Au sommaire

Des salariés en libertés surveillées

Au-delà d'Internet, nombre de technologies (vidéosurveillance, biométrie et géolocalisation) posent la question de la place des libertés individuelles dans le champ professionnel, mais aussi celle de la responsabilité des employeurs pour des actes commis par leurs salariés.

L'essentiel

1 **La Cnil veille au respect de la réglementation des techniques** qui engendrent le recueil de données personnelles.

2 Les technologies introduites **sont des outils de sécurisation et de productivité.**

3 L'usage d'Internet sur le lieu de travail **est présumé professionnel.**

Vidéosurveillance, biométrie, géolocalisation, Internet, les nouvelles technologies se multiplient en entreprise. Simultanément, elles introduisent des dispositifs de contrôle des salariés, même si ce n'est pas leur objectif premier. En tout état de cause, elles amènent les employeurs à enregistrer de nombreuses informations à caractère personnel sur leurs salariés, protégées par la loi informatique et libertés (1). Alors, faut-il tomber dans la paranoïa Big Brother ? Pas sûr. La géolocalisation, par exemple, présente un réel intérêt en termes d'organisation des tournées de techniciens, d'économie de carburant et de sécurité en cas de vols. « Même si, au départ, cette technologie a été mal vécue par des conducteurs de camions habitués à la liberté, c'est aussi un moyen d'être moins isolé de sa base en cas d'agression. Et les dérapages sont un épiphénomène », estime Maxime Dumont, secrétaire général de la FGTE-CFDT (Fédération générale des transports et de l'équipement). Franck Gaulin, délégué syndical CGT de Carrefour, se souvient, lui, des pratiques occultes du distributeur, révélées par l'émission *Pièces à conviction*, sur France 3, le 20 janvier 2006. L'entreprise avait employé un agent de sécurité pour espionner les salariés, notamment en dissimulant des caméras. « Il faudrait avoir la certitude que les caméras non déclarées sont une pratique révolue », dit-il, sceptique.

« La principale dérive est d'implanter une technologie ayant pour but de surveiller les personnes à leur insu, ou de l'utiliser pour un objectif non annoncé au départ »

Une vie privée « résiduelle »

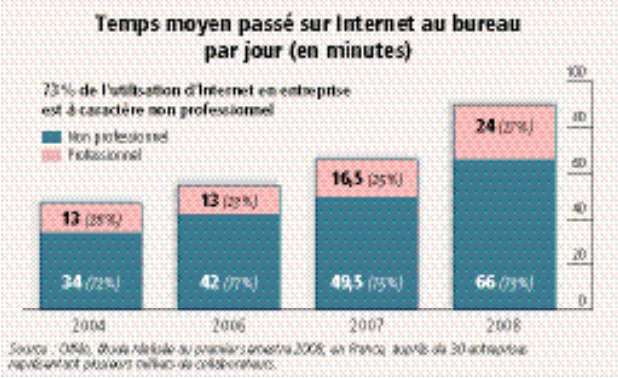
La vie privée existe pourtant en entreprise, mais elle est « résiduelle », souligne Eric Barbry, avocat au cabinet Alain Bensoussan. Comment la concilier avec le devoir de contrôle de l'employeur sur l'activité des salariés ? S'agissant de l'usage d'Internet au bureau, la plupart des entreprises ont, aujourd'hui, formalisé une règle du jeu, introduite dans une charte Internet, qui est une extension du règlement intérieur (lire p. 25). « L'employeur peut limiter les accès de ses collaborateurs à Internet, et il y a même fortement intérêt, prévient Eric Barbry. En effet, sa responsabilité peut être engagée, à la fois civilement et pénalement, pour des actes commis par ses collaborateurs, comme, par exemple, le surf sur des sites pédophiles. »

