La cybersurveillance des salariés

Emmanuelle Barbot – CREIS Terminal

L'essor des NTIC (Nouvelles Technologies de l'Information et de la Communication) dans les entreprises depuis la fin des années 90 a eu pour conséquence une utilisation croissante de ces outils (Internet, mails…) par les salariés à des fins professionnelles mais aussi personnelles.

En 2000 déjà, 2/3 des sociétés américaines utilisaient un moyen électronique pour surveiller les salariés et près de la moitié inspectaient les e-mails, plus de 63 % des employeurs de grandes sociétés examinaient les mails sortant en juin 2005.
Depuis octobre 2000, en Grande Bretagne, les employeurs sont autorisés à surveiller les courriers électroniques de leurs salariés.

Quelle est la situation actuelle en France ? La jurisprudence s'enrichit régulièrement et des règles sur les droits et obligations du salarié et de l'employeur existent déjà dans le Code du travail, la CNIL et le Forum des droits sur l'Internet ont émis des recommandations.

Les différents aspects de cette problématique vont être présentés :
D'un côté l'employeur a le droit de contrôler le travail effectué par le salarié, de l'autre le salarié a le droit au respect de sa vie privée (article 9 du Code Civil).

II. Les points de vue

- De l'employeur

L'employeur soucieux d'améliorer les performances de son entreprise a de plus en plus recours aux nouvelles technologies. Dans de nombreuses entreprises et dans les SSII en particulier, une grande partie des actifs patrimoniaux immatériels est contenue dans le système d'information de l'entreprise : données sensibles stratégiques, commerciales, savoir-faire….
Si la perte de productivité des salariés liée à une utilisation massive des NTIC peut constituer une inquiétude, l'ouverture des réseaux rend le système d'information très sensible aux attaques extérieures, à la diffusion d'informations sensibles ou confidentielles, ou aux fraudes internes à l'entreprise, ces dernières constituant la majorité des cas de sinistralité informatique.
Selon une étude réalisée entre 2008 et 2009 par la société Olfeo, sur 1h26 d'utilisation quotidienne d'Internet au travail, 58 minutes correspondaient à un usage non-professionnel. Les entreprises n'encadrant pas l'usage d'Internet subiraient une perte de productivité journalière de 13.8 %.

Outre les atteintes classiques à la sécurité informatique, programmes malveillants et atteintes à distance à l'intégrité des systèmes d'information, le risque est lié aux usages actuels de l'Internet, du web 2.0 en particulier (les blogs, forums, réseaux sociaux, messageries instantanées…) et à l'utilisation de nouveaux outils (clef USB, disque dur externe, ordinateur portable, smartphone…) pouvant mettre en péril les données confidentielles de l'entreprise et de ses salariés. Les PME sont particulièrement vulnérables, la sécurisation de leur système d'information étant souvent imparfaite.

L'employeur souhaite donc exercer un contrôle de l'usage des NTIC dans son entreprise et de l'usage des réseaux par les salariés, ces droits de surveillance et de contrôle sur l'activité et la productivité du salarié lui sont reconnus dans le cadre de son pouvoir de direction.

En outre, la responsabilité juridique notamment pénale de l'employeur ou de l'entreprise peut être engagée en cas de violation de la loi par un salarié indélicat (par exemple en cas de téléchargement illicite, du non-respect de la loi sur la protection des données personnelles, d'atteinte à la sécurité informatique…) :
Deux exemples :
Ainsi, « détenir une image ou sa représentation » est puni de trois ans de prison et 75 000 € d'amende. Or les images illicites téléchargées par un salarié peuvent être stockées sur le serveur de l'entreprise.
Le responsable de l'entreprise doit assurer également la sécurité des données sous peine d'une peine de cinq ans de prison et 300 000 € d'amende.

Une délégation des pouvoirs du dirigeant vers un spécialiste de la sécurité des systèmes d'information se traduisant par un transfert de la responsabilité pénale peut se justifier dans certains cas.

- Le salarié

Cependant, les menaces sur le respect de la vie privée du salarié dans l'entreprise sont réelles :

Nul ne peut être surveillé à son insu. Or, les NTIC permettent de conserver des traces des flux d'informations directement ou indirectement personnelles : autocommutateurs téléphoniques, logiciels de contrôle et d'enregistrement de boîtes mails ou des sites visités, logiciels de filtrage, outils de géolocalisation des salariés nomades….

Se pose aussi le problème du rôle de l'administrateur système qui a en charge de mettre en place les procédures de contrôle et de surveillance des réseaux, mais qui peut avoir accès à des informations personnelles et se retrouver dans une position délicate vis à vis de son employeur et supérieur.

