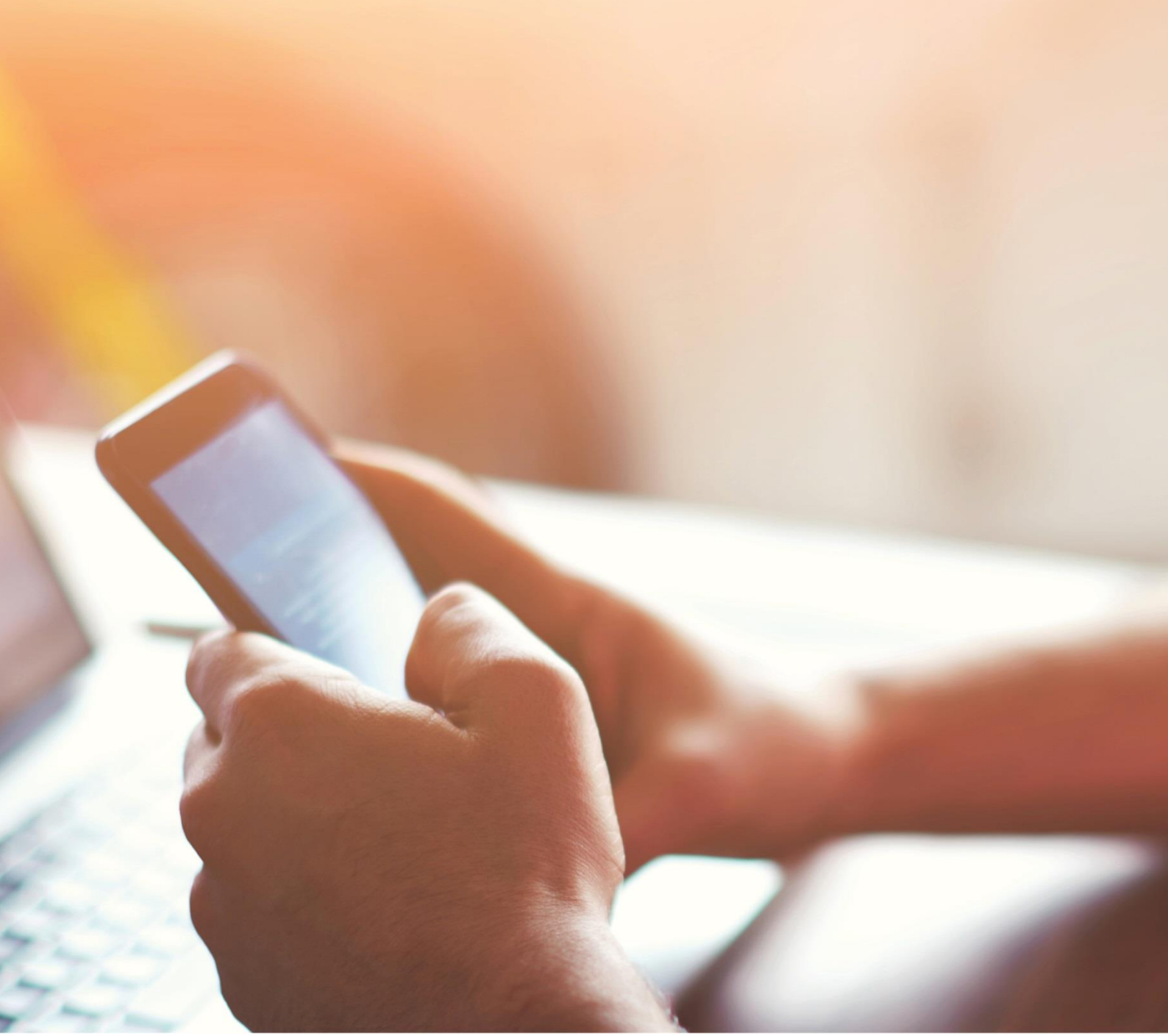

Filtrage et Internet au bureau

LIVRE BLANC JURIDIQUE VOL. II :

Nouveaux usages et filtrage

Olfeo
La sécurité positive

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

VOLUME II

NOUVEAUX USAGES ET FILTRAGE

En quelques années les usages ont changé tout comme le filtrage.