Filtrage d'URL

La solution ? « Le filtrage d'URL (adresses Internet, *NDLR*), qui permet d'exclure d'emblée les sites illicites et d'affiner les interdits en fonction des problématiques de l'entreprise », préconise-t-il. Ce que propose, par exemple, l'éditeur français Olfeo, ou l'américain Websense. Des solutions qui devraient encore davantage retenir l'intérêt des employeurs après le vote de la loi Hadopi et de ses dispositions sur le téléchargement de fichiers illégaux.
Plus généralement, avant d'introduire une nouvelle technologie, quelques grands principes doivent être respectés par les entreprises, parmi lesquels l'information préalable des salariés. « La principale dérive est d'implanter une technologie permettant de surveiller les personnes, sans les avertir ou sans qu'elles sachent à quoi elle sert, ou bien de l'utiliser pour un objectif qui n'était pas annoncé au départ », souligne Ariane Mole, avocate associée au cabinet Bird & Bird. L'employeur doit également prévoir une information-consultation préalable du comité d'entreprise.

Déclaration

De plus, toute technique qui aboutit au recueil de données personnelles fait l'objet d'une déclaration à la



Cnil (lire encadré ci-dessous). « Beaucoup d'entreprises, à l'exclusion des grandes, ne savent pas qu'il faut faire ces déclarations avant même la mise en place des dispositifs », remarque Florence Chafiol Chaumont, avocate au cabinet August & Debouzy. L'employeur peut recourir à deux formules : déclaration simple ou normale. Avec la première, il s'engage à se conformer strictement aux normes établies par l'institution ; avec la seconde, il s'autorise à ne pas suivre ces normes : « Il s'agit d'ailleurs d'un choix stratégique puisque la déclaration normale lui donne une marge de manœuvre beaucoup plus importante que la déclaration simplifiée », précise Ariane Mole.

Question de la preuve

Les conséquences d'un défaut d'information ou de déclaration peuvent être préjudiciables. « La question la plus douloureuse pour un employeur est celle de la preuve. S'il présente une vidéo démontrant la faute lourde d'un salarié, et qu'il a omis de déclarer son installation à la Cnil, sa preuve sera non seulement irrecevable, mais il risque aussi de très lourdes sanctions pénales », rappelle Jean-Emmanuel Ray, professeur à Paris 1-Sorbonne. L'article 226-16 du Code pénal prévoit que les manquements aux obligations de déclaration sont punis par une peine d'emprisonnement pouvant aller jusqu'à cinq ans et une amende de 300 000 euros.

Mais la Cnil agit davantage sur le registre de la pédagogie que sur celui de la répression. Lorsqu'elle reçoit une plainte, elle écrit à l'entreprise ou à l'administration concernée pour lui demander une réponse, dans un certain délai. « Les sanctions ne sont pas fréquentes, car, en général, le responsable du traitement se met en conformité », indique Norbert Fort, chef du service des plaintes. En revanche, la Cnil reçoit de plus en plus de plaintes liées à la vidéosurveillance (une croissance de 43 % en 2008) : sur 200 plaintes en 2008, près de 100 concernaient des lieux de travail.

Technologies intrusives

Autre exigence liée à l'usage de technologies intrusives : tout matériel installé doit avoir une finalité précise, un « usage déterminé et légitime », précise la Cnil (2). Par exemple, la géolocalisation peut servir à assurer la sécurité des personnes ou des marchandises transportées ; une meilleure gestion des personnels et des véhicules dispersés ; le suivi et la facturation d'une prestation ; le suivi du temps de travail des employés quand il ne peut pas être réalisé par d'autres moyens. A l'inverse, ce procédé ne peut pas être justifié pour des VRP ou des visiteurs médicaux, qui sont libres dans l'organisation de leurs déplacements. Enfin, pour éviter un contrôle permanent, la Cnil recommande la désactivation du système en dehors des horaires de travail, pour les véhicules de fonction.

