



Alain Ménard,
Avocat Associé,
Racine

1) Cass. soc ; 2 octobre 2010.

2) Arrêt Phone House, Cass. soc ; 30 mai 2007.

3) Cass. soc ; 18 octobre 2006.

Droit social et nouvelles technologies de l'information et de la communication (NTIC)

La vie 'professionnelle' n'est pas en soi un élément protégeable au sens de notre Code civil (art.9) ; mais le salarié a droit au respect de sa vie privée, y compris pendant et sur son lieu de travail Arrêt Nikon. (1)

Il revient donc à l'employeur de concilier l'exercice de son droit d'organisation de l'entreprise et de son pouvoir disciplinaire avec le respect de la vie privée de ses salariés, alors que la frontière entre la vie privée et la vie professionnelle est de plus en plus ténue avec l'utilisation croissante des nouvelles technologies de communication au sein de l'entreprise (internet, smart phones, réseaux sociaux...).

I. Les fichiers et mails ne sont protégés que s'ils sont « confidentialisés »

L'utilisation par le salarié de la **messaging professionnelle** à des fins personnelles, y compris sur le lieu et pendant le temps de travail, ne peut pas ne plus être tolérée par l'employeur, mais son utilisation doit rester raisonnable. Ce caractère raisonnable de l'utilisation est apprécié par les juges d'un point de vue quantitatif (nombre de mails envoyés lorsqu'il affecte l'organisation ou la qualité du travail) mais également qualitatif (contenu illégal des mails envoyés).

Quelles sont dans ces conditions les limites du contrôle de l'employeur ? Quand et comment peut-il accéder à la messagerie du salarié ?

La jurisprudence précise que les mails et fichiers sont présumés « professionnels », l'employeur peut alors y accéder librement. (2)

Il appartient donc au salarié de protéger sa sphère privée dans l'ordinateur que l'employeur met à sa disposition.

C'est ce qu'il fera en identifiant un fichier ou un mail comme « *personnel* » ou « *confidentiel* », qui ne peut alors être ouvert par l'employeur qu'en présence du salarié ou celui-ci dûment appelé, en cas de risque ou d'évènement particulier. (3)

II. L'employeur peut contrôler les accès internet

Il n'est plus non plus sérieusement envisageable d'interdire au salarié d'accéder à **Internet** depuis son lieu de travail.

Les connexions à Internet depuis le système informatique de l'employeur sont présumées avoir un caractère professionnel, de sorte que l'employeur peut les contrôler.

Il peut également mettre en place des systèmes de contrôles des périodes et durées de connexion (se connecter de manière excessive à des fins privées peut en effet constituer une faute grave), et de systèmes de filtrages des sites prohibés (l'employeur qui tolère la visite de sites illégaux par le salarié peut engager sa responsabilité pénale pour complicité de fourniture de moyens). Il doit veiller à informer préalablement les IRP (Institutions Représentatives du Personnel), et ce peut être l'occasion de la mise en place d'une véritable charte informatique dans ces hypothèses.

III. Blogs et réseaux sociaux, espaces publics ou privés ?

La liberté d'expression du salarié sur Internet lui reste acquise à condition toutefois de ne pas dérapier dans l'injure ou le dénigrement. Le développement des **réseaux sociaux** et des **blogs**, sur lesquels les salariés peuvent s'exprimer sur leur entreprise et ses dirigeants rend la frontière entre espace public et privé de plus en plus difficile à appréhender.

Les blogs, accessibles à tous, doivent être considérés comme un espace public, mais pour les réseaux sociaux (Facebook), les choses sont plus floues. Les échanges sur la messagerie Facebook restent privés mais qu'en est-il du « *mur* », de la page Facebook du salarié, librement accessible à tous ses « *amis* » au nombre illimité ?

Pour certains, si le nombre d'« *amis* » est important, l'échange prend une dimension publique. C'est la position adoptée par l'employeur qui a licencié trois salariées pour les propos qu'elles avaient tenus sur Facebook dans une affaire portée devant le Conseil de prud'hommes de Boulogne Billancourt qui par un jugement du 19 novembre dernier, a considéré que le « *mode d'accès à Facebook dépasse la sphère privée* » parce qu'il était paramétré pour un partage avec « *ses amis et leurs amis* », critère somme toute aléatoire pour tracer les frontières d'une sphère privée. Les amis de mes amis ne sont-ils plus mes amis ? La détermination du seuil du nombre d'amis à partir duquel l'échange deviendrait public est périlleuse et il semblerait plus conforme de considérer les messages Facebook comme privés. L'affaire en question sur le bureau de la Cour d'appel, attendons...

En tout état de cause, l'employeur qui ne fait pas partie des « amis » du salarié et qui a intercepté des propos tenus sur Facebook et souhaite les sanctionner, risque de se rendre coupable d'« interception illicite de communication ».

Il s'agit précisément des faits de l'affaire qui sera jugée par le Conseil de Prud'hommes de Périgueux le 14 mars 2011, dans laquelle des salariés avaient été licenciés pour faute lourde en raison de propos tenus sur Facebook.

Il ne faut toutefois pas oublier que le salarié, auteur de critiques blâmables sur un réseau social « privé », reste à la merci de la « dénonciation » de l'un de ses « amis ».

IV. Une charte pour fixer les règles d'utilisation des outils informatiques

Il faut enfin évoquer la loi dite « HADOPI », du 12 juin 2009, partiellement censurée par le Conseil constitutionnel et complétée par la loi du 28 octobre 2009, qui vise à protéger les droits des auteurs et des ayant droits, et sanctionne la pratique du téléchargement illégal sur Internet, y compris au sein de l'entreprise.

En pratique, si un salarié effectue des téléchargements illégaux depuis son poste de travail, c'est l'adresse IP de l'entreprise qui sera identifiée et l'entreprise sera désignée comme responsable.

Elle recevra alors un premier avertissement

l'incitant à sécuriser son accès pour prévenir les téléchargements illégaux et, en cas de récidive dans l'année qui suit, elle risque une contravention et un mois de suspension d'accès à Internet !...

Pour prévenir le risque d'une sanction aussi dangereuse pour la survie de l'entreprise, il lui incombe de :

- se munir de moyens techniques de prévention contre les téléchargements illégaux,
- mettre à jour sa déclaration auprès de la CNIL, afin de pouvoir identifier depuis quel poste a été effectué le téléchargement,
- élaborer une charte informatique interdisant les téléchargements illégaux et informant les salariés des moyens de contrôle mis en place.

De tout ce qui précède, il ressort que l'adoption d'une **charte informatique** doit être recommandée.

Elle permettra d'informer les salariés des conditions d'utilisation des moyens d'information et de communication dans l'entreprise, sur leurs limites et sur les outils de surveillance mis en place. La charte ne sera mise en œuvre qu'après consultation préalable des instances représentatives du personnel existantes dans l'entreprise, et notamment du CHSCT dès lors qu'elle influe sur les conditions de travail des salariés.

JOURNAL SPÉCIAL DES SOCIÉTÉS



8, rue Saint Augustin - 75080 Paris Cedex 02

Tél. : 01 47 03 10 10 - Fax : 01 47 03 99 00

annonces@jss.fr - formalites@jss.fr

www.jss.fr

D. G. : Myriam de MONTIS