La Cour d'appel de Paris, (arrêt du 17 décembre 2001) a rappelé qu'il était dans la mission des administrateurs d'assurer le fonctionnement normal des réseaux et de veiller à leur sécurité.
http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-d-appel-de-paris-11e-chambre-section-a-17-decembre-2001.html

Le rapport de la CNIL publié en 2004 parle de secret professionnel ou d'obligation de discrétion des administrateurs qui ne doivent pas révéler de manière systématique des données considérées comme personnelles si elles ne mettent pas en cause le fonctionnement du système ou l'intérêt de l'entreprise :

http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf

III. Les fondements juridiques de la cybersurveillance

Base : Le contrat de travail

- la surveillance des locaux et du personnel

Toute mise en place d'un système de surveillance et de contrôle de l'activité des salariés ne peut se faire que si les représentants du personnel ont été préalablement consultés (le comité d'entreprise) et les salariés avertis selon le principe de transparence.
En particulier, les procédés de contrôle doivent être justifiés par la tâche à accomplir (principe de proportionnalité).

Les *systèmes de vidéosurveillance* doivent être déclarés à la CNIL dès lors que les images sont enregistrées ou conservées.
La CNIL a ainsi prononcé une sanction pécuniaire de 10 000 € à l'encontre d'une société ayant filmé ses salariés à leur poste de travail sans les en avoir averti.
http://www.cnil.fr/dossiers/travail/actualites/article/26/10-000-euros-damende-pour-avoir-installe-une-videosurveillance-permanente-des-salaries/

Tout recours aux *techniques de géolocalisation* des salariés relève de la même règle (voir les recommandations de la CNIL en 2006) :
http://www.cnil.fr/index.php?id=1999&news[uid]=342&cHash=73ab4d0100

L'application en France de la loi américaine Sarbanes-Oxley sur les *dispositifs d'alerte professionnelle* est encadrée par la CNIL :
http://www.cnil.fr/index.php?id=2053

La conséquence du non respect de ces principes est l'illicéité de la preuve en cas de litige :

Arrêt de la Cour d'Appel de Dijon du 14 septembre 2010 : la surveillance d'un salarié par la géolocalisation n'était pas légale. Le licenciement a donc été déclaré sans cause réelle et sérieuse.
http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2999

- La surveillance des correspondances électroniques et échanges

En principe, le matériel mis à la disposition des salariés est destiné à un usage professionnel. Cependant, comme pour la correspondance postale, les mails ont un caractère privé.
L'employeur dispose d'un droit de contrôle des mails professionnels ; par contre il ne peut prendre connaissance des informations contenues dans le mail personnel qu'avec l'accord du salarié ou en cas de motif grave ou légitime.

L'arrêt « Nikon » de la Cour de Cassation du 2 octobre 2001 précise que le salarié a droit, même sur son lieu de travail, au respect de l'intimité de sa vie privée et au secret des correspondances, y compris si l'usage non professionnel des TIC est interdit.

http://www.foruminternet.org/actualites/lire.phtml?id=787

Les arrêts du 23 mai 2007 et du 10 juin 2008 reconnaissent à l'employeur le droit, sous conditions (sous contrôle d'un huissier avec présence du salarié), d'accéder à la messagerie personnelle d'un salarié soupçonné de concurrence déloyale, sans qu'il s'agisse de violation du secret de la correspondance privée.

http://www.cnil.fr/index.php?id=1840&news[uid]=269&cHash=541f390577
http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-sociale-10-juin-2008-2695.html

L'arrêt de la Cour de cassation du 21 octobre 2009 établit en outre qu'un dossier informatique identifié par les initiales du salarié ne peut être considéré comme personnel.

http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-sociale-21-octobre-2009-2953.html

En pratique, l'employeur doit distinguer la correspondance électronique professionnelle du mèl personnel, ce qui n'est pas toujours facile à mettre en pratique.

- La surveillance des fichiers et des répertoires personnels

Le pouvoir de contrôle de l'employeur est précisé dans deux arrêts récents :

Selon l'arrêt de la Cour de cassation du 17 mai 2005, l'employeur ne peut ouvrir les fichiers contenus dans les répertoires personnels des ordinateurs en dehors de la présence du salarié sauf s'il existe un risque avéré. Cette décision est à rapprocher des cas jugés concernant les fouilles irrégulières dans les effets personnels des salariés.

http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=926

Les Arrêts de la Cour de cassation du 18/10/2006 précisent que les documents, fichiers et dossiers et outils détenus par le salarié au travail sont présumés avoir un caractère professionnel sauf s'ils sont identifiés comme personnels, l'employeur peut y avoir accès. D'autre part, un salarié ne peut crypter ses dossiers personnels sans autorisation de son employeur.

http://www.legalis.net/jurisprudence-decision.php3?id_article=1774

Néanmoins l'application de cette règle peut être problématique quand le caractère privé ou personnel de l'outil informatique n'apparaît pas explicitement, par exemple l'utilisation d'un outil de sauvegarde externe.