De nombreux usages se sont répandus : l'accès intensif des entreprises aux réseaux sociaux, l'accès Internet aux invités de l'organisation, l'accès aux flux chiffrés ou encore la présence de matériaux personnels connectés au réseau de l'entreprise.

Le filtrage lui aussi a changé en évoluant d'une forme dédiée au contrôle d'URL vers un filtrage techniquement étendu.

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

LES RESEAUX SOCIAUX ET L'ENTREPRISE

Les réseaux sociaux ne sont plus une simple « mode » utilisée en dehors de l'entreprise.

Aujourd'hui les réseaux sociaux font partie intégrante des outils de travail des salariés.

Ce sont de nouvelles formes de travail et de communication d'entreprise :

- Travail en réseaux (networking)
- Travail en communauté (hubworking)
- Web TV d'entreprise
- Communication 2.0 (Facebook…)
- Mise en contact professionnelle via plusieurs plates-formes
- Tweeter et blog d'entreprise…

Les réseaux sociaux permettent aux entreprises de bénéficier d'une nouvelle visibilité sur Internet et constituent un moyen de communication à grande échelle.

Les entreprises peuvent par exemple créer une page, un groupe sur les réseaux sociaux présentant leur entreprise afin d'attirer des prospects, fidéliser les clients…

Par le biais de différentes applications, l'entreprise peut annoncer les nouveautés concernant la marque, recueillir l'avis des consommateurs, réaliser des sondages et donc analyser les attentes et réactions de ses clients.

En termes de marketing, la présence sur les réseaux sociaux est donc devenue un outil indispensable de compétitivité.

En outre, la création d'applications dédiées aux salariés d'une entreprise permet de renforcer le sentiment d'appartenance à l'entreprise et constitue un moyen de socialisation[1].

Toutefois, les propos pouvant être publiés par les collaborateurs sur ces plates-formes ainsi que leur utilisation sur le lieu de travail constituent un risque juridique important. En effet, si beaucoup de législations leur sont applicables notamment la législation relative aux droits d'auteur, à la loi

[1] Article « Les réseaux sociaux en entreprise : un potentiel inexploité qui fait saliver. » sur le site emergenceweb.com.

Informatique et Libertés, les incriminations relatives aux STAD[2] ou encore la loi pour la confiance dans l'économie numérique, bien d'autres règles s'appliquent à l'utilisation d'Internet telles que la liberté d'expression et les limites qui sont les siennes : diffamation, injure, dénigrement, concurrence déloyale, pour ne citer que les principales.

Par conséquent un bon nombre de questions se posent à l'entreprise :

- Un salarié a-t-il le droit de parler librement de son entreprise ?
- Peut-il la critiquer sans risques ?
- Et, inversement, une société peut-elle décider des conditions d'utilisation des services web 2.0 et des réseaux sociaux par ses employés ?
- Et dans le cas d'un salarié qui, dans sa sphère privée, s'exprimerait négativement sur son entreprise ?
- La société qui aurait connaissance de telles critiques pourrait-elle sanctionner son collaborateur ?

De nombreuses jurisprudences ont vu le jour en la matière :

- **Le Conseil des prud'hommes de Boulogne-Billancourt, le 19 novembre 2010** : Trois salariés, employés de la même société, ont été licenciés pour faute grave pour « incitation à la rébellion contre la hiérarchie et dénigrement envers la société » sur le mur Facebook d'un autre salarié. Ces propos n'avaient pas été publiés depuis le poste informatique de l'entreprise mais durant le week-end

