Le point sur…

Nouvelles technologies et salariés : que faut-il faire ?

Les nouvelles technologies sont chaque jour plus présentes dans l'univers du travail, ce qui ne manque pas de soulever de nombreuses questions sur les conditions de leur utilisation par les employeurs comme par les salariés.

Interview d'Alain Bensoussan

Grâce à internet et à la messagerie électronique, les salariés peuvent occuper une partie de leur temps de travail à des fins purement personnelles. En ont-ils le droit ?

La Cour de cassation a consacré depuis son célèbre arrêt Nikon du 2 octobre 2001 le droit de tout salarié à une vie privée « résiduelle » sur le lieu de travail. Chaque salarié se voit reconnaître pendant son temps de travail la possibilité, par exemple, d'envoyer des méls personnels, de passer des coups de téléphone à ses proches, ou encore de stocker sur son ordinateur des photos de famille. A condition de ne pas en abuser.

Quelles précautions prendre pour marquer la limite entre le droit à la vie privée résiduelle et l'abus pouvant naître de l'exercice de ce droit ?

Le mieux, selon nous, est de fixer au travers d'une « charte d'utilisation » les modalités selon lesquelles s'exercera le droit à la vie privée résiduelle. Communiquée à chaque salarié, cette charte précisera les conditions normales d'utilisation du matériel informatique mis à la disposition du personnel, la façon dont s'exercera le droit à la vie privée résiduelle, les moyens de contrôle mis en œuvre pour s'assurer de l'absence d'abus et, enfin, les conséquences du non-respect de la charte (Informatique et libertés, Editions Francis Lefebvre, préface d'Alex Türk, février 2008 n°s 6940 s.).

L'employeur court-il des risques s'il ne fixe pas de telles règles ?

Si l'employeur ne fixe pas d'emblée les « règles du jeu », il lui sera difficile de reprocher à un salarié une utilisation abusive de son ordinateur professionnel. Le droit à la vie privée résiduelle est un acquis de l'arrêt Nikon qui ne souffre aucune discussion. Ce sont les limites de ce droit qui sont entourées de flou. A l'employeur de lever ce flou, de préférence au travers de cette charte d'utilisation. Faute de quoi le salarié pourrait lui opposer l'incertitude dans laquelle il a été laissé sur ce qui lui était ou non permis.

Si comme vous le préconisez une charte d'utilisation définit l'expression du droit à la vie privée résiduelle, dans quelles conditions l'employeur peut-il ensuite consulter les méls et fichiers stockés sur l'ordinateur de l'un de ses salariés ?

La Cour de cassation pose ici une présomption : « les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son 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 » (Cass. soc. 18-10-2006 n°s 04-48.025 et 04-47.400 : RJS 12/06 n° 1241).
Si le caractère privé d'un mél ou d'un fichier ne fait pas de doute, l'employeur ne peut pas le consulter, sauf à violer le secret des correspondances ou la vie privée, violation dans les deux cas pénalement sanctionnée.
Si le document mentionne qu'il est privé mais que l'employeur a un doute sur sa véritable nature, il doit convoquer le salarié et ouvrir le fichier en sa présence. La présence lors du contrôle d'un représentant du personnel est recommandée car elle permettra à l'employeur de démontrer que les droits du salarié ont été préservés.
Mais même en présence du salarié voire d'un représentant du personnel, les risques de contestation existent. Pour limiter de telles contestations, l'employeur peut préférer saisir le juge afin qu'un huissier de justice soit désigné pour procéder aux investigations nécessaires et constater les faits, sans que le salarié en ait été préalablement informé (CPC art. 145). Cette procédure a le double mérite d'être rapide, l'autorisation du juge pouvant être obtenue dans la journée, et de préserver l'effet de surprise, qui est primordial.

De telles précautions sont-elles toujours vraiment nécessaires ?

La Cour de cassation admet que l'urgence puisse justifier que l'employeur consulte sans aucun formalisme préalable le contenu de l'ordinateur d'un salarié, y compris les fichiers identifiés comme personnels de celui-

ci. Une telle urgence doit selon nous être strictement entendue : la démarche de l'employeur doit se fonder sur le risque d'une perte imminente des preuves du comportement déloyal du salarié, par exemple si ce dernier a effectué une opération illicite dont les traces sont sur le point de disparaître. Il s'agit dans tous les cas de concilier, d'une part, les intérêts légitimes de l'entreprise, d'autre part, la sphère d'intimité à laquelle le salarié peut prétendre, y compris sur son lieu de travail. Et si l'on peut saluer la solution équilibrée qui se dégage des décisions de justice rendues en la matière, une intervention du législateur permettrait de clarifier davantage les règles applicables, dans l'intérêt des employeurs comme des salariés.

Nous venons de voir que l'employeur pouvait sous certaines conditions accéder à l'ordinateur professionnel du salarié. Mais que faire si ce dernier a protégé l'ordinateur ou certains de ses contenus avec un mot de passe ?

Dans son rapport de février 2002, la Cnil rappelle que « l'ordinateur mis à la disposition du salarié peut être protégé par un mot de passe ou un login, mais cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers ; elle n'a pas pour effet de transformer l'ordinateur de l'entreprise en un ordinateur privé ».

