AVOCAT
Nicole Babeau

INFOS

NEWSLETTER - *JUILLET 2016*

SOMMAIRE

22, rue Lafayette
31000 – TOULOUSE
Tél. 05 61 12 30 31
Fax 05 61 12 16 74

8, rue de l'Hôtel de Ville
81000 - ALBI
Tél. 05 63 38 73 04

babeau@jurisdefi.com
www.babeau-avocat.com

INTERNET et L'ENTREPRISE

Comment se protéger ?

Toute entreprise utilise aujourd'hui les moyens de communications des nouvelles technologies de l'information et de la communication.

Le chef d'entreprise doit prendre les mesures nécessaires pour pallier ou pour se garantir une preuve.

Quelques questions à se poser

Le Courrier électronique

La salariée utilise une messagerie personnelle, quel droits pour l'employeur ?

Une société avait engagé Mme X en tant qu'assistante administrative et commerciale le 21 février 2006. Par lettre du 17 novembre 2011, la salariée a pris acte de la rupture aux torts de l'employeur et a saisi le Conseil de Prud'Hommes.

L'employeur avait produit une pièce provenant de la messagerie de la salariée. Pour la Cour de Cassation : *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****. Les courriels et fichiers intégrés dans le disque dur de l'ordinateur mis à disposition du salarié par l'employeur ne sont pas identifiés comme personnels du seul fait qu'ils sont émis de ou vers la messagerie électronique personnelle du salarié.*

Or ladite pièce produite, bien que provenant de l'ordinateur professionnel mis à la disposition de la salariée est un échange de courriels en octobre 2011 reçu par la salariée sur sa boîte de messagerie personnelle et émanant d'adresses privées non professionnelles, de telle sorte que sa production porterait atteinte au secret des correspondances.

Les messages électroniques litigieux provenaient de la messagerie personnelle de la salariée distincte de la messagerie professionnelle dont celle-ci disposait pour les besoins de son activité ; en conséquence, ces messages électroniques devaient donc être écartés des débats en ce que leur production en justice portait atteinte au secret des correspondances.

Cass. sociale du 26 janvier 2016 N°14-15360

Comment suivre ou contrôler le courrier informatique ?

Pour maitriser les courriels vous devez posséder votre propre domaine internet (moi@mon-entreprise.com) et utiliser des services ou matériels de sécurité permettant de garantir au mieux la provenance, la transmission et le contenu des messages.

EN PARTENARIAT AVEC

L'INFOGÉREUR TOULOUSAIN by SOFT SYSTEMS

Soft Systems Group SAS
Parc Technologique du Canal
10, avenue de l'Europe - 31520 RAMONVILLE St AGNE
TéL. 33 (0) 5 34 320 380 - Fax : 33 (0) 5 31 619 923
www.linfogereur-toulousain.fr

membre de JURISDEFI

L'Utilisation d'Internet

Le salarié a-t-il-le droit d'utiliser l'accès internet à des fins personnelles pour visiter des sites prohibés ?

Le salarié avait été licencié pour faute grave et il contestait son licenciement. Devant la Cour de Cassation, il faisait valoir l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et l'article 9 du code civil, le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée, celle-ci implique en particulier le secret de ses communications.
L'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des sites internet consultés par le salarié grâce à un outil informatique mis à sa disposition pour son travail
La Cour de Cassation confirme le licenciement pour faute grave, car le salarié a utilisé l'outil informatique mis à sa disposition par l'employeur, à des fins personnelles et abusives. L'employeur l'a découvert en inspectant l'ordinateur mis à la disposition du salarié par la société ce qui a établi les **sites internet consultés** par le salarié pendant son temps de travail.
Cass sociale du 9 juillet 2008 N° 06-45.800 arrêt n° 1392.

Comment suivre ou contrôler l'accès aux sites internet pendant le temps de travail ?
Pour cela l'installation d'un pare-feu professionnel (UTM) accompagné d'un contrat de service est obligatoire afin de garantir le contrôle des sites Internet où les utilisateurs ont le droit de se rendre et ceci en correspondance avec la politique Internet de l'entreprise. L'ensemble des sites internet doivent être répertoriés et qualifiés, ceci n'est possible qu'au travers de base de données mondiale et mise à jour quotidiennement.
Garantir que les fichiers téléchargés sur Internet ne contiennent pas de code malveillant, et ceci ce fait aussi grâce à l'usage d'un matériel de traitement unifié des menaces.