  Le Conseil de prud'hommes[3] décide que le licenciement pour faute grave des deux salariées est fondé considérant que « [l'un des salariés] a choisi dans le paramètre de son compte, de partager sa page Facebook avec « ses amis et leurs amis » permettant ainsi un accès ouvert notamment par les salariés ou anciens salariés de la société. (…) ce mode d'accès à Facebook dépasse la sphère privée (…) la production aux débats de la page mentionnant les propos incriminés constitue un mode de preuve licite du caractère bien fondé du licenciement ». Les salariés ont interjeté appel

- **La Cour d'appel de Besançon, le 15 novembre 2011** a également condamné une salariée pour avoir tenus des propos injurieux et diffamant envers son employeur sur le mur Facebook

  Elle précise **concernant le réseau social Facebook** qu'il « **doit être considéré au regard de sa finalité et de son organisation, comme un espace public**. Elle ajoute en outre « qu'il appartient en conséquence à celui qui souhaite conserver la confidentialité de ses propos tenus sur Facebook, soit **d'adopter les fonctionnalités idoines offertes par ce site**, soit de s'assurer préalablement auprès de son interlocuteur qu'il a limité l'accès à son «mur»[4]

- **La Chambre correctionnelle du Tribunal de Grande Instance de Paris, le 17 Janvier 2012** a également condamné un représentant du personnel et un délégué syndical pour **injure publique sur Facebook**.[5]

[2] Système de traitement automatisé de données
[3] CPH Boulogne-Billancourt, 19 nov. 2010, n°10-853
[4] CA de Besançon, 15 nov. 2011, n°10-02642
[5] TGI 17 ch correctionnel 17 Janvier 2012

- **La Cour d'appel de Reims, le 24 octobre 2012,** un apprenti salarié a été condamné à 500 euros d'amende pour avoir insulté son employeur sur Facebook6. La Cour d'Appel de Reims a constaté que les propos tenus par l'apprenti sur Facebook « auxquels ont accès nombre d'internautes sont manifestement insultants » et que celui-ci s'était « prêté sans réserve aux commentaires pour le moins désobligeants de ses correspondants ». La Cour a donc relevé que cette attitude était « manifestement fautive » et avait occasionné un préjudice à l'employeur.

L'entreprise ne peut, sauf circonstances tout à fait exceptionnelles, interdire à ses salariés d'utiliser les réseaux sociaux et les services web 2.0 dans leur sphère privée.

Mais la société, gardienne de ses secrets, de son image et, de manière générale, de sa sécurité, peut définir les conditions sous lesquelles elle accepte ou non que ses salariés s'expriment sur ses activités.

Par conséquent se pose la question des moyens légaux d'encadrer ces nouveaux usages.

Sur ce sujet, l'entreprise pourra interdire deux choses :

- **L'accès à ces outils** depuis les postes de travail ou durant le temps de travail

La publication d'informations au sujet de certaines activités de l'entreprise (projets spécifiques, activités, résultats financiers, etc…). Ainsi, doivent être ici précisées les **interdictions de communication sur et au nom de l'établissement, aussi bien dans la sphère privée,** dans le respect du principe de la liberté d'expression, **que professionnelle**, et la possibilité d'effectuer des signalements d'éventuels abus de la part d'un tiers. Il faut toutefois que cela soit indiqué de manière spécifique et colle à l'activité de l'entreprise

Il appartient à l'employeur de définir les règles du jeu quant à l'utilisation des réseaux sociaux et des services web 2.0 depuis le lieu de travail. A charge pour lui d'interdire, tolérer ou limiter les usages, en établissant un document de référence communément appelé «Charte d'utilisation des systèmes d'information».

LE SAVIEZ-VOUS ?

> IL EST AUJOURD'HUI POSSIBLE DE METTRE EN ŒUVRE UN ACCES AU WEB AVEC UNE GRANULARITE TELLE, QUE L'ON PEUT PARAMETRER L'OUTIL DE MANIERE A AUTORISER TELLE PERSONNE A ACCEDER A TELLE PLATE-FORME WEB 2.0 ET L'AUTORISER A REALISER TELLE OU TELLE OPERATION OU LUI INTERDIRE TELLE OU TELLE AUTRE

[6] CA Reims-ch soc 24 octobre 2012, n ° 11-01249- cf contra CA Rouen 15 11 2011 n°11-01827 et n°11-01830

LES ACCES INVITES AU RESEAU INTERNET DE L'ENTREPRISE

L'accès à un public tiers au web se développe comme une traînée de poudre.