En plus d'un objectif précis, le dispositif installé doit respecter un principe de proportionnalité. Illustration : « La mise sous vidéosurveillance permanente d'un poste de travail ne pourrait intervenir qu'en cas de risque particulier et dûment avéré pour la sécurité du salarié concerné », explique la Cnil. « Attention à l'emplacement et à l'orientation des caméras, insiste Norbert Fort. Sauf rares exceptions, il n'est pas nécessaire qu'elles filment les bureaux, les couloirs et encore moins les vestiaires et les lieux de pause. » *Idem* pour la biométrie : l'accès à des locaux contrôlé par les empreintes digitales ne peut se justifier que par un fort impératif de sécurité. La Cnil est particulièrement vigilante sur ce procédé, qui touche à des caractéristiques physiques : « Il faut obtenir une autorisation expresse et un défaut de réponse dans les deux mois équivaut à un refus, explique Ariane Mole. Elle distingue les biométries sans traces, comme celles qui reposent sur la reconnaissance du contour

« Tout matériel installé doit avoir une finalité précise, un "usage déterminé et légitime" »

Quelles déclarations à la Cnil ?

Biométrie	Autorisation.
Géolocalisation	Déclaration simplifiée si le dispositif est conforme aux conditions énoncées par la Cnil dans sa norme simplifiée n°51 (par exemple : durée de conservation, liste des données enregistrées). Ou déclaration normale si l'employeur décide de ne pas se conformer à la norme simplifiée n°51.
Internet	Déclaration normale lorsque l'entreprise met en place un dispositif de contrôle individuel des salariés afin de produire un relevé des connexions ou des sites visités, poste par poste.
Vidéosurveillance	**Lieu privé** (non ouvert au public) : une déclaration normale auprès de la Cnil est requise quand les images sont enregistrées ou conservées dans des traitements qui permettent d'identifier des personnes. **Lieu public ou ouvert au public :** une autorisation préfectorale est nécessaire. **Lieu mixte :** pour la Cnil, le régime juridique « n'est pas clair », la question du cumul des deux déclarations se pose. Elle milite pour sa compétence unique dans son dernier rapport annuel 2008.

A noter : lorsque l'entreprise désigne un Cil (correspondant informatique et libertés), elle est dispensée des procédures de déclaration, mais pas des demandes d'autorisation.

de la main ou du réseau veineux et qui ne peuvent s'effectuer à l'insu des personnes, et les biométries avec traces, comme les empreintes digitales, qui laissent des marques sur tous les objets touchés et sont donc facilement capturables. » Elle juge l'utilisation de l'empreinte digitale totalement disproportionnée pour un système de contrôle du temps de travail des salariés, et lui préfère la volumétrie de la main (lire p. 30).

Confidentialité

L'employeur qui collecte des données personnelles doit en assurer la sécurité et la confidentialité. C'est pour cette raison que chaque salarié doit disposer d'un mot de passe individuel régulièrement changé. Et ces données ne peuvent être consultées que par les personnes habilitées, à savoir les administrateurs réseaux pour les données de connexion à Internet. En outre, les informations recueillies sont conservées pour une durée limitée, un mois pour les enregistrements de vidéosurveillance par exemple. On est loin de la licence "perpétuelle" à laquelle Facebook a dû renoncer en ce début d'année. Mais le débat n'en est pas moins révélateur. Les entreprises commencent à réfléchir à leur façon de "gérer" les réseaux sociaux. A l'instar de Patrick Langrand, responsable de la sécurité des systèmes d'information du groupe La Poste, qui signale que l'entreprise va bientôt « trancher sur l'autorisation de l'usage des réseaux sociaux ». ■

VIRGINIE LEBLANC

(1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

(2) *Guide pour les employeurs et les salariés*, accessible sur le site de la Cnil, <www.cnil.fr.>

JURISPRUDENCE

Internet : un usage toléré sous conditions

Les limites sont aujourd'hui bien tracées. Des dispositions protègent les employeurs et leurs salariés, tout comme elles admettent l'usage extraprofessionnel du matériel de l'entreprise. A condition de ne pas franchir la ligne jaune.

