Filtrage et Internet au bureau

LIVRE BLANC JURIDIQUE VOL. III :

Ne pas filtrer, ne pas loguer : conséquences

Olfeo
La sécurité positive

Lexing
Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

VOLUME III

NE PAS FILTRER, NE PAS LOGUER : QUELLES CONSEQUENCES ?

La conséquence se mesure nécessairement à l'aune du droit applicable. Mais dans cette hypothèse le droit français apparaît comme la seule référence possible pour toutes les entreprises françaises ou étrangères disposant de personnel sur le territoire national.

Une fois la question du droit applicable, il est possible d'apprécier le risque d'une part et la responsabilité d'autre part.

Note : les paragraphes marqués de ce marque-page rouge sont des nouveautés par rapport à la 3ème édition du livre blanc juridique Olfeo.

QUEL DROIT APPLIQUER ?

Pour une entreprise française, salariant du personnel sur le territoire national et commercialisant en France la question ne se pose pas.

Elle se pose à l'inverse pour les entreprises multinationales ou pour les entreprises étrangères salariant des personnels en France.

- **L'article 1837 du Code civil** dispose que « **Toute société dont le siège est situé sur le territoire français est soumise aux dispositions de la loi française**. Les tiers peuvent se prévaloir du siège statutaire, mais celui-ci ne leur est pas opposable par la société si le siège réel est situé en un autre lieu. »

- **L'article 14 du code civil dispose que : «** L'étranger, même non résidant en France, pourra être cité devant les tribunaux français, pour l'exécution des obligations par lui contractées en France avec un Français ; il pourra être traduit devant les tribunaux de France, pour les obligations par lui contractées en pays étranger envers des Français. »

- **Au plan pénal** la chose est toute aussi simple et fixée par **l'article L 113-2 du code pénal** qui précise que « **La loi pénale française est applicable aux infractions commises sur le territoire de la République**. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire ».

Par principe, à partir du moment où l'entreprise, sa filiale et ses salariés sont sur le territoire français, ils sont soumis à la loi française.

Le droit français s'applique à toutes les entreprises dont le siège est situé en France ainsi qu'aux infractions commises en France

QUEL RISQUES ?

Les risques de ne pas filtrer sont de deux niveaux :

- **Un risque direct** de ne pas respecter la loi ou d'une décision de justice
- **Un risque de devenir responsable** des accès des autres

LE NON-RESPECT DE L'OBLIGATION LEGALE DE FILTRAGE

Pour certains acteurs

Le droit impose à certains acteurs de mettre en œuvre ou de mettre à la disposition de leurs propres utilisateurs des moyens de contrôle ou de restriction des accès à Internet, c'est-à-dire en pratique de mettre en œuvre des outils de filtrage. Le droit impose également à certains acteurs de conserver les journaux de logs.

L'obligation légale la plus exemplaire dans ce domaine correspond à celle qui pèse sur les fournisseurs d'accès à Internet :

- **L'article 6 I. – 1° de la LCEN** dispose que « **Les personnes dont l'activité est d'offrir un accès** à des services de communication au public en ligne **informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès** à certains services ou de les sélectionner et leur proposent au moins un de ces moyens. »

Cet article, s'il impose directement au fournisseur d'accès de proposer à ses abonnés un moyen technique permettant de restreindre l'accès à Internet, implique indirectement l'obligation pour ledit abonné de le mettre en œuvre, sous sa responsabilité.

Les fournisseurs d'accès et les hébergeurs sont également tenus à une obligation de conservation des données d'identification :

- **L'article 6 II. de la LCEN** dispose que : « **Les personnes** mentionnées aux 1 et 2 du I **détiennent et conservent les données de nature à permettre l'identification de quiconque** a contribué à la création du contenu ou de l'un des contenus dont elles sont prestataires. »

De même le fait pour un tribunal d'ordonner à une entreprise de mettre en œuvre des outils de filtrage devient une obligation à part entière.

Au plan jurisprudentiel, l'arrêt **de la Cour d'appel de Paris du 4 février 2005**[1], aurait pour certains auteurs, assimilé l'employeur qui donne accès à ses employés à Internet, à un fournisseur d'accès.

De fait, si cette interprétation devait s'avérer exacte, tout employeur qui mettrait à disposition de ses employés, de ses agents ou de toute autre personne un accès à Internet, pourrait se voir opposer l'obligation légale posée à l'article 6 de la loi pour la confiance dans l'économie numérique :

- De **mettre à disposition des outils de filtrage** et d'informer les utilisateurs

- De **conserver les données d'identification** énumérées au sein du décret n °2011-219 du 25 février 2011[2] relatif à la conservation et à la communication de données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

Le risque spécial : Code de la propriété intellectuelle

L'article L 336-3 du Code de la propriété intellectuelle précise que « **La personne titulaire de l'accès** à des services de communication au public en ligne a **l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation** à des fins de reproduction, de représentation, de mise à disposition ou de communication au public **d'œuvres ou d'objets protégés par un droit d'auteur** ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ».