Hier limitée aux cybercafés et à quelques aéroports pionniers dans le domaine des hot-spot, aujourd'hui l'accès public au web est partout : salons, hôtels, restaurant, point d'information public.

Cette pratique qui se développe de plus dans des entreprises et administrations laissant accès uniquement à Internet via leur Wi-Fi, est souvent appelée la pratique du Wi-Fi « invité » ou « visiteur ».

Il faut ici rappeler deux réalités juridiques :

- **L'article L 34-1 du Code des postes et des communications électroniques** dispose « Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article ».

  En langue naturelle cela signifie que les hot-spot professionnels sont soumis aux mêmes obligations que les opérateurs de télécommunications notamment en termes **d'identification des utilisateurs et de conservation des données de trafic**.

  Les entreprises fournissant un réseau interne ouvert au public au sein de l'entreprise constituent des **réseaux internes ouverts au public**[7]. Ces réseaux **ne sont pas soumis à l'obligation de se déclarer opérateur auprès de l'Arcep**, seuls les réseaux ouverts au public sont soumis à l'obligation de déclaration[8].

- **L'article L. 336-3 alinéa 1, du code de la propriété intellectuelle issue de la loi dite HADOPI**, dispose « 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

[7] CPCE, art.32 définit le réseau interne comme « tout réseau de communications électroniques entièrement établi sur une même propriété, sans emprunter ni le domaine public - y compris hertzien - ni une propriété tierce. »
[8] CPCE, art ; D98.

des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. Le manquement de la personne titulaire de l'accès à l'obligation définitive au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé sous réserve **des articles L 335-7 et L 335-7-1 du code de la propriété intellectuelle**».

De fait les personnes qui gèrent des accès publics ou invités au web seraient très inspirées de mettre en œuvre des mesures de filtrage, de recueil de leur identité et d'en informer les utilisateurs. Il est également évident qu'ils ont l'obligation de loguer.

Comment un employeur peut-il encadrer les accès Wi-Fi invité ?

Il est possible d'encadrer l'accès Wi-Fi invité mis à disposition par un organisme à ses invités ou même d'un employeur à ses salariés en prévoyant :

- **La limitation de l'accès à certains sites et services**, par conséquent, mettre en œuvre un système de filtrage
- **La conservation des données** de connexion
- **La charte Wi-Fi** présentant a minima une clause de mise en garde : « L'organisation se réserve le droit de mettre en place des dispositifs de sécurisation afin de s'assurer que l'accès ne fasse pas l'objet d'une utilisation frauduleuse ou illicite. L'entreprise pourra à sa seule discrétion, et sans avis préalable, modifier, suspendre ou interrompre l'accès à tout ou partie du Wi-Fi»

LE SAVIEZ-VOUS ?

TOUTE PERSONNE QUI « OFFRE » UN ACCES PUBLIC PEUT VOIR SA RESPONSABILITE ENGAGEE DU FAIT DES ACCES ILLICITES DES TIERS

LES FLUX SECURISES : HTTPS, FTPS…

Parmi les flux qui transitent sur le réseau de l'entreprise, les flux sécurisés constituent un cas particulier. Le protocole https offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web.

Pour ce faire, le HTTPS fait usage du protocole SSL/TLS qui utilise des méthodes de cryptographie asymétrique pour l'authentification, et des méthodes de cryptographie symétrique pour le chiffrement des échanges.