L'ordinateur reste la propriété de l'employeur ; il est mis à disposition du personnel pour l'exercice de son activité professionnelle, et les documents, fichiers et messages électroniques qui y sont stockés sont présumés être professionnels. L'employeur doit donc pouvoir y accéder et le salarié est tenu de lui communiquer les éventuels mots de passe permettant un tel accès. La Cour de cassation a ainsi jugé qu'un salarié en arrêt maladie qui refusait de communiquer à l'employeur le mot de passe de son ordinateur professionnel, bloquant ce faisant le fonctionnement de l'entreprise, commettait une faute pouvant justifier son licenciement (Cass. soc. 18-3-2003 n° 01-41.343 : RJS 6/03 n° 723). Dans son arrêt précité du 18 octobre 2006, la Cour de cassation a jugé dans le même sens que le licenciement pour faute grave d'un salarié était justifié dès lors que celui-ci avait volontairement procédé au cryptage de son poste informatique, sans l'autorisation de l'employeur, ce qui avait empêché ce dernier d'accéder aux dossiers professionnels stockés dans l'ordinateur.

La navigation sur internet à des fins personnelles est, elle aussi, source d'abus. Comment l'employeur peut-il lutter contre de tels abus ?

L'employeur peut d'abord limiter le risque en mettant en place un système de filtrage qui empêchera techniquement les salariés d'accéder à certains sites internet. Mais il doit respecter le principe de transparence : avant de mettre en place un tel filtrage, l'employeur doit consulter les représentants du personnel, s'il y en a, et informer individuellement chaque salarié, par exemple par le biais de la charte d'utilisation que nous avons évoquée.

Il est aussi possible de contrôler l'usage d'internet en mettant en place un dispositif de cybersurveillance qui permette de vérifier tous les sites consultés par les salariés et de conserver les logs de connexion. La mise en place d'un tel dispositif est soumise à déclaration préalable auprès de la Cnil (Informatique et libertés nos 6940 s.). Il faut là aussi que l'employeur consulte au préalable les représentants du personnel et informe chaque salarié des moyens de contrôle mis en œuvre.

Et le téléphone ? De quels moyens dispose l'employeur pour contrôler son absence d'utilisation abusive à des fins personnelles ?

Les autocommutateurs téléphoniques sont des standards téléphoniques qui permettent notamment d'orienter les appels entrants et sortants de l'entreprise. Ils peuvent aussi enregistrer les numéros de téléphone composés par les salariés à partir de leur poste de travail et la durée de leurs conversations téléphoniques. Il s'agit donc d'un moyen permettant de révéler un usage personnel abusif du téléphone qui, en tant que tel, doit être déclaré à la Cnil conformément à la norme simplifiée établie par celle-ci (Délibération 2005-19 du 3-2-2005). L'employeur doit aussi consulter les représentants du personnel et informer chaque salarié avant la mise en œuvre de ce dispositif de contrôle. Si toutefois l'autocommutateur est utilisé, non pas pour surveiller l'activité des salariés, mais comme un outil de rationalisation des coûts (comptabilisation statistique des flux entrants et sortants au niveau de l'organisation, d'un service ou d'un poste particulier), sans porter sur des données à caractère personnel (quatre derniers numéros de téléphone occultés), il semble que l'existence du dispositif n'ait pas à être préalablement portée à la connaissance du salarié. La Cour de cassation a en effet jugé que la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste édités au moyen de l'autocommutateur téléphonique de l'entreprise ne constitue pas un procédé de surveillance illicite pour n'avoir pas été préalablement porté à la connaissance du salarié (Cass. soc. 29-1-2008 n° 06-45.279 : RJS 5/08 n° 511).

Qu'est-ce que le « correspondant informatique et libertés ». Pouvez-vous nous en dire davantage ?

Chaque entreprise ou organisation peut désigner un correspondant informatique et libertés (CIL).

Facultative, cette désignation permet d'alléger les formalités déclaratives qu'impliquent les traitements de données à caractère personnel. L'entreprise est dispensée de déclaration, sauf pour les traitements soumis à autorisation et les flux transfrontières de données. En contrepartie, le CIL doit établir dans les trois mois de sa désignation la liste exhaustive des traitements mis en œuvre au sein de son entreprise, faire un bilan annuel d'activité et, surtout, veiller à la bonne application de la loi Informatique et libertés dans son entreprise.
La création du CIL constitue une avancée majeure qui doit permettre d'assurer le nécessaire équilibre entre le développement des usages nominatifs des données informatisées et le respect de l'intimité « binaire » de chaque individu.

Un regret tout de même. Lorsque plus de 50 personnes sont chargées de mettre en œuvre les traitements de données ou y ont directement accès, l'organisation qui souhaite avoir un CIL doit en principe le désigner parmi ses membres. Ce n'est qu'en deçà de ce seuil que l'organisation peut désigner un correspondant extérieur à celle-ci. Le seuil de 50 salariés me semble trop bas. Son relèvement permettrait de développer la présence des CIL dans le monde du travail. Mais aussi de garantir au mieux leur compétence avec l'espoir, à terme, que voie le jour un nouveau corps de professionnels, spécialistes de l'informatique et des libertés, les commissaires aux données.