

Surfer au bureau ?

Notre compatriote du Puy-de-Dôme, Florence Gladel, avocat à la Cour, traite un sujet juridique dans un domaine en plein essor. La récente discussion au Parlement sur la "licence globale" montre la difficulté de concilier le droit traditionnel et les technologies nouvelles.

La surveillance et le contrôle des salariés sur le lieu et pendant le temps de travail sont des prérogatives reconnues à l'employeur. Elles découlent directement du contrat de travail et plus spécialement du lien de subordination.

L'introduction des nouvelles technologies de l'information et de la communication (NTIC) dans le monde du travail engendre des difficultés pour l'employeur. En effet, l'utilisation d'Internet ou de l'Intranet par les salariés expose les entreprises à certains risques. Par exemple, des risques directement préjudiciables à la bonne marche de l'entreprise :

- le salarié émet des informations confidentielles relatives à la société, et l'Internet provoque une diffusion massive et non contrôlée ;
- le salarié divulgue ses codes d'accès personnels, à des tiers non autorisés qui peuvent ainsi bénéficier d'informations confidentielles, voire intervenir dans la gestion (prise de commandes, stocks, sécurité, etc.).



Mais il existe aussi des risques qui mettent en cause l'image de marque de l'entreprise et ses rapports avec autrui, par exemple :

- réception par le salarié d'éléments protégés (droits d'auteurs) et copiés sans autorisation ;
- connexion du salarié à des sites illicites (violents, pornographiques, pédophiles ou racistes) ;

- actions de nature à porter atteinte au bon fonctionnement de l'Internet (virus, etc.).

L'employeur doit donc légitimement réglementer le fonctionnement et l'utilisation d'Internet et de l'Intranet pour éviter tout abus. Ce contrôle doit se faire dans le respect de quelques principes, notamment : transparence, loyauté et proportionnalité.

Transparence

Les salariés doivent être informés de l'existence des procédés de contrôle les concernant, et ceci préalablement à leur mise en œuvre. A défaut d'une telle information, la prise de connaissance du contenu de messages électroniques à caractère personnel adressés ou reçus par les salariés sur le lieu de travail est constitutive du délit de violation du secret des correspondances et fait encourir à l'employeur des peines d'emprisonnement (un an) et d'amende (45.000 €).

Le comité d'entreprise doit être non seulement informé, mais aussi consulté, et ceci, préalablement à la décision de mise en œuvre du procédé de contrôle. Le défaut d'une telle consultation est constitutif du délit d'entrave et fait encourir à l'employeur des peines d'emprisonnement (un an) ou d'amende (3.750 €).

L'entreprise doit impérativement déclarer à la *Commission nationale de l'informatique et des libertés* (CNIL) les méthodes de contrôle (logiciels utilisés) ainsi que leurs évolutions. Le fait de procéder à des traitements automatisés d'informations nominatives, sans qu'aient été respectées les formalités préalables, fût-ce par négligence, est puni de trois ans d'emprisonnement et de 45.000 € d'amende. Ainsi, la Cour de cassation a jugé que, faute d'une déclaration préalable par l'entreprise, auprès de la CNIL, et alors même qu'il ne s'agissait que d'un système de badges géré par des moyens automatisés, il ne pouvait être reproché à un salarié de refuser de déférer à une exigence de son employeur.

Loyauté de la preuve

L'employeur peut contrôler son salarié, seul l'emploi de procédés clandestins est illicite. Cela concerne principalement la messagerie électronique. Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée et en particulier au secret de ses correspondances. L'employeur ne saurait, dès lors, prendre connaissance des messages personnels émis par le salarié ou reçus par lui grâce à l'outil informatique mis à sa disposition pour son travail, et cela, quand bien même l'utilisation non professionnelle de l'ordinateur aurait été interdite.

Toutefois, la cour d'appel de Paris a précisé que *"la préoccupation de la sécurité du réseau justifie que les administrateurs de réseaux informatiques fassent usage des possibilités techniques dont ils disposent pour mener à bien des investigations"*. Elle a donc considéré que la lecture et la retranscription de messages par les administrateurs de réseaux dans le but de régler les problèmes techniques ou de sécurité informatique ne peuvent être qualifiées d'interception illicite, dans la mesure où celles-ci *"ne nécessitent ni dérivation ou branchement et sont effectuées sans artifice ni stratagème"*.

Mais cette décision implique que les administrateurs réseaux qui peuvent prendre connaissance de l'ensemble des données reçues, émises ou élaborées par un salarié, ne peuvent utiliser le contenu de l'information ainsi trouvée quand cette divulgation porterait atteinte au secret des correspondances. Ils sont tenus à une obligation de confidentialité qui les empêche de divulguer à qui que ce soit au sein de l'entreprise, y compris à la hiérarchie, les informations personnelles relatives aux salariés et captées dans le cadre de leurs fonctions. A défaut, non seulement cela rendrait illicite et donc nul le moyen de preuve ainsi obtenu pour sanctionner le salarié, mais cela pourrait aussi engager leur responsabilité pénale ou celle de l'employeur.

Proportionnalité

La Cour européenne des droits de l'homme (CEDH), à la lecture de la *Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* ("*Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance*") a jugé que le salarié avait droit à la protection de l'intimité de sa vie privé dans le cadre de sa vie professionnelle. Le code du travail semble modérer ce principe en

disposant que *"nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché"*. Dès lors, une jurisprudence commence lentement à se constituer dessinant un équilibre subtil entre les droits de l'employeur et ceux du salarié, entre la vie professionnelle et la vie privée.