L'article ne vise en effet pas expressément le filtrage, l'abonné a « simplement » l'obligation de veiller à ce que l'accès à Internet ne permette pas de contrevenir aux droits de propriété intellectuelle par un téléchargement illégal d'œuvres protégées par le droit d'auteur. Pour ce faire, il doit mettre en place un moyen de sécurisation de son accès au réseau, qui consiste selon les lois Hadopi en un moyen de reconnaissance des contenus et de filtrage.

De fait, cela implique pour lui de mettre en place des moyens de filtrage de l'accès aux réseaux.
L'abonné a par conséquent une obligation spéciale de contrôle de l'utilisation de l'accès à Internet qu'il utilise et met à disposition.

Il faut bien distinguer l'abonné de l'Internaute. L'abonné est la personne physique ou morale qui est « juridiquement » liée à un fournisseur d'accès, l'internaute n'est pas nécessairement un abonné à Internet. Il est celui qui navigue sur Internet et accède aux services en ligne.

L'employeur titulaire de l'abonnement qui met à disposition de ses salariés un accès à Internet dans le cadre de leur travail est qualifié d'abonné et est par conséquent, responsable de leur activité sur les réseaux sur le fondement des lois Hadopi, et plus particulièrement en ce qui concerne le téléchargement d'œuvres protégées par un droit d'auteur.

Le code de la propriété intellectuelle renforce l'obligation de filtrage des entreprises

[1] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005
[2] Décret modifié par le Décret n ° 2014-1576 du 24 12 2014

LE RISQUE POUR UNE ENTREPRISE OU ADMINISTRATION DE NE PAS FILTRER

L'entreprise peut voir sa responsabilité engagée sur au moins trois fondements :

- L'article **1242** du code civil
- L'article **121-2** du code pénal
- L'article **L 336-3** du code de la propriété intellectuelle

Sans oublier l'impact toujours réel mais difficilement mesurable aujourd'hui de **l'arrêt de la Cour d'appel de Paris du 4 février 2005**[3].

Le risque civil

L'article 1242 alinéa 5 du code civil dispose « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. (…) Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ».

En d'autres termes **l'employeur est responsable des dommages causés par ses salariés** dans l'exercice de leurs fonctions.

Le risque civil consiste à devoir répondre des préjudices causés et donc de réparer le dommage causé et d'indemniser la victime par le paiement de dommages et intérêts.

Le risque pénal

L'article 121-2 du Code pénal dispose « Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions **des articles 121-4 à 121-7**, des infractions commises, pour leur compte, par leurs organes ou représentants. ».

En d'autres termes **l'employeur est responsable des actes de ses salariés au pénal si l'entreprise est bénéficiaire de l'acte illicite.**

Le risque pénal consiste à devoir répondre de la commission d'infractions et donc d'être sanctionné pénalement.

L'entreprise pourrait donc voir sa responsabilité engagée, notamment en tant que complice, pour des accès illicites, par ses organes ou représentants et pour le compte de l'entreprise :

[3] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005

- A des sites en raison de leurs contenus portant notamment atteinte :

  - **Aux mineurs**, tels que les contenus pédopornographiques
  - **A des sites de jeux en ligne illégaux** (ceux qui sont accessibles depuis le territoire français alors qu'ils n'ont pas bénéficié de l'agrément délivré par l'Autorité de régulation des jeux en ligne)
  - **A la protection des auteurs**, s'agissant des sites contrefaisants
  - A des sites faisant **l'apologie du terrorisme**

Il s'agit également de sites dont les contenus dépassent la liberté d'expression, tels que les sites racistes ou révisionnistes[4]. A l'avenir les sites contestant des crimes contre l'humanité pourront également être concernés, comme le mentionne le projet de loi « égalité et citoyenneté ».

- A des sites au regard des produits et services qu'ils commercialisent tels que notamment :
  - Des organes et produits du corps humain
  - Des drogues
  - Des objets à caractère pédophile
  - Des armes à feu et explosifs
  - Des médicaments
  - Du tabac
  - De l'alcool
  - Des logiciels permettant de porter atteinte à un système de traitement automatisé de données
  - Des logiciels de contournement de mesures techniques de protection ou d'information

Plus généralement, des produits interdits ou réglementés.

L'entreprise peut voir sa responsabilité engagée du fait des agissements de ses salariés

[4] TGI Paris 20-4-2005, ordonnance de référé Uejf et a. c/ olm llc et a.

QUI EST RESPONSABLE ?

LA RESPONSABILITE DE L'EMPLOYEUR

Au civil

Selon l'article 1242 alinéa 5 du code civil, l'employeur est responsable des dommages causés par ses salariés dans l'exercice de leurs fonctions.

Aujourd'hui la question se pose clairement de savoir si un employeur, qu'il soit un acteur privé (entreprise, association, fédération) ou public (ministère, collectivité territoriale, établissement public) est tenu ou non de mettre en place au sein de sa structure des outils de filtrage et de loguer.