L'arrêt Nikon de 2001 avait donné le ton : le salarié a droit au respect de sa vie privée au travail, notamment en ce qui concerne les messages électroniques qu'il émet et reçoit sur son poste. Point de salut, donc, pour les employeurs trop curieux et intrusifs. Les juges ont, depuis, non pas fait machine arrière mais assoupli leur propos. « Ainsi, dans divers arrêts et, notamment, celui du 9 juillet 2008, la Cour de cassation confirme la présomption du caractère professionnel des fichiers informatiques, des connexions Internet et des messages électroniques sur le lieu de travail, sauf mention contraire. C'est tout simplement l'indication "personnel" dans l'objet du courrier envoyé », introduit Cyril Catté, avocat au cabinet parisien Gibier, Souchon, Festivi, Rivierre. En clair, elle admet que les salariés peuvent envoyer des mails sans lien avec leur activité professionnelle. En matière de connexion, cette indulgence est également de mise. « L'accès à Internet constitue, comme l'a rappelé le Conseil constitutionnel, le 10 juin 2009, une liberté fondamentale », souligne Agnès Cloarec-Mérendon, avocate au cabinet Latham & Watkins.

Information individuelle

Il est toujours possible de passer outre. Mais attention, il faut y mettre les formes, comme le précise l'avocate : « Sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier, ou celui-ci dûment appelé, selon l'arrêt du 17 mai 2005, baptisé "Cathnet Science". » La surveillance en tant que telle doit faire l'objet d'une information individuelle aux salariés et d'une autre, collective, aux représentants du personnel, sans oublier les déclarations à la Cnil.

Requête au TGI

A cela s'ajoute une procédure très lourde pour ceux qui veulent accéder à la consultation des mails dits personnels. « Il faut, en effet, que l'employeur fasse une requête au TGI en justifiant son propos par un motif légitime. Le tribunal mandatera, ensuite, un huissier », décrit Isabelle Ayache-Revah, avocate associée au cabinet Raphaël. Parfois, le jeu en vaut la chandelle, comme le suggère la décision de 2008 des juges dans l'affaire Mediasystem. « Ils ont considéré que le respect de la vie personnelle du salarié ne constitue pas un obstacle quand l'employeur a des raisons légitimes et sérieuses de craindre que l'ordinateur mis à la disposition de l'intéressé ait été utilisé pour favoriser des actes de

concurrence déloyale », explique Matthias Rubner, avocat au cabinet Latham & Watkins. Autrement dit, si la loi et les différentes décisions de justice tendent à protéger les salariés, elles sont également protectrices à l'égard de l'employeur abusé. Deux récents exemples sont assez parlants. Le premier date du 18 mars 2009 et met en scène un salarié à qui l'employeur reproche d'avoir navigué 41 heures sur Internet pour raisons personnelles, et ce, au cours d'un seul mois. La Cour de cassation a validé son licenciement pour faute grave. Le second concerne le licenciement, en 2007, d'une salariée, confirmé par les prud'hommes d'Angers. Au cœur du sujet : l'envoi, en deux mois, de 156 mails purement personnels à partir de la messagerie de l'entreprise.

Notion d'abus

« Les juges ne reprochent plus uniquement la nature des sites ou des messages, mais la fréquence et le volume. C'est une nouvelle approche de l'abus », note Marion Ayadi, avocate associée au cabinet Raphaël, qui évoque sur ce point les arrêts d'avril 2003 et de juin 2004. Les juges avaient alors sanctionné deux salariés pour atteinte portée à l'image de marque et à la réputation de leur entreprise. Le premier avait associé le nom de cette dernière à des activités à caractère pornographique ou échangiste ; le second, à des propos antisémites, dans les deux cas *via* l'utilisation de leur adresse électronique. Dernièrement, un licenciement, évoqué par Matthias Rubner, a été confirmé par la cour d'appel de Limoges après l'utilisation abusive de la messagerie électronique professionnelle par un salarié pour l'envoi de mails à de nombreux collègues afin de les inciter à intenter une action prud'homale. « Les juridictions concluent alors à un détournement de l'usage qui peut même être qualifié d'abus de confiance », précise Cyril Catté. Tout est toujours une question de proportion et de loyauté. ■

CÉLINE LACOURCELLE