LeJournaldunet

Cybersurveillance du salarié : ce qui change

Un récent jugement précise la jurisprudence en matière de surveillance de l'utilisation des moyens informatiques par les salariés. Les droits de l'employeur s'en trouvent renforcés. Le point.
(04/08/2008)

Sept ans après l'arrêt Nikon, la jurisprudence précise désormais les limites de "la vie privée informatique" du salarié pendant son temps de travail face au pouvoir de contrôle de l'employeur. En 2001, la Cour de Cassation avait en effet consacré le droit du salarié au respect de l'intimité de sa vie privée, même pendant le temps et au lieu de travail, s'agissant en particulier de l'utilisation personnelle des outils informatiques professionnels mis à disposition par l'employeur : ordinateur, connexion Internet, messagerie. L'employeur ne pouvait accéder au contenu de la messagerie du salarié sans violer le secret des correspondances qui en découle ; il ne pouvait pas non plus interdire toute utilisation personnelle de ces outils informatiques professionnels.

Par la suite, la jurisprudence a, à plusieurs reprises, précisé les contours de ce droit à la vie privée, souvent dans un sens favorable au salarié. Aujourd'hui, les tribunaux opèrent un rééquilibrage au profit de l'employeur, notamment dans des situations d'abus manifeste des premiers. Ainsi les dossiers, fichiers se sont vu reconnaître récemment une présomption de caractère professionnel, rendant possible un accès libre par l'employeur (voir partie 1). De même, un arrêt important de la Cour de Cassation du 9 juillet 2008 vient juste de reconnaître une telle présomption s'agissant de l'usage de la connexion Internet de l'entreprise par le salarié (voir partie 2). Retour sur ces dernières évolutions.

1. Les dossiers, fichiers, emails du salarié sont présumés être professionnels

Suite à l'arrêt Nikon (Soc. 2 Octobre 2001), une distinction était apparue : les dossiers, fichiers et emails comportant la mention "personnel" étaient soustraits du pouvoir de contrôle de l'employeur, ceux qui ne l'arboraient pas le demeuraient. Cette pratique pouvait aboutir à des dérives, certains salariés dissimulant sous cette mention des photos érotiques ou encore des informations confidentielles qu'ils transmettaient à des concurrents. Le préjudice pour l'employeur était alors énorme puisque du fait de cette mention, il ne pouvait rien faire.

C'est ainsi que dans un arrêt du 17 mai 2005 "Cathnet-Science", la Cour de Cassation condamnait un employeur qui avait accédé à un fichier "personnel" de son salarié contenant des photos "torrides", invalidant le licenciement pour faute grave fondé sur cette base. Implicitement, cette décision reconnaissait cependant que l'employeur pouvait ouvrir les fichiers "personnels" du salarié soit "en sa présence ou celui-ci dûment appelé", soit hors sa présence et sans que celui-ci n'ait été prévenu, "en cas de risque ou d'événement particulier". Reste à définir ce qui peut constituer un tel risque ou événement particulier...

Par deux arrêts rendus le 18 octobre 2006, la Cour de cassation s'est montrée plus explicite sur le pouvoir de contrôle de l'employeur :

- Dans la première affaire, elle considère que "**les documents** détenus par le salarié dans le bureau de l'entreprise mis à sa disposition sont, sauf lorsqu'il les identifie comme étant personnels, **présumés avoir un caractère professionnel**, en sorte que **l'employeur peut y avoir accès hors sa présence**".
- Dans la seconde affaire, elle précise que "**les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par**

l'employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel, de sorte que l'employeur peut y avoir accès hors sa présence". Elle tire également une circonstance aggravante du fait du cryptage délibéré par le salarié de son poste informatique "**sans autorisation de la société faisant ainsi obstacle à la consultation**". "Ce comportement du salarié qui avait déjà fait l'objet d'une mise en garde au sujet des manipulations sur l'ordinateur, rendait impossible le maintien des relations contractuelles pendant la durée du préavis et constituait une faute grave". Ainsi est clairement affirmé le droit légitime de l'employeur d'accéder à TOUS les documents du salarié, qu'ils soient électroniques ou pas ; ces documents sont présumés être professionnels, sauf lorsque figure la mention "personnel". Dans ce cas, il conviendra de se référer aux modalités d'accès définies par l'arrêt Cathnet-Science. Le pouvoir de contrôle de l'employeur même en l'absence du salarié en ressort conforté.

Toutefois l'identification du caractère privée des documents pourrait ne pas dépendre systématiquement de la seule apposition de la mention "personnel". Ainsi, si des documents présumés professionnels (donc sans mention) comportent une partie manifestement privée, sans qu'un abus du salarié ne puisse être reproché, l'employeur serait obligé de faire la part des choses entre la partie professionnelle (opposable) et la partie privée (non opposable car relevant de la vie privée du salarié). C'est le sens d'un jugement du TGI de Quimper du 17 juillet 08, condamnant le DGS d'une commune pour atteinte au secret des correspondances.