Le débat porte essentiellement sur le niveau de responsabilité de l'employeur face à un usage illicite de l'Internet par ses employés et lorsqu'il donne accès à Internet à des tiers.

Il existe une jurisprudence abondante qui fixe les limites de cette responsabilité.

La jurisprudence précise que la responsabilité du dirigeant peut être limitée si l'employé a agi[5] :

- Hors du cadre de ses fonctions
- Sans autorisation
- En dehors de ses attributions

A priori les agissements hors contrat de travail ne devraient donc pas aboutir à la mise en cause de l'employeur.

Il existe toutefois des cas où la responsabilité de l'employeur a été retenue alors même que le salarié agissait en dehors de la fonction qui était la sienne :

La Cour d'appel d'Aix en Provence qui a rendu un arrêt retenant la responsabilité de l'employeur au motif principal que[6] :

- « En ce qui concerne par contre la responsabilité de la société Lucent Technologies en sa qualité de commettant, il n'est pas contestable que Monsieur X occupait les fonctions

[5] Cass. ass. plén. 19-5-1988 pourvoi n° 87-82654.
[6] CA Aix-en-Provence 2e ch. 13-3-2006.

de technicien test dans une entreprise "dont l'activité est construction d'équipements et de systèmes de télécommunication" selon ses propres écritures, et dans lesquelles l'usage d'un ordinateur, et d'Internet, doit être quotidien, a agi dans le cadre de ses fonctions

- Il est par ailleurs établi qu'il a agi avec l'autorisation de son employeur, qui avait d'ailleurs permis à son personnel, selon une note de service du 13 juillet 1999, "d'utiliser les équipements informatiques mis à leur disposition pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité"

- Il est enfin certain qu'il n'a pas agi à des fins étrangères à ses attributions, puisque selon le règlement précité, il était même autorisé à disposer d'un accès Internet, y compris en dehors de ses heures de travail. »

Cette position de la jurisprudence, tout comme **l'article 1242 alinéa 5 du Code civil** militent fortement en faveur de la mise en place par l'employeur de tous les outils permettant de maîtriser, voire de contrôler l'utilisation de l'Internet par les employés.

Cette mesure de prudence s'impose quel que soit le débat résiduel qui demeure quant à la fiabilité totale des solutions disponibles.

A côté de la responsabilité civile de l'employeur se pose naturellement la question de sa responsabilité pénale.

Au pénal

Selon l'article 121-2 du Code pénal, la responsabilité pénale de l'employeur peut elle-même être appréhendée sous deux angles :

- **L'employeur est-il responsable des infractions pénales** commises par **ses employés** qui utilisent les accès professionnels à Internet ?

- **L'employeur est-il responsable s'il n'empêche pas** ou permet même de manière fortuite à ses employés d'accéder à des contenus illicites ?

La réponse est loin d'être simple et trouve un de ses fondements à **l'article 121-1 du Code pénal** qui dispose que : « **Nul n'est responsable que de son propre fait** ».

Par principe, l'employeur n'a donc pas à être responsable des fautes pénales commises par ses employés.

Il convient cependant de tempérer cette position de principe en se référant à **l'article 121-2 du Code pénal** : « **Les personnes morales**, à l'exclusion de l'Etat, **sont responsables pénalement**, selon les distinctions des articles 121-4 à 121-7, **des infractions commises, pour leur compte, par leurs organes ou représentants**. »

A la question de savoir si l'employeur est responsable d'infractions pénales commises par ses employés qui utiliseraient les outils professionnels mis à leur disposition, il semble qu'il y ait deux réponses :

- **Soit l'infraction est commise sans lien avec l'entreprise** elle-même et alors on peut supposer que **seule la responsabilité de l'employé** sera retenue

- **Soit l'infraction est commise et l'entreprise en est bénéficiaire** et alors la responsabilité de l'entreprise et de ses **dirigeants pourra être engagée**

A la question de savoir si l'employeur peut être responsable du fait que ses employés puissent accéder à des sites illicites (sites à caractère pédophiles, sites racistes ou révisionnistes, sites attentatoires à la dignité, sites d'incitation au suicide, sites de jeux d'argent etc.) ou publier du contenu illicite (diffamatoire…) avec l'explosion de la contribution des utilisateurs sur la toile : la réponse dépend essentiellement des obligations légales posées par le législateur.

> Si l'on se réfère à l'article L. 335-7 et L.335-7-1 du Code de la propriété intellectuelle :

On peut estimer que l'employeur, qui est de fait et de droit titulaire de l'accès à Internet auprès d'un fournisseur d'accès est tenu à l'obligation de mettre en œuvre les outils de restriction d'accès qui lui sont proposés permettant d'éviter les actes de contrefaçon.

Ainsi **si l'employeur a commis une « négligence caractérisée**[7] » la commission de protection des droits de l'Hadopi, **en application de l'article L. 331-25 du Code de la propriété intellectuelle**, pourra lui adresser une recommandation l'informant notamment de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 (obligation pour la personne titulaire de l'accès à des services de communication au public en ligne de veiller à ce que cet accès ne conduise pas à des téléchargements illicites d'œuvres).

