leur cryptage constitue une faute susceptible d'entraîner le licenciement du salarié (Cour de cassation chambre sociale 18 octobre 2006)

Cependant cette présomption de professionnalité n'autorise pas l'employeur à consulter les fichiers personnels du salarié. Le célèbre arrêt Nikon rendu par la Cour de cassation en 2001 précise que « le salarié a droit au temps et au lieu de travail, au respect de l'intimité de la vie privée, que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à l'outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation professionnelle de son ordinateur ».

Le salarié a donc droit, sur son lieu de travail, au respect de sa vie privée auquel la jurisprudence a rattaché le secret des correspondances privées. Le salarié doit clairement identifier ses fichiers personnels afin d'en interdire l'accès à l'employeur. Toute violation est sanctionnée par l'article 9 du code civil et l'article 8 de la convention européenne des droits de l'homme

Par un arrêt de principe du 17 mai 2005 il est désormais admis que la consultation par l'employeur des fichiers personnels du salarié stockés sur son poste de travail peut intervenir :

- en cas de circonstances exceptionnelles « risque ou événement particulier »
- si le salarié en a été informé et qu'il a dûment été convoqué pour assister à l'ouverture de son disque dur

## **3. Encadrement de l'usage des outils numériques au lieu de travail**

- L'employeur peut soumettre à la signature de ses salariés une charte, fixant les conditions d'usage des outils informatiques et de la messagerie dans l'entreprise
- La charte fixe des règles en matière d'utilisation du système informatique, de la messagerie, de l'identification des fichiers personnels. Ces règles sont opposables aux salariés à condition que le Règlement intérieur fasse mention de la charte en question.
- Cette charte permet
  - de prévenir d'éventuels litiges entre employeur et salariés
  - de remplir l'obligation d'information quant au système de contrôle des salariés
  - de renforcer la présomption de professionnalité du matériel informatique de l'entreprise
- Les tribunaux accordent une valeur juridique à cette charte si :
  - elle est signée par les salariés
  - elle a été soumise aux institutions représentatives du personnel
  - elle a été adressée à l'inspection du travail
  - elle est affichée dans les locaux de l'entreprise

### **En résumé**

Les Tic ont finalement instauré un nouvel ordre relationnel en rupture avec les habitudes passées. Désormais les nouveaux outils à la disposition de l'employeur, s'ils augmentent son pouvoir, doivent nécessairement être encadrés afin de préserver les droits du salarié. Ce dernier peut utiliser les outils mis à sa disposition mais ces utilisations sont encadrées.

### **Des exemples pour illustrer**

La CNIL a publié deux rapports sur ce thème « *Cybersurveillance sur les lieux de travail* ».  
Aux Etats-Unis, la sphère privée (v/s la sphère professionnelle) du salarié est presque inexistante : les documents et fichiers des salariés sont présumés professionnels.

Toute reproduction sur un autre site INTERDITE