

Des téléchargements aux réseaux sociaux : la liberté du salarié sous contrôle

Avec l'accès à Internet, les sites de téléchargement et les réseaux sociaux, le lieu de travail est plus que jamais ouvert sur l'extérieur. Face aux risques liés aux contenus illicites, comment le contrôle de l'employeur peut-il s'exercer sans empiéter sur les libertés du salarié ?

Par Christiane Féral-Schuhl*, avocate associée, Bâtonnier désigné, cabinet Féral-Schuhl/Sainte-Marie.



L'accès Internet est devenu, à l'instar du téléphone, un véritable outil de travail. La connexion au Web fait partie des moyens mis à la disposition de l'employé lui permettant d'exécuter son travail. Néanmoins, les employés utilisent également leur connexion professionnelle pour accéder à des sites de commerce électronique, à des plateformes de téléchargement d'œuvres culturelles ou encore à des réseaux sociaux (1).

Liberté, responsabilité et piratage

Si une zone de tolérance de cette utilisation à des fins privées est admise, elle est, néanmoins, limitée. En effet, la chambre sociale de la Cour de cassation a considéré qu'un licenciement pour faute grave était fondé dès lors que « le salarié avait usé de la connexion Internet de l'entreprise, à des fins non professionnelles, pour une durée totale d'environ 41 heures durant le mois de décembre 2004 » (2).

L'essor de ces outils modernes de communication et d'échange s'accompagne dans bien des cas d'une volonté accrue de contrôle de la part de l'employeur. Après avoir consacré le droit pour le salarié au respect de sa vie privée « même au temps et sur le lieu de travail » (3), la jurisprudence est intervenue pour encadrer ce droit. Se trouvant dans une relation de subordination, l'employé est tenu à l'égard de son employeur à un devoir de loyauté (4) lui imposant également une obligation de discrétion tant vis-à-vis des tiers que des autres employés. Le lien de subordination unissant le salarié au contrat de travail ne le prive pas pour autant de ses droits fondamentaux tels que la liberté d'opinion et d'expression. En tant que salarié, l'article L.2281-1 du Code du travail lui reconnaît un « droit à l'expression directe et collective sur le contenu, les conditions d'exercice et l'organisa-

tion de leur travail ». L'employé ne peut néanmoins abuser de ce droit en proférant des propos injurieux ou diffamatoires.

L'article 1384 alinéa 5 du Code civil dispose que l'employeur engage sa responsabilité civile en cas de faute commise par l'un de ses employés ayant agi dans le cadre de ses fonctions. Cette connexité peut être retenue lorsque la faute est commise par l'employé avec les moyens mis à sa disposition par l'employeur. Ce dernier a donc tout intérêt à contrôler l'usage de l'outil informatique par ses employés, afin de prévenir le risque d'utilisation illicite de ce dernier et les échanges des contenus illicites. Avec le dispositif de « réponse graduée » mis en œuvre par la Haute autorité pour la diffusion des œuvres et pour la protection des droits sur Internet (Hadopi), à la suite de la promulgation des lois Hadopi 1 et 2, adoptées respectivement les 13 juin et 29 octobre 2009, et de son décret d'application du 25 juin 2010 instituant une contravention de négligence caractérisée, la responsabilité de l'employeur peut en effet être aussi engagée. Et ce, en sa qualité de « titulaire de l'accès à des services de communication au public en ligne » dès lors que les téléchargements illégaux sur Internet (musiques, films, livres, logiciels, jeux vidéo, etc) réalisés par un salarié seront identifiés par l'adresse IP dont est titulaire son entreprise. Le décret d'application publié le 26 juin 2010 impose aux entreprises d'installer des moyens de sécurisation de l'accès Internet pour éviter tout téléchargement de contenus illicites.

Pouvoir de contrôle de l'employeur

À défaut, il encourt les sanctions de la contravention de négligence caractérisée (5) punie de l'amende prévue pour les contraventions de cinquième classe (1.500 euros, somme multipliée par cinq pour les personnes morales). Par conséquent, il est conseillé à l'employeur de s'assurer que les contenus échangés ne portent

Notes

(1) - Etude d'Opinion Way.

(2) - Soc. 18 mars 2009, n° 07-44.247, NP, RLDI 2009/06, n° 50, note Saint-Martin.

(3) - Soc. 2 oct. 2001, n° 99-42.942, Nikon France c/M. Onof, Bull. civ. V, n° 291.

(4) - Art. L.1222-1 C. trav.; Soc. 16 juin 1998, n° 96-41.558, Bull. civ. V, n° 323; D. 1998, IR 177.

(5) - R. 335-8 CPI.

(6) - Soc. 11 mars 1998, n° 96-40.147, NP, RJS 1998/4, n° 415.

pas atteinte aux droits d'auteur, au droit des marques, au droit des consommateurs, ... Pour cela, l'employeur peut sensibiliser ses employés par des pages-écrans ou des notes de service expliquant les risques d'échanges de contenus illicites, mais surtout, il doit installer des moyens de sécurisation adéquats.