Si la peine de suspension de l'accès Internet pour négligence caractérisée a été abrogée lors d'un décret du 8 juillet 2013, en revanche, **est maintenue** dans **le Code de la propriété intellectuelle la peine complémentaire de suspension de l'accès à Internet prévu par l'article L. 335-7** en cas d'actes de **contrefaçon sanctionnés** par les articles L. 335-2, L. 335-3 et L. 335-4 du Code de la propriété intellectuelle lorsqu'ils sont commis au moyen d'un service de communication au public en ligne.

Ainsi l'entreprise peut se voir condamner à une:

- **Suspension de l'accès à un service de communication** au public en ligne pour une durée maximale d'un mois

- **Interdiction de souscrire** pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur

En cas de non-respect de l'interdiction de souscrire pendant 1 mois un autre contrat portant sur un service de même nature auprès de tout opérateur, l'abonné sera passible d'une amende d'un montant de 3750 euros maximum.

> Si l'on se réfère aux dispositions pénales de lutte contre la pédophilie :

[7] Selon l'article R. 335-5-I du Code de la propriété intellectuelle, créé par le décret 2010-695 du 25 juin 2010 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur internet, constitue une négligence caractérisée « le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, soit de ne pas avoir mis en place un moyen de sécurisation de cet accès, soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen. ».

Les termes « le fait d'offrir ou de rendre disponible » laissent à penser que la responsabilité de l'employeur pourrait être recherchée du fait que ses employés pourraient accéder à de tels contenus.

L'article 227-23 du Code pénal dispose notamment : « le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende. **Cet article** ajoute: « Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation ».

« Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines ».

> Si l'on se réfère à l'article 227-24 du Code pénal relatif à la protection des mineurs

Ce texte **vise à empêcher que des mineurs puissent accéder à des messages à caractère violent, ou incitant au terrorisme, ou pornographique ou de nature à porter gravement atteinte à leur dignité humaine.**

Une entreprise qui compterait parmi ses **stagiaires des mineurs**, **s'exposerait aux risques d'infractions prévus à cet article**, confirmant plus encore la nécessité de mise en œuvre de solutions de filtrage.

Cette appréciation peut être transposée à l'ensemble des autres dispositions à caractère pénal visant à restreindre l'accès à certains contenus.

En résumé, que l'employeur soit tenu de manière exprès ou qu'il y soit vivement invité, selon le fameux principe de précaution, il est dans son intérêt aujourd'hui de mettre en œuvre et de déployer des mesures de contrôle d'accès à Internet et de loguer les actes de ses salariés sur Internet.

> En est-il de même pour les administrations ou les collectivités territoriales ?

En effet, dans l'hypothèse où une collectivité territoriale n'a pas mis en place des mesures nécessaires pour la sécurité et le contrôle d'Internet utilisé par son personnel, et notamment pas utilisé de logiciel de filtrage, sa responsabilité pénale peut-elle être engagée du fait de la commission d'une infraction par l'un des membres de son personnel (ex : un agent qui aurait téléchargé sur Internet des images pédophiles via le système d'information de la collectivité territoriale[8]) ?

La réponse est plutôt négative.

En effet, l'hypothèse n'entrant pas dans les prévisions **de l'article 121-2 du Code pénal**, l'absence de mise en place de mesures de filtrage pour sécuriser l'utilisation d'Internet par son personnel ne fait pas partie des activités dans lesquelles la responsabilité pénale de celle-ci peut être engagée.

Néanmoins, sa responsabilité pourra être engagée en tant que commettant de son préposé si les conditions sont remplies.

Pour s'en défendre, l'administration devra prouver les trois éléments cumulatifs suivants, à savoir que l'agent a agi :

[8] Code pénal, art. 227-23 et 227-28-1

- Hors du cadre de ses fonctions
- Sans autorisation
- En dehors de ses attributions

Mais cela n'exclura pas toujours sa responsabilité. En effet, depuis **l'arrêt Lemonnier**[9], les mêmes faits peuvent constituer à la fois une faute personnelle de l'agent et une faute de service pour laquelle l'administration devra rendre des comptes.

A ce titre, la doctrine précise qu'à partir du moment où la faute a un lien avec le service, cette faute personnelle apparait comme « non dépourvue de tout lien avec le service », du fait qu'elle avait été réalisée soit pendant l'exercice des fonctions de l'agent, soit parce que l'exercice de sa mission avait pu faciliter sa commission d'une quelconque manière.