Si la chambre sociale de la Cour de cassation interdit à l'employeur de prendre connaissance des messages personnels émis ou reçus par le salarié, en revanche la chambre criminelle de la même cour ne retient la violation de la correspondance que lorsqu'il s'agit d'un courrier privé. Le problème se pose donc pour les courriels ne contenant pas expressément la mention *"courrier personnel"*. Le problème en pratique est que ce n'est souvent qu'en prenant connaissance du courriel que l'on sait s'il est personnel ou professionnel.

En conséquence, par mesure de précaution, l'entreprise pourrait faire intervenir l'administrateur réseau afin qu'il prenne connaissance d'un message sans indication particulière et le requalifie éventuellement en message personnel. Mais il incombe au salarié de bien distinguer son courriel professionnel et son courriel personnel. Naturellement, la distinction exige l'engagement du salarié à ne pas qualifier de personnelles des informations professionnelles. Il est préconisé de mentionner cette obligation de bonne foi dans le règlement intérieur de l'entreprise.

La charte

La charte des technologies de l'information définit précisément les modalités d'utilisation des systèmes d'information et de communication au sein de l'entreprise, des accès à Internet, à l'Intranet, de la messagerie, etc. qui permettent d'alerter ou de sanctionner le salarié pour simple manque à cette Charte.

Une interdiction générale et absolue de toute utilisation de l'Internet à des fins autres que professionnelles paraît irréaliste et disproportionnés (rapport CNIL du 28 mars 2001). La charte pourrait préconiser, par exemple ...

- que l'usage d'Internet pour des connexions autres que professionnelles doit être raisonnable, ne pas amoindrir les conditions d'accès professionnel au réseau, et ne pas nuire à la productivité ;
- des interdictions de connexions à l'égard de sites particuliers (pornographie, négationnisme, jeu) ;

- des mesures de sécurité légitimes compte tenu des risques pour l'entreprise (contamination de virus, etc.), et notamment l'interdiction de se connecter à Internet via un modem autonome, de télécharger certains fichiers volumineux, de s'inscrire à des forums de discussion sans autorisation préalable, etc.

Dans de telles hypothèses, le contrôle a posteriori de l'usage fait par les salariés d'une telle tolérance peut être légitime (rapport CNIL du 28 mars 2001). Le manquement d'un salarié peut aussi être constaté sans que l'ouverture des fichiers et des messages personnels ne soit nécessaire.

Valeur juridique de la charte

La charte doit être conforme au règlement intérieur pour que ses prescriptions puissent conduire aux sanctions disciplinaires nécessaires, et le contrat de travail devra contenir une mention explicite sur elle. Elle doit être soumise pour avis au comité d'entreprise ou à défaut, à l'avis des délégués du personnel ainsi que, le cas échéant, à l'avis du comité d'hygiène et de sécurité. Elle doit également faire l'objet de publicité et être transmise à l'inspecteur du travail. Logiquement, la modification de ces règles doit s'effectuer suivant les mêmes modalités. Il est recommandé aux entreprises de demander aux salariés de signer individuellement la charte, notamment à ceux ayant accès à des données importantes pour l'entreprise.

Contrôles "à l'aveugle"

Le contrôle technique effectué par l'administrateur de réseau fait partie du fonctionnement normal du système d'information de l'entreprise. Cette dernière doit pouvoir, par des logiciels appropriés, contrôler et rejeter éventuellement des pièces jointes aux messages ou des fichiers téléchargés qui contiendraient des virus informatiques ; elle doit également pouvoir empêcher le téléchargement de fichiers trop volumineux (par exemple vidéos). De telles procédures, indispensables au respect de la sécurité de l'entreprise, ne s'exercent pas sur le contenu de l'information ; il s'agit d'un contrôle "aveugle" ne portant pas atteinte à la vie privée du salarié.

Contrôles ciblés

L'entreprise peut, par ailleurs, mettre en place un dispositif de contrôle individuel destiné à produire, poste par poste, un relevé des durées de connexion ou des sites visités. Dans ce cadre, ce contrôle en

volume peut également s'exercer en matière de courriels. L'employeur a alors accès au nombre de messages envoyés ou reçus ainsi qu'à la taille et à la nature des pièces jointes. Il s'agit de cerner les temps de consultations excessifs. Il peut également permettre de contrôler indirectement que l'application "personnel" est utilisée à bon escient. Ainsi, l'envoi d'un fichier client confidentiel de grosse taille sera détecté par ce contrôle en volume même si le courriel est indiqué comme étant personnel... de même, le répertoire "personnel" sur le disque dur peut faire l'objet d'un contrôle en volume (nombre de fichiers détenus, taille de ces fichiers, nature de ces fichiers).

La jurisprudence est aussi neuve que ces nouvelles technologies, elle évoluera avec les progrès techniques et l'attention que l'époque accordera à la vie privée. L'exercice de l'informatique au bureau nous rappelle qu'une entreprise est d'abord l'œuvre d'hommes faits de chair, de sang et de sentiments ; au bureau, ils auront toujours un coup de fil à donner à un enfant malade ou au livreur d'électroménager, mais au domicile, ils suivent l'actualité économique et soignent leur forme au profit de leur entreprise. Tout contrat social requiert un certain équilibre.

Florence Gladel

*Avocat à la Cour (droit social)
78 avenue Mozart, 75016 Paris*