Cette solution est intimement liée aux faits très précis de l'affaire et il serait hâtif d'en tirer un principe, un appel ayant été formé. Une généralisation de cette solution jetterait cependant le trouble dans l'effort de simplification mené par la Cour de Cassation en consacrant la présomption de caractère professionnel des documents détenus par le salarié, et compliquerait d'avantage la tâche de l'employeur.

2. L'usage de la connexion Internet de l'entreprise est présumé être professionnel

S'il est aisé d'identifier un fichier ou un message comme étant personnel, la question d'un usage personnel de la connexion Internet de l'entreprise est plus délicate. En 2001, l'arrêt Nikon avait invalidé toute interdiction par l'employeur d'une utilisation personnelle de l'ordinateur mis à disposition : en vertu de son droit à la vie privée même au temps et au lieu de travail, le salarié peut utiliser l'outil informatique professionnel à des fins personnelles, comme il peut passer des appels téléphoniques privés ou réaliser des photocopies pour ses besoins propres. Cela inclut la connexion Internet de l'entreprise et donc une navigation privée du salarié.

Pour autant, cette sphère de vie privée au travail couvre t-elle tout type de navigation de la part du salarié ?

Dans l'arrêt Nortel, la Chambre criminelle de la Cour de Cassation a considéré qu'un salarié qui pendant son temps de travail et à partir de la connexion Internet de l'entreprise :
- visitait des sites échangistes et pornographiques,
- alimentait son propre site échangiste et pornographique,
- utilisait sa messagerie professionnelle pour envoyer et recevoir des messages sur des thèmes sexuels ou des propositions échangistes,
- avait détourné son ordinateur et la connexion Internet de l'usage pour lequel ils avaient été mis à sa disposition,
se rendait coupable de l'infraction pénale d'abus de confiance (Crim 19 mai 2004, Nortel).

Toute navigation ne pourra donc pas être protégée par le droit à la vie privée du salarié. Comme pour le téléphone ou les photocopies, l'utilisation privée de la connexion Internet de l'entreprise doit rester **raisonnable**, le salarié étant tenu d'une obligation de loyauté vis-à-vis de son employeur (article L 120-4 du Code du Travail). En cas d'abus, la sanction s'en trouverait justifiée.

Plus récemment, la Chambre sociale de la Cour de Cassation vient de juger le 9 juillet 2008 que "les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail **sont présumées avoir un caractère professionnel, de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence**" (Soc. 9 juillet 2008, Entreprise Martin).

Cet arrêt généralise donc le droit d'accès de l'employeur sur l'historique de navigation de chaque salarié, ainsi que son pouvoir quasi inquisitoire de rechercher si le salarié a effectivement fait une utilisation raisonnable de la connexion mise à sa disposition.

Comment alors considérer si une navigation est abusive ou non ? Si le caractère abusif ne fait aucun doute s'agissant de la consultation de sites pornographiques, quid des autres sites n'ayant pas de lien direct avec les missions du salarié et dont le contenu n'est manifestement pas répréhensible (messagerie personnelle, site communautaires, site d'informations diverses...) ? De toute évidence, le temps de visite passé sur chaque site sera déterminant pour apprécier s'il y a abus ou pas ; une déclaration CNIL sera indispensable en cas de relevé nominatif des connexions, à côté des autres principes de discussion collective, transparence et proportionnalité préalables à la mise en place de toute cybersurveillance*. Enfin, doit-on déduire que la responsabilité de l'administrateur réseau ne serait pas engagée s'il fournit l'historique de navigation d'un salarié sur demande de l'employeur, compte tenu de la reconnaissance jurisprudentielle du pouvoir d'inspection de ce dernier ?

Avec autant d'interrogations, la charte informatique revêt alors un rôle crucial surtout lorsqu'elle sera annexée au règlement intérieur de l'entreprise : c'est elle qui fixe les règles du jeu. En cas de conflit, c'est à elle qu'on fera référence en priorité.

Conclusion

Après la reconnaissance d'un droit à la vie privée informatique du salarié, voici maintenant la confirmation explicite d'un égal droit d'accès de l'employeur. Certes, ce droit d'accès continue à être limité par l'apposition de la mention "personnel" sur tous documents détenus pas le salarié, mais il est difficile d'apposer une telle mention sur ses connexions Internet. Le havre de la vie privée succombe alors au profit de l'employeur dans des situations d'abus manifestes qu'il appartiendra d'apprécier au cas par cas. Nul doute que la charte informatique continuera de jouer un rôle déterminant dans cette tâche délicate.

* Voir sur ce point notre précédente publication dans le magazine Réunion Multimédia : La cybersurveillance du salarié dans l'entreprise : quels risques pour quels enjeux, 2005

Sulliman Omarjee

Lancer l'impression