De plus, même lorsque la faute personnelle est commise en-dehors du temps et du lieu d'exercice des fonctions, qu'elle cause un préjudice et est commise par l'usage d'instruments fournis à l'agent par le service, l'administration est responsable du fait de son agent au titre de la faute de service, ayant contribué de manière quelconque à sa commission. [10]

La jurisprudence a estimé que dans ce cas **la faute personnelle n'est « pas dépourvue de tout lien avec le service** »[11]

Le premier dont la responsabilité sera recherchée, c'est l'employeur

RESPONSABILITE DE L'UTILISATEUR

En tant qu'utilisateur des moyens informatiques et de communications électroniques mis à sa disposition par son employeur, l'employé est responsable de ses actes, aussi bien sur le plan pénal que sur le plan civil.

Sur le plan civil,

L'engagement de sa responsabilité se fonde sur les articles 1240 et 1241 du Code civil :

- « Tout fait quelconque de l'homme, **qui cause à autrui un dommage**, oblige celui par la faute duquel il est arrivé **à le réparer** »

- « **chacun est responsable du dommage** qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence»

La responsabilité de l'utilisateur est subordonnée à la preuve :

- D'une faute ou d'une **négligence commise**
- D'un **préjudice subi**

[9] CE 26 juill. 1918, Épx Lemonnier
[10] Dalloz encyclopédie « Répertoire de la responsabilité de la puissance publique -Faute des agents et responsabilité administrative » – Jean-Pierre DUBOIS – avril 2014
[11] CE 18 nov. 1949, Demoiselle Mimeur, Lebon 492 ; JCP 1950. II. 5286, concl. Gazier).

- D'un **lien de causalité** entre la faute ou la négligence et le préjudice

Sur le plan pénal

L'utilisateur pourra voir sa responsabilité engagée dès lors que sera apportée la preuve qu'il est l'auteur ou le complice de l'infraction ou de la tentative d'infraction, de la même manière que pour son employeur personne physique.

L'engagement de la responsabilité de l'utilisateur tant sur le plan pénal que civil pourra le cas échéant se cumuler avec celle de son employeur, si elle est établie.

Le licenciement d'un employé pour une utilisation des moyens informatiques et de communications électroniques mis à sa disposition par son employeur, pouvant revêtir une qualification pénale pourra être qualifié de licenciement pour faute grave ou lourde.

Sur le plan de l'obligation de respecter le règlement intérieur, la charte

On relève plusieurs arrêts où la Cour a qualifié de licenciement pour faute grave le licenciement de salariés pour leur utilisation à des fins personnelles ou en violation des règles de l'entreprise de l'outil informatique mis à disposition par l'employeur pour les besoins de leur travail.

- **Dans le premier arrêt**, le salarié avait envoyé des **courriers à caractère pornographique** depuis sa messagerie professionnelle. Or, **la Cour de Cassation** a rappelé que les courriers adressés par le salarié depuis sa messagerie professionnelle étant présumés avoir un caractère professionnel, l'employeur peut les ouvrir hors la présence du salarié, sauf si celui-ci les identifie comme étant personnels.[12]
- **Dans le second arrêt, la Cour de Cassation** a qualifié le licenciement d'un salarié ayant violé une interdiction posée par la charte informatique mise en place par l'entreprise et intégrée au règlement intérieur de licenciement pour faute grave justifiant le licenciement immédiat de l'intéressé. En effet, le salarié avait utilisé sa messagerie professionnelle pour la réception et l'envoi de documents à caractère pornographique et la conservation sur son disque dur d'un nombre conséquent de tels fichiers, à savoir 480, alors que la charte prohibe formellement la consultation, la diffusion ou le téléchargement d'images à caractère pornographiques. De plus, la Cour de Cassation a ajouté que ces agissements étaient susceptibles de revêtir une qualification pénale.[13]

- **Dans un troisième arrêt, la Cour d'appel de Versailles** a affirmé que **l'installation d'un logiciel permettant le téléchargement illégal** d'œuvres musicales à partir de l'adresse IP de l'employeur était constitutif d'une faute grave rendant impossible le maintien du salarié à son poste, même pendant la durée du préavis[14].

- **Plus récemment**, à la suite **du jugement du Conseil de Prud'hommes de Nice du 30 octobre 2012**, la **Cour d'appel d'Aix-en-Provence** a rendu un **arrêt le 13 janvier 2015** validant le licenciement pour faute grave d'un salarié qui passait plus d'une heure par jour sur Internet pour son usage personnel. La Cour d'appel retient ainsi **une violation délibérée et répétée de la charte informatique, et fait droit aux arguments de son**

[12] Cass soc 15 12 2010 n ° 08-42486
[13] Cass soc 15 12 2010 n ° 09-42.691
[14] CA Versailles 31-5-2011 Mickael P. c/ Mireille B.P.

employeur arguant notamment lui avoir payé de très nombreuses heures de présence sans contrepartie d'un travail effectif.