Réseaux sociaux et vies privées

Ce pouvoir de contrôle doit s'exercer en toute transparence et de manière « proportionnée » (6). Au préalable, l'employeur doit déclarer les dispositifs de contrôle à la Commission nationale informatique et libertés (Cnil), informer ses employés et le comité d'entreprise. A plusieurs reprises, la Cour de cassation a rappelé cette règle : « Si l'employeur a le droit de contrôler et de surveiller l'activité de son personnel durant le temps de travail, il ne peut mettre en œuvre un dispositif de contrôle qui n'a pas été porté préalablement à la connaissance des salariés » (7). Pour anticiper les conflits, il est recommandé d'organiser les conditions d'utilisation des accès Internet dans le cadre d'un règlement intérieur ou d'une charte informatique intégrée à ce règlement. D'ailleurs, le fait de caractériser une faute grave dans la charte peut justifier un licenciement. Ainsi, dans un arrêt du 15 décembre 2010 (8), la Cour de cassation a validé le licenciement d'un salarié ayant conservé des documents à caractère pornographique sur son ordinateur puisque cette faute était visée dans la charte informatique. Dans une autre affaire (9), aucune charte n'ayant été signée, le licenciement était dépourvu de cause réelle et sérieuse.

Les réseaux sociaux ont été définis dans un avis du 12 juin 2009 (10) du G29, groupe des « Cnil » européennes, comme des plateformes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs.

Une récente enquête (11) constate que 67 % des utilisateurs de réseaux sociaux pensent qu'Internet a profondément changé la manière dont ils s'informent sur les entreprises.

Ainsi, l'e-réputation d'une entreprise comprend deux composantes : d'une part, la communication qu'une entreprise réalise pour son compte sur la toile et d'autre part, les propos ou contenus qui la concernent et sur lesquels son pouvoir de contrôle est beaucoup plus réduit.

La décision du conseil de prud'hommes de

Boulogne-Billancourt du 19 novembre 2010 (12) illustre la complexité d'appréciation du caractère privé ou public des propos tenus sur ces réseaux sociaux. En l'espèce, des salariés d'une société de conseil et d'ingénierie en technologies ont été licenciés pour faute grave au motif qu'ils auraient dénigré leur hiérarchie sur une page Facebook qu'ils ont créée et intitulée le « club des néfastes ». Ces propos avaient été publiés en dehors des horaires et du lieu de travail. Après avoir relevé que le salarié avait choisi de partager sa page Facebook avec « ses amis et leurs amis », les juges concluent que « ce mode d'accès à Facebook dépasse la sphère privée et qu'ainsi la production aux débats de la page mentionnant les propos incriminés constitue un moyen de preuve licite du caractère fondé du licenciement ». Dans une autre affaire, la cour d'appel de Reims (13) a jugé que le « mur » d'un ami se rapporte à un forum de discussion dès lors que la personne dénommée « ami » est susceptible d'avoir une centaine d'amis ou n'ait pas restreint l'accès à son mur.

Une affaire plaidée le 14 mars prochain devant le conseil de prud'hommes de Périgueux est attendue dans la mesure où les propos incriminés étaient publiés dans des circonstances de confidentialité plus strictes puisque les propos n'étaient accessibles qu'aux « amis ».

Face à cette nouvelle difficulté à définir les sphères publiques et privées, il faut conserver à l'esprit que diffuser du contenu n'est jamais anodin, d'autant plus que les réseaux sociaux sont davantage des outils de communication que de correspondance privée.

Inciter à une plus grande prudence

Plus précisément, la sphère privée sur un réseau social n'est plus synonyme de confidentialité puisque, par nature, ces réseaux ont pour philosophie la communication et le partage des contenus.

En publiant des propos sur un réseau social, même en paramétrant avec soins les destinataires, un salarié ne peut exclure que l'un de ses « amis », puis « amis d'amis » transfèrent son message. Publier présente donc toujours un risque qui doit inciter à une grande prudence. @

* *Christiane Féral-Schuhl a publié aux éditions Dalloz (collection Praxis Dalloz) la sixième édition de « Cyberdroit. Le droit à l'épreuve de l'Internet » (2011-2012).*

Notes

(7) - Soc. 20 nov. 1991, n° 88-43.120, Bull. civ. V, n° 519 ; D. 1992, jur. 73, note Chauvy : s'agissant d'une caméra dissimulée — Soc. 22 mai 1995, n° 93-44.078, Bull. civ. V, n° 164 ; Rev. soc. Francis Lefebvre 1995, n° 7, p. 489, note Chauvy : s'agissant de la filature d'un salarié par un détective privé.

(8) - Soc. 15 déc. 2010 n° 09-42.691, NP.

(9) - Soc. 8 déc. 2009, n° 08-42.097, NP.

(10) - JG29, avis 5/2009, 12 juin 2009, sur les réseaux sociaux.

(11) - Etude TNS SOFRES – Top Com « La réputation des entreprises se joue-t-elle sur les réseaux sociaux ? » publiée le 8 février 2011.

(12) - Cons. Prud'h. Boulogne-Billancourt, 19 nov. 2010, n° 10-00.853.

(13) - CA Reims, 9 juin 2010, n° 09-03.209.