- La surveillance des réseaux

Pour des motifs de sécurité ou pour des raisons légales ou règlementaires, la surveillance des réseaux s'avère nécessaire avec la consultation des mails reçus et envoyés, le suivi des adresses des sites visités, la durée de la connexion, les fichiers téléchargés, les mots de passe, l'enregistrement des opérations effectuées par le salarié sur son poste de travail, utilisation de logiciel de prise en main à distance, la téléphonie sous IP…

L'arrêt du 9 juillet 2008 réaffirme le caractère professionnel des connexions établies par un salarié sur son lieu de travail pendant son temps de travail.

http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-sociale-9-juillet-2008-2760.html

La loi du 6 janvier 1978 prévoit l'obligation d'informer le salarié lors de la collecte d'informations personnelles : Le salarié doit être averti des moyens de contrôle direct sinon il s'agit d'une atteinte à sa vie privée et les représentants du personnel doivent être informés, le principe de proportionnalité doit être respecté.

Le système de traçabilité doit être déterminé a priori, les fichiers de journalisation (enregistrement des opérations effectuées par les salariés) doivent être déclarés à la CNIL.
La durée de conservation des données doit être précisée.

- Les écoutes téléphoniques

L'usage du téléphone à des fins personnelles sur le lieu de travail est généralement admis à condition qu'il ne soit pas abusif. Les respects de la vie privée et de la liberté individuelle doivent être garantis. Les fichiers mis en œuvre dans le cadre de la téléphonie fixe et mobile avec usage d'un autocommutateur doivent être déclarés à la CNIL. Il est interdit de contrôler les appels des représentants du personnel et représentants syndicaux.

En outre, l'enregistrement des conversations téléphoniques sur le lieu de travail doit faire l'objet d'une information préalable du personnel et doit être proportionné aux objectifs poursuivis. Les écoutes téléphoniques à l'insu du salarié sont donc considérées comme illicites ; en revanche, la simple surveillance des communications téléphoniques à partir des relevés de facturation peut être exercée même en l'absence d'information préalable du salarié : voir l'arrêt de la Cour de Cassation du 29 janvier 2008 :
http://www.legalis.net/jurisprudence-decision.php3?id_article=2213

- Les mesures techniques de protection

La loi sur les Droits d'Auteur et les Droits Voisins dans la Société de l'Information du 1/08/2006 autorise la mise en place de mesures techniques de protection pour éviter les copies ou téléchargement d'œuvres protégées.

http://www.foruminternet.org/documents/lois/lire.phtml?id=1099

D'une manière générale, la justice est méfiante vis à vis des preuves résultant de moyens de surveillance électronique ; des cas de licenciement pour faute grave ont été transformés en licenciement pour cause réelle et sérieuse.
L'utilisation du courrier électronique ne semble pas constituer un moyen de preuve pour justifier une sanction ou un licenciement mais il semblerait que la jurisprudence évolue : le mail commence à être reconnu comme preuve de la naissance d'une obligation.

IV. Les droits et obligations des salariés

Si les moyens informatiques utilisés sur le lieu de travail sont d'abord à usage professionnel, il est reconnu au salarié le droit d'avoir du temps « privé » au bureau, à condition qu'il ne soit pas excessif selon une décision de la Cour de Justice européenne.

Si la Cour de cassation avait affirmé en 2001 (arrêt Nikon) le droit au respect de l'intimité de la vie privée y compris sur le lieu de travail , il est à noter que la jurisprudence récente tend à reconnaître le caractère professionnel des outils informatiques, les juges tendant à sanctionner un usage manifestement excessif des NTIC sur le lieu de travail ou le comportement déloyal du salarié.

Une utilisation personnelle et modérée des outils informatiques est généralement permise en dehors des heures de travail, à condition que cette utilisation ne soit pas abusive, nuisible (obligation de loyauté du salarié vis-à-vis de son employeur découlant du contrat de travail) : par exemple, il est interdit de transformer un mèl professionnel en un mèl personnel.

L'employeur peut ainsi interdire ou restreindre l'utilisation de certains matériels représentant un certain coût, interdire la consultation de certains sites Internet ou en limiter l'accès (sites de réseaux sociaux ou de streaming par exemple).

Un arrêt de la Cour de cassation du 18 mars 2009 a confirmé le licenciement pour faute grave d'un salarié ayant passé trop de temps sur Internet durant ses heures de travail (41 heures dans le mois, soit 25 % de son temps de travail).

http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-sociale-18-mars-2009-2859.html

Les utilisateurs doivent respecter la législation ; la consultation de sites illicites, le téléchargement d'œuvres protégées par le droit d'auteur sont une infraction pénale.