Dans le cas contraire, l'inexistence de règles dans l'entreprise relatives à l'utilisation de l'outil informatique ne permet pas de prouver d'éventuelles fautes du salarié :

- la Cour d'appel de Nîmes, le 26 juillet 2016[15], a rendu un arrêt dans lequel, une association avait mis à pied l'un de ses salariés, un cuisinier, en lui reprochant la consultation de site de vente en ligne, de sites de sport et de sites pornographiques pendant son temps de travail. La Cour relève que **l'association n'avait adopté aucune charte informatique et que l'ordinateur en question n'était pas protégé par un mot de passe et était en libre accès**. La Cour relève que la seule présence concomitante de l'employé lors de ces utilisations est d'une portée probatoire insuffisante dès lors que l'ordinateur était situé dans pièce annexe. La Cour conclue que le doute profitant à l'employé, **il n'est pas établi que l'intéressé ait fait une utilisation abusive de l'ordinateur**. Le jugement est donc confirmé en ce qu'il a prononcé l'annulation de la mise à pied.

- la Cour d'appel d'Aix en Provence, dans un arrêt en date du 8 juillet 2016[16], a eu à connaître d'un licenciement pour faute grave ayant été prononcé contre un salarié en raison de la consultation de nombreux sites pornographiques pendant son temps de travail. **La société en question n'avait pas adopté de charte informatique et les codes d'accès de chacun des ordinateurs de la société consistaient dans les simples initiales** de leurs utilisateurs habituels respectifs et les doubles des clefs de l'ensemble des bureaux étaient accessibles, de sorte que n'importe quel salarié aurait pu avoir accès au poste du salarié mis en cause. La Cour en conclue que **l'employeur échoue à rapporter la preuve qui lui incombe** et constate que le licenciement prononcé est dépourvu de cause réelle et sérieuse.

- la Cour d'appel de Nancy, dans un arrêt du 22 juillet 2016[17], a conclu que **l'installation par le salarié d'un logiciel anti espion** sur sa machine, pour savoir si celle-ci était placée sous la surveillance d'un logiciel espion permettant de savoir ce qui était tapé sur son clavier et ainsi identifier s'il avait des conversations privées, **n'est pas de nature à justifier sérieusement un licenciement**.

Ces trois arrêts récents démontrent la nécessité de poser des règles strictes, en l'espèce sur les modalités d'utilisation de l'outil informatique, l'usage de mots de passe personnalisés et l'interdiction d'installer certains types de logiciels, afin notamment de sécuriser l'outil informatique et de pouvoir faciliter la preuve d'éventuelles fautes des salariés.

L'utilisateur est responsable de ses actes… encore faut-il que l'entreprise soit en mesure de l'identifier.

[15] CA Nîmes 26 07 2016 n° 15/04114
[16] CA Aix-en-Provence 8 juillet 2016 n° 2016/473
[17] CA Nancy 22 juillet 2016 n° 14/00624

Le rôle des administrateurs

Comme le précise la CNIL dans son **« Guide pratique pour les employeurs et les salariés »**[18], les administrateurs ont pour fonction d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes.

Dans le cadre de leurs fonctions, ils peuvent être amenés à accéder à des informations personnelles concernant les utilisateurs (messagerie, historique des sites consultés, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…).

D'après la CNIL, un tel accès n'est justifié que lorsque le bon fonctionnement des systèmes informatiques ne pourrait être assuré.
Selon la fiche pratique CNIL « Peut-on accéder à l'ordinateur d'un salarié en vacances »[19], un administrateur réseau ne doit pas communiquer systématiquement l'ensemble des mots de passe et des identifiants des salariés de l'entreprise à l'employeur, même si les fichiers contenus dans un ordinateur sont présumés être professionnels.

En effet, les mots de passe et identifiants sont personnels et les administrateurs sont soumis à une obligation de confidentialité.

L'ANSSI précise enfin que « les administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes dont ils ont la charge et qu'ils sont ainsi, tenus par une obligation de confidentialité. »[20].

Ils ne doivent donc pas divulguer des informations dont ils ont eu connaissance dans le cadre de leurs fonctions.

Ils peuvent révéler les informations entrant dans le champ du secret des correspondances et de la vie privée des utilisateurs, que si de telles informations portent atteinte :

- Au **bon fonctionnement technique** des applications
- A **la sécurité**
- A **l'intérêt de l'entreprise**

Les administrateurs ne pourraient, par ailleurs, être contraints de divulguer de telles informations, sauf disposition législative particulière en ce sens, d'après la CNIL.

Cependant, si un employé s'absente, l'employeur peut lui demander son mot de passe lorsque les informations détenues par cet employé sont nécessaires à la poursuite de l'activité de l'entreprise[21]. L'employeur ne doit cependant pas accéder aux contenus identifiés comme personnels par l'employé.

Tous les fichiers qui ne sont pas identifiés comme « personnel » sont réputés être professionnels de sorte que l'employeur peut y accéder hors la présence du salarié[22]. En revanche, si un fichier est

[18] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2010.
[19] Fiche pratique CNIL « Peut-on accéder à l'ordinateur d'un salarié en vacances », 19 juillet 2010.
[20] Recommandation de l'ANSSI Flux HTTPS n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.
[21] Cass. 18-3-2003.
[22] Cass. 18-10-2006.

identifié comme personnel, l'employeur ne peut y avoir accès « qu'en présence du salarié ou si celui-ci a été dûment appelé, ou en cas de risque ou évènement particulier. Le salarié ne peut s'opposer à un tel accès si ces conditions ont été respectées. »

S'agissant des données de **connexions à Internet**, une jurisprudence a retenu qu'elles **ne relevaient pas de la vie privée**, mais étaient présumées professionnelles. **L'employeur peut donc y avoir accès, en dehors de la présence du salarié**[23].