L'accès au compte utilisateur

L'accès au poste informatique peut-il être une sécurité pour le salarié et pour l'employeur ?

Une salariée comptable, qualifiée et expérimentée, a travaillé en tant que comptable d'une association durant 34 ans. Elle a volontairement supprimé le fichier achats de l'exercice comptable antérieur. L'employeur a pu déterminer que seule cette salariée avait pu effacer ce fichier car *le poste informatique disposait d'un **code d'accès** et d'un **mot de passe** protégeant l'accès utilisateur*.
Le rapport technique effectué par un prestataire informatique indiquait « *L'édition informatique du journal des suppressions constatait que toutes les suppressions provenaient de son poste informatique, de son adresse IP et qu'elle était la seule utilisatrice. Aucune autre personne ne pouvait avoir accès aux données de cet ordinateur, la salariée étant la seul à connaître le **mot de passe***. ».
Le licenciement a été prononcé pour faute grave.
Cass, sociale du 15 janvier 2014, N° 12-21.399 arrêt n° 27.

Comment sécuriser l'accès au compte utilisateur ?
Pour cela l'usage d'un annuaire d'entreprise de type Microsoft Active Directory associé à une politique réelle de sécurité permet de garantir une meilleure protection contre l'usurpation d'un profil utilisateur.
D'autres outils d'authentification forte peuvent être associés à l'Active Directory, comme un lecteur d'empreinte, de carte à puce ou un système de mot de passe à usage unique (OTP). Ils permettent alors de garantir l'identité de l'utilisateur. Ces systèmes d'authentification peuvent alors être l'élément constituant la base d'une structure de signature électronique.

L'effacement des données

Est-il possible de savoir qui a supprimer les fichiers informatiques ?

Le salarié s'est livré, pendant les heures et temps de travail, à la consultation de sites « *d'activité sexuelle et de rencontres* », et a téléchargé un logiciel permettant d'**effacer** les fichiers temporaires du **disque dur** afin de masquer ses agissements.
La Cour de Cassation a confirmé la faute grave rendant impossible le maintien du salarié dans l'entreprise. En effet, ayant constaté que le tableau des permanences de M. X... et la liste des heures de connexion sur les différents sites internet de l'ordinateur de l'agence révélaient que les heures de consultation des sites étaient celles où celui-ci s'y trouvait seul, chargé de la permanence téléphonique et que les sites les plus nombreux étaient les sites " d'activité sexuelle et de rencontres ", le dernier site étant celui destiné au téléchargement d'un logiciel permettant d'**effacer** les fichiers temporaires du **disque dur**, de tels faits constituent à eux seuls des manquements graves du salarié à ses obligations découlant du contrat de travail, et justifient la faute grave. Durant ses heures de travail, le salarié ne doit pas passer son temps à surfer sur internet à titre personnel...
Cass. soc., 21 sept. 2011, n° 10-14.869, P+B+I

Comment protéger un disque dur contre l'effacement des données ?
Une entreprise étant par principe responsable des données qu'elle détient, elle doit mettre en œuvre un certain nombre de moyens pour éviter que des informations dont elle est détentrice et qui sont confidentielles ou simplement qui ne lui appartiennent pas, ne puissent être divulguées à des tiers.
Pour cela une seule solution existe elle consiste dans le chiffrement des données. On peut mettre en jeux ce chiffrement à plusieurs niveaux en fonction du risque qui doit être couvert : le chiffrement de surface (on chiffre tout le disque dur) est le moyen le plus commun utilisé pour y faire face, le sauvegarde (externalisée ou non) ou encore des « coffres forts » électroniques garantissant l'authenticité, l'intégrité et la confidentialité de l'information.

Afin sécuriser la relation de travail pour l'entreprise et pour le salarié, une **charte informatique**, charte **d**'utilisation des moyens d'information et de communication de l'entreprise, doit être mise en place.

Parlons-en ensemble !