AST 67
Alsace Santé au Travail
Partenaire des entreprises

Salarié surveillé *versus* employeur responsable

Michel Meyer
Directeur informatique

SMSTS, 11 mars 2016

Plan

- Contexte
- Moyens de « surveiller » les salariés
- Droits des salariés
- Devoirs des salariés
- Devoirs des entreprises
- Responsabilités des entreprises
- Bonnes pratiques

TIC omniprésentes

Taux d'équipement des entreprises* :

- Ordinateurs : 98%
- Connexion internet : 97%

*source Insee, enquête TIC 2007

Taux d'équipement des particuliers* :

- Ordinateur : 79%
- Smartphone : 56%
- Tablette : 29%
- Connexion internet : 82%

*source CSA, 2013

Hausse de la cybercriminalité

Cas médiatisés d'attaques ou de vols de données informatisées :

- Wallmart
  → 100 millions de cartes de crédit volées
- TV5-monde, 8 avril 2015
  → arrêt des émissions pendant 24h
- Ashley Madison
  → Vol des données (recours collectif en justice)
- …

Suppression des frontières

Personnel

Professionnel

Suppression des frontières

Personnel

Professionnel

Moyens techniques qui permettent de surveiller les salariés

- Collecter des « Logs » d'accès à internet
- Collecter des « Logs » d'accès aux applications
- Consulter le contenu des disques durs des ordinateurs
- Collecter des logiciels installés
- Accéder au contenu de la messagerie
- Géolocaliser : Smartphone, GPS de voiture
- Autres moyens : Vidéosurveilllance, écoute téléphonique…

Droit des salariés

Respect de la vie privée (art. 9 du Code civil) :

> *Chacun a droit au respect de sa vie privée. Les juges peuvent sans préjudice de la réparation du dommage subi, prescrire toutes mesures ... propres à empêcher ou faire cesser une atteinte à la vie privée. Ces mesures peuvent s'il y a urgence, être ordonnées en référé.*

Art. L 1121-1 du Code du travail :

> *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.*

Droit des salariés

Le droit à l'intimité, le droit à l'image, le droit au secret des correspondances et des conversations téléphoniques et télématiques rentrent **dans le champ d'application de l'article 9 du Code civil par le biais de la jurisprudence étant donné que la loi ne détermine pas son champ d'application explicitement.**

Par ricochet, on peut inclure ces droits dans ceux visés par l'article L. 1121-1 du Code du travail tout en gardant en tête cette **exigence de proportionnalité**.

Utilisation personnelle d'ordinateur professionnel

- Le salarié a le droit d'utiliser un ordinateur d'entreprise à des fins personnelles.

- Les données contenues dans les ordinateurs y compris les périphériques (clés USB…) des entreprises sont présupposées être des données professionnelles.
  Il convient de classer les données personnelles dans des dossiers spécifiques estampillés « Personnel »

Limites de l'arrêt Nikon

- L'arrêt « CATHNET-SCIENCE » pose 2 limites à ce principe : l'employeur peut accéder aux fichiers non personnels si le salarié est présent ou s'il est informé.

  Par ailleurs, s'il existe un risque ou un événement particulier, l'employeur peut se passer de la présence du salarié.

Cour de cassation, 2005 : un salarié stockait sur son disque dur des fichiers privés (photos érotiques), sous un dossier intitulé « perso ». Licencié pour faute grave, il conteste son licenciement en arguant du fait que l'employeur n'avait pas demandé ni obtenu son accord pour accéder à ces fichiers.

Le salarié doit effectuer un travail

Le Code du travail définit le temps de travail effectif comme celui où le salarié est à la disposition de l'employeur sans pouvoir vaquer à ses occupations personnelles.

C'est sur la base de cette obligation que la jurisprudence a tendance à sanctionner un usage excessif d'Internet qui viendrait nuire au travail à réaliser. Un salarié peut donc être licencié pour une utilisation abusive d'Internet.