Dans ce contexte, comme le souligne la CNIL, il reste préférable de rappeler l'obligation de confidentialité des administrateurs dans leur contrat de travail ainsi que dans la charte d'utilisation des moyens informatiques et de communications électroniques, le cas échéant.

L'ANSSI rappelle enfin que « **l'administrateur fonctionnaire ou tout agent public contractuel**, est tenu par **une obligation de dénonciation de portée générale**, qui est de nature à le délier de son obligation de secret professionnel y compris en cas de délit commis par un membre de sa hiérarchie dans l'exercice de ses fonctions ».

Il conviendra également de déterminer en amont quel personne, au sein de l'organisme employeur, aura le pouvoir de demander et de recevoir les logs et dans quelles conditions. Ceci pourra être établi dans **la charte des Systèmes d'information** et la procédure formalisée dans un **guide d'opérations de contrôle**.

Les responsabilités des administrateurs et DSI

Les personnels, qu'ils soient directeurs de la sécurité des Systèmes d'information ou administrateurs sont nécessairement responsables des fautes qu'ils commettent à titre personnel, dans le cadre de leur présence au sein de l'entreprise :

- **La décision de la Cour d'appel de Paris** du 4 octobre 2007[24] a confirmé le licenciement d'un administrateur qui avait téléchargé pendant ses heures de travail des fichiers piratés et contrefaits en utilisant le système, à des fins personnelles étrangères à l'activité de son employeur.

Cependant, c'est sur un double terrain que la responsabilité des personnels en charge des moyens informatiques et de communications électroniques pourra être recherchée, dans le cadre de leur sphère professionnelle :

- Le premier axe de responsabilité pourra être celui de **l'incompétence professionnelle ou de négligence fautive** ; la question sera un jour posée de savoir si le fait pour un DSI de ne pas informer ses dirigeants de l'existence de moyens de contrôle et de restriction d'accès à Internet constitue ou non un manquement à ses obligations ;

- Le deuxième axe de responsabilité portera sur **l'exécution de demandes formulées par l'employeur et qui s'avéreraient manifestement illicites** quant à la mise en œuvre, au déploiement ou à l'utilisation des données relatives à l'outil de filtrage.

Les logiciels de prise en main à distance permettent aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique.

[23] Cass. soc. 9-7-2008 : « Mais attendu que les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence ».
[24] CA Paris 22e ch. C 4-10-2007 RG 03/12345.

De tels outils pourraient être utilisés par l'employeur à des fins de contrôle des activités de ses employés.

La CNIL précise dans son guide[25], qu'une telle utilisation n'est pas conforme aux principes de proportionnalité et de finalité posés par la loi « Informatique et Libertés ».
Lors de l'utilisation de tels logiciels, la CNIL recommande aux gestionnaires techniques de prendre deux précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquels ils accèdent :

- Recueillir l'accord de l'utilisateur qui aura été préalablement informé pour « donner la main »
- Tracer les opérations de maintenance.

Le défaut de filtrage pourrait être considéré comme une faute professionnelle par défaut de mise en œuvre de bonnes pratiques

[25] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2010.

POUR ALLER PLUS LOIN…

Découvrez nos 3 autres volumes sur les enjeux juridiques du filtrage Internet :

Volume I :
Droit de filtrer, droit de loguer

Volume II :
Filtrage et Internet au bureau

Volume IV :
Plan de déploiement juridique
d'une solution de filtrage

Disponibles au téléchargement via le lien suivant :
https://www.olfeo.com/proteger-votre-entreprise/maitriser-les-enjeux/juridique/demande-telechargement-du-livre-blanc

Le cabinet Alain Bensoussan et Olfeo publient également un guide de la charte informatique.

Découvrez dans ce guide quelles sont les bonnes pratiques en matière de charte, comment aborder la rédaction de la charte ? Comment la rendre opposable aux salariés ? …

http://www.olfeo.com/sites/olfeo/files/pdf/guide-charte-informatique-olfeo.pdf

A PROPOS D'OLFEO

Olfeo est éditeur de logiciel et expert de la sécurité web et du filtrage de contenus. Chez Olfeo, nous croyons que la sécurité positive est le meilleur moyen de vous protéger contre les nouvelles menaces du web tout en accompagnant les nouveaux usages chez vos collaborateurs.

Notre solution a aujourd'hui été adoptée par 2000 clients, représentant plus de 3 millions d'utilisateurs.