La participation à des forums de discussion ne peut se faire qu'avec l'autorisation de l'employeur. L'utilisation de boîte webmail, l'inscription à des messageries instantanées ou la participation à des espaces communautaires virtuels sont largement proscrites, tout comme l'est l'utilisation par le salarié de ses propres logiciels.

Le salarié a droit au respect du secret de sa correspondance privée. Cependant, il est tenu de communiquer son mot de passe ou ses fichiers en sa possession quand le bon fonctionnement de l'entreprise dépend des données qu'il détient et en cas d'absence.

Il possède également un droit à l'information sur les procédés de surveillance et de contrôle utilisés.

La loi relative à la formation professionnelle tout au long de la vie et au dialogue social du 4 mai 2004 officialise la possibilité pour les organisations syndicales d'utiliser l'intranet ou la messagerie interne sous réserve de la signature d'un accord d'entreprise.

http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=SOCX0300159L

Certains soulèvent l'idée d'instaurer un droit à la déconnexion afin que la sphère professionnelle n'empiète pas sur la vie privée, avec le problème de la possession d'un ordinateur portable d'entreprise ou d'un téléphone portable : le salarié devient joignable à tout moment.

IV. La charte : une nécessité pour une bonne utilisation des NTIC

Dans son rapport sur la cybersurveillance publié en 2004, la CNIL recommandait aux employeurs d'élaborer en collaboration avec les salariés une charte de bonne utilisation des NTIC au travail. Elle préconise également la rédaction d'un bilan annuel Informatique et Libertés.

Les entreprises ont intérêt à rédiger des chartes sur l'utilisation d'Internet, elles sont de plus en plus nombreuses à le faire. Les avantages pour l'employeur se traduisent en terme de sécurité juridique et de responsabilité. Le salarié est informé sur ses droits et obligations sur son lieu de travail et sur les sanctions applicables. La charte apparaît comme un équilibre entre la préservation des droits légitimes de l'employeur et le droit au respect de la vie privée du salarié. Elle doit être connue de tous les salariés.

L'Arrêt de la Cour d'appel d'Aix en Provence (13/03/2006) est à cet égard intéressant en reconnaissant la responsabilité civile de l'employeur.

http://www.legalis.net/breves-article.php3?id_article=1611

Certaines chartes ne sont que de simples conseils à destination des salariés, d'autres prennent la forme d'annexe au règlement intérieur ; elles sont à privilégier car le règlement intérieur possède une valeur juridique que ne possède pas la simple charte d'utilisation : en effet, le contrat de travail signé entre les deux parties se réfère au règlement intérieur et peut entraîner la prononciation de sanctions effectives en cas de non-respect des règles fixées.

Toute charte devrait informer au minimum sur les règles d'utilisation d'Internet et du mèl, la sécurité du réseau et les procédures de surveillance mises en place, le respect des droits de la propriété intellectuelle, les droits des salariés sur leurs données personnelles et le respect de leur vie privée.
Le document doit être clair, lisible et surtout compréhensible pour un salarié non spécialiste en informatique.
La rédaction d'une charte s'avère essentielle en cas d'intégration de personnel extérieur à l'entreprise (salariés d'un prestataire, stagiaires) et lorsque les outils technologiques mobiles sont largement utilisés (ordinateurs portables, clef USB par exemple). Une neutralité de rédaction est conseillée afin que la charte soit pérenne en cas d'évolution technologique.

Il est donc nécessaire de :

- Veiller à la mise en conformité réglementaire des différents traitements existants de données personnelles,
- Veiller à la sécurisation juridique des contrats de travail (surtout pour les salariés nomades)
- Veiller à la mise en place ou à la refonte de la charte informatique en collaboration avec les différentes directions et avec une présentation au comité d'entreprise.
- Sensibiliser les salariés

La loi Informatique et Libertés modifiée le 6 août 2004 prévoit la nomination d'un correspondant Informatique et Libertés dans les entreprises qui est chargé du respect de la loi sur la protection des données personnelles. Celui-ci aura un rôle essentiel en matière de l'application des règles sur la cybersurveillance qui devra être intégré dans la charte sur l'usage des NTIC.

Le rôle du correspondant informatique et libertés :
http://www.cnil.fr/index.php?id=1821

La problématique de la cybersurveillance se révèle d'autant plus d'actualité que l'évolution technologique est très rapide.
Plus que jamais, à l'heure de l'essor dans la société des techniques biométriques et alors que les espaces public et privé sur Internet s'interpénètrent de plus en plus, la bonne utilisation des outils de nouvelles technologies de l'information doit faire l'objet d'une vigilance particulière.

Actualisé en novembre 2010