Arrêt de la Cour de cassation, 18 mars 2009, LAUZIN

Le salarié doit respecter le pouvoir réglementaire de son employeur

L'employeur organise le travail et en contrôle le résultat. Il a donc le droit, mais aussi l'obligation de contrôler l'usage fait par ses salariés de l'outil informatique. Son pouvoir de direction et d'instruction lui permet de déterminer les conditions et les usages de ces outils.

Cour d'appel d'Aix en Provence, le 17 déc. 2002,
a jugé qu'un salarié pouvait être licencié pour faute grave, pour avoir visité de manière très prolongée des sites pornographiques.
La Cour d'appel a en effet pris en compte les risques qu'encourt l'entreprise : « *la gravité de la faute se trouve notamment caractérisée par les risques de poursuites judiciaires que le salarié a fait encourir à son employeur* »

Le salarié à une obligation de loyauté

- L'obligation de loyauté est définie par l'article 1135 du Code civil et l'article L.1222-1 du Code du travail : "Le contrat de travail est exécuté de bonne foi "
- Le conseil des Prud'hommes de Boulogne Billancourt a ainsi considéré comme valable, en novembre 2010, le licenciement pour "dénigrement de l'entreprise" et "incitation à la rébellion" de salariés qui avaient critiqué leur entreprise sur leur mur Facebook.

Le salarié doit respecter le cadre des règles sociales et pénales

- L'employeur peut être tenu pour responsable des actes de ses salariés sur Internet, en matière de téléchargement (loi Hadopi) par exemple.
- Certains sites sont illégaux par nature : sites pédophiles, incitation au terrorisme, à la haine raciale.

Obligation de l'employeur

- Obligations d'information :
  - Article L. 1222-4 : “ Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.”
- Respect de la vie privée
- Exigence de proportionnalité

Obligation de l'employeur

- Conséquence d'un défaut d'information :

Arrêt de la chambre sociale de la Cour de Cassation rendu le 10 décembre 1997 : Ordonne le retrait de toute procédure des éléments de preuve obtenus par l'employeur au moyen de l'enregistrement vidéo mis en place en 1993

Menaces informatiques

- Perturbation du système d'information : virus, cryptolocker, vol de matériel
- Vol de données
- Attaque des sites internet

Entreprise responsable

- Responsable du bon fonctionnement de son système d'information :
  - 82% des PME non préparées ne survivent pas à un important crash informatique
- Responsable de la performance économique

Protéger son système d'information

- La majorité des incidents est d'origine interne
  - Hôpital de Marseille :
    - Cas de la divulgation de dossiers médicaux sur internet (03/2013)

Entreprise responsable

Responsable des données hébergées :

- du personnel de l'entreprise
- de ses clients

Entreprise responsable

Commission Européenne :

« les données personnelles ne peuvent être collectées légalement que sous de strictes conditions et dans un but légitime.
De plus, les personnes physiques ou morales qui recueillent et gèrent vos informations personnelles doivent les protéger de tout usage abusif. »

Entreprise responsable

- Vol de données, Sony Pictures 11/2014 :
  - Vol et publication des données
  - Coût estimé remise en état du Système d'information : 35 millions $
- Hôpital de Los Angeles, 5 fév. 2016
  - 10 jours sans système d'information

Comment assurer la sécurité des données ?

- Sécuriser l'infrastructure (sécurité physique, logique)
- Adopter le chiffrement
- Assurer la traçabilité et l'intégrité
- Sauvegarder les données
- Sensibiliser les salariés
- Prendre en compte la dimension légale
- Evaluer les risques

Bonnes pratiques

Réaliser une charte TIC adossée au règlement intérieur qui décrit :

- Les mécanismes de surveillance
- Le rôle et les responsabilités des différents acteurs : salarié, employeur, administrateur informatique
- La conduite à tenir en cas d'incident

Bonnes pratiques

- Pour les données sensibles : définir un référentiel de sécurité spécifique
- Si possible, séparer les pouvoirs Administrateur informatique de la Direction
- Sensibiliser régulièrement aux risques informatiques

Remerciements

Cabinet d'avocats Mathias

Communication AST67