Il est dans notre ADN de considérer les projets de sécurité web au-delà des seuls aspects fonctionnels et techniques. Pour cela, nous proposons aux organisations exigeantes, la seule passerelle de sécurité Web basée sur une infrastructure proxy qui réunit à la fois l'expertise technologique, la conformité légale et culturelle ainsi que le facteur humain au service de la sécurité positive.

La sécurité positive doit être vue au sens large du terme. C'est l'approche novatrice d'Olfeo qui réunit ces trois enjeux fondamentaux de la sécurité Web dont deux d'entre eux sont trop souvent négligés dans beaucoup d'autres solutions. Olfeo est ainsi la seule solution qui peut réellement créer un environnement de confiance pour vos utilisateurs sur le Web.

Notre objectif est double : nous améliorons la fiabilité de votre sécurité web et nous accompagnons vos utilisateurs pour faire évoluer leurs pratiques et les responsabiliser dans leurs usages.

Notre passerelle de sécurité web, basée sur une infrastructure Proxy inclut les modules suivants :

- Proxy Cache QoS et déchiffrement SSL
- Filtrage d'URL
- Filtrage Protocolaire
- Antivirus de flux
- Portail Public

Retrouvez des actualités juridiques, métier et produit sur nos réseaux sociaux :

www.linkedin.com/company/olfeo

https://twitter.com/olfeo

www.youtube.com/user/OlfeoTV

www.facebook.com/societeolfeo

A PROPOS DU CABINET D'AVOCATS LEXING ALAIN BENSOUSSAN

Ce livre blanc a été co-écrit en collaboration avec le cabinet d'avocats Alain Bensoussan. Depuis sa création, Alain Bensoussan Avocats a élargi ses domaines de compétence, du cœur de métier constitué par l'informatique et les télécommunications vers les technologies avancées.

Le cabinet a reçu le Premier prix dans la catégorie « Technologies de l'information – Médias & Télécommunications », Palmarès des cabinets d'avocats d'affaires en 2015, 2014 et 2013 (Le Monde du Droit) et le Client Choice Awards en 2014 dans la catégorie « Information Technology »

Deux avocats spécialisés dans le Droit des technologies et la Sécurité des Systèmes d'informations ont participé à l'élaboration de ce livre blanc juridique :

Maître Eric Barbry

Avocat au Barreau de Paris
Directeur du Pôle « Droit du numérique »

Maître Polyanna Bigle

Avocat au Barreau de Paris.
Directeur du Département « Sécurité des Systèmes d'information et dématérialisation »

Le cabinet Alain Bensoussan Avocats assiste ses clients depuis 1978 dans le domaine du droit de l'informatique.

Depuis sa création, Alain Bensoussan Avocats a élargi ses domaines de compétence, du cœur de métier constitué par l'informatique et les télécommunications vers les technologies avancées.

Ces constantes évolutions technologiques ont été source de réflexion et de créativité l'amenant à rédiger, entre autres, le premier traité de droit de l'informatique en 1985, puis « Informatique, Télécoms, Internet » (1997, 2001, 2004, 2008, 2012), « Informatique et Libertés » (2008, 2010, 2014) ou encore le « Code de la sécurité informatique et télécom » aux Editions Larcier en 2016. Novateur dans son organisation, sa gestion et son système qualité, son positionnement d'origine, centré sur le droit des nouvelles technologies, l'amène naturellement à intervenir dans tous les autres secteurs des technologies avancées au fur et à mesure de leur apparition et développement.

Installé à Paris, Alain Bensoussan Avocats ouvre de nouveaux bureaux en province en 1990 et se développe à l'étranger dès 1992 par des accords de correspondance organique conclus en Europe (notamment Allemagne, Suisse, Belgique), aux Etats-Unis et au Japon.

En janvier 2012, Alain Bensoussan Avocats crée Lexing ®, premier réseau international d'avocats technologues dédié au droit des technologies avancées. Toute son activité résulte d'un positionnement voulu par une stratégique d'innovation et de développement du droit du numérique qui lui valent d'obtenir la reconnaissance de ses pairs, tant au niveau national qu'international.

En 2015, la revue juridique américaine « Best Lawyers » confirme pour la 5ème année consécutive, le positionnement d'Alain Bensoussan Avocats qu'il classe parmi les « avocats jugés incontournables » dans les catégories Technologies, Technologies de l'Information, et Contentieux.

Plus récemment, le cabinet a reçu le Premier prix dans la catégorie « Technologies de l'information – Médias & Télécommunications » du Palmarès
des cabinets d'avocats d'affaires en 2016, 2015, 2014 et 2013 (Le Monde du Droit) et le Client Choice Awards en 2014 et 2016 dans la catégorie « Information Technology »

Enfin, Alain Bensoussan a été distingué, en tant que Best Lawyer en Droit des Technologies de 2011 à 2015 et Law Firm of the Year pour l'année 2017 par la revue juridique américaine « Best Lawyers ».

www.alain-bensoussan.com

Réseau Lexing : network.lexing.eu/?lang=fr

www.youtube.com/channel/UC7xrTpr0LGPWVNbYxxDcFVQ