Ainsi, en principe, l'utilisation du protocole SSL/TLS permet d'assurer :

- L'authentification de l'une ou des deux parties communicantes
- La confidentialité des échanges
- L'intégrité des données échangées

Son usage s'étend aussi bien aux contenus professionnels qu'aux contenus personnels : banques en ligne, commerce en lignes…

Le flux étant chiffré entre le poste utilisateur et le serveur web, l'entreprise ne dispose pas de moyen de contrôle sur son contenu. L'antivirus de flux est, par exemple, inopérant. Des sites mal intentionnés pourraient donc utiliser ce protocole pour introduire du contenu indésirable à l'insu de l'entreprise.

Une technique de cryptanalyse, dite Man In the Middle, jusqu'ici utilisée par les pirates et les agences de renseignement, permet cependant de pouvoir déchiffrer ce flux et donc y appliquer des techniques de contrôle de contenu.

Il convient de s'interroger sur les risques juridiques d'une désencapsulation d'un flux chiffré y compris « personnel » sur le lieu de travail notamment au regard des référentiels légaux applicables en la matière :

- De vol d'identité
- D'usurpation d'identité
- D'atteinte aux STAD (Système de Traitement Automatisé des Données)
- D'atteinte au secret des correspondances

A défaut d'élément intentionnel, un grand nombre d'infractions pénales identifiées semblent pouvoir être écartées.

En revanche, il existe un risque d'atteinte au secret des correspondances ainsi qu'un risque lié à l'accès aux données contre lesquels les entreprises désireuses de déchiffrer ces flux doivent se prémunir.

A ce titre, une toute récente **note de l'ANSSI** sur le décryptage des flux https apporte de nouvelles précisions sur ce point, où elle qualifie notamment les risques juridiques du décryptage de flux HTTPS :

Elle définit en premier lieu le protocole de cryptage HTTPS qui est« la déclinaison sécurisée de HTTP encapsulé à l'aide d'un protocole de niveau inférieur nommé TLS 1, et anciennement nommé SSL »[9], permettant de protéger la confidentialité l'intégrité des communications entre un client et un serveur informatique.

Elle rappelle ainsi que le décryptage contient des risques dans la mesure où cette opération conduit à rompre la sécurité d'une transmission chiffrée et à faire apparaitre en « clair » les données qui étaient chiffrées et donc illisibles.

L'ANSSI précise que le déchiffrement en entreprise de tel flux ne doit être décidé qu'après validation de la direction des Systèmes d'information voire d'une autorité de niveau supérieur.

L'ANSSI présente le cadre légal du décryptage de flux cryptés et notamment :

- **Les articles 100 et suivants du code de procédure pénale** qui imposent une obligation légale de déchiffrement dans le cadre spécifique des interceptions judiciaires
- **Les articles L 241-1 à L 245-3 du code de la sécurité intérieure** qui autorisent cet usage dans le cadre des interceptions de sécurité
- **L'article 230-1 du code de procédure pénale** qui autorise le décryptage dans le cadre d'une enquête ou d'une instruction

En dehors de ces textes, plusieurs articles de loi s'opposent directement ou indirectement à une telle initiative et notamment :

- **L'article 226-15 du code pénal** garantissant le secret des correspondances privées
- **Les articles 226-16 à 226-24 du code pénal** prévoient la protection des données à caractère personnel
- **Les articles 226-1 à 226-7 du code pénal** protègent également la vie privée des salariés en dehors de leur cadre de travail

Enfin, il est également important de noter les risques juridiques entourant l'intervention de tiers sur les systèmes d'information, tels que des sous-traitants notamment, ou des prestataires techniques chargés de réaliser l'audit des systèmes d'information et découvrant des vulnérabilités contenant des données à caractère personnel.

Selon l'ANSSI, un employeur pourrait engager sa responsabilité s'il n'a pas prévu des dispositions spécifiques pour d'encadrer cet usage et ne pas porter atteinte aux droits des salariés, et s'ils ne prévoient pas les mêmes obligations spécifiques pour les sous-traitants de l'entreprise.

[9] Recommandation de l'ANSSI Flux HTTPS n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.

Afin d'éviter de tels risques pour l'employeur, l'ANSSI recommande d'encadrer cet usage et notamment de :

- **Prévoir son implémentation dans une charte** d'utilisation du système d'information rédigée par l'employeur

- **Nommer un administrateur** qui sera la **seule personne à être autorisé** expressément à prendre connaissance des contenus déchiffrés. Il sera soumis à une obligation de confidentialité sur toutes ces informations

- **Créer un article spécifique dans la politique de sécurité** des Systèmes d'information de l'entreprise prévoyant la possibilité de pouvoir déchiffrer des flux https et les dispositions s'appliquant aux sous-traitants

- **Procéder aux déclarations CNIL de ces outils de déchiffrement**. Il est impératif de bien indiquer les finalités de ces traitements

Cette possibilité devra être toutefois justifiée par deux finalités :

- **L'impossibilité d'assurer le bon fonctionnement** et de maintenir les conditions de sécurité informatiques par d'autres moyens

- **La présence, ou tout du moins la convocation[10] du salarié concerné** en cas de connaissance de contenus considérés comme personnels ou privés[11]

A cet égard, **dans son article du 31 mars 2015, la CNIL rassure et précise que "Du point de vue " Informatique et Libertés ", ce déchiffrement [des flux Https] est légitime** du fait que l'employeur doit assurer la sécurité de son système d'information. Pour ce faire, il peut fixer les conditions et limites de l'utilisation des outils informatiques.

Toutefois, le recours au déchiffrement doit être encadré et peut faire l'objet des mesures suivantes » :

- **Une information précise** des salariés

- **Une gestion stricte des droits d'accès des administrateurs** aux courriers électroniques

- **Une minimisation des traces** conservées

- **Une protection des données d'alertes extraite de l'analyse** (ex : chiffrement, stockage en dehors de l'environnement de production et durée de conservation de 6 mois maximum)

Enfin, on prendra soin de ne pas risquer de porter atteinte au respect à la vie privée des employés de sélectionner une liste blanche des sites Internets sécurisés ne devant pas être déchiffrés par l'employeur comme par exemple les sites d'organismes de sécurité sociale, mutuelle, laboratoires d'analyses médicales, …

[10] Cass, Soc 17 6 2009 n° pourvoi 08-40274
[11] Cass, Soc 17 5 2005, n° pourvoi 03-40017

LE SAVIEZ-VOUS?

LE DECRYPTAGE DE FLUX HTTPS DOIT ETRE STRICTEMENT ENCADRE PAR L'EMPLOYEUR AFIN DE NE PAS ENTRAINER UNE VIOLATION DES DROITS DE PROPRIETE INTELLECTUELLE ET DES DROITS DES DONNEES A CARACTERE PERSONNEL

LE FILTRAGE ETENDU

Le http(s) est sans doute le protocole le plus utilisé par les salariés. Cependant il existe bien d'autres protocoles pour échanger ou télécharger des contenus.

Or tous ces autres protocoles sont, comme le web, source de risque juridique et/ou technologique.

Il importe donc de maîtriser non seulement le filtrage URL mais aussi le filtrage sur les autres protocoles.

De fait la notion technico-fonctionnelle du filtrage évolue vers un filtrage étendu : le filtrage protocolaire.

CE QU'IL FAUT RETENIR

LE FILTRAGE URL EST UN PREMIER REMPART TECHNIQUE POUR PROTEGER JURIDIQUEMENT L'ENTREPRISE MAIS EST INSUFFISANT.
POUR ETRE EFFICACE LE FILTRAGE DOIT ETRE ETENDU A L'ENSEMBLE DES FLUX ET PROTOCOLES.

BYOD (BRING YOUR OWN DEVICE)

Le BYOD est l'abréviation de l'expression « Bring your own device », consistant en l'utilisation dans un cadre professionnel, d'un matériel personnel tel qu'un téléphone multifonction ou un ordinateur.[12]

En France, l'abréviation utilisée est AVEC pour « apportez votre équipement personnel de communication ». Les appareils utilisés ont pour utilité technique de faciliter l'accès aux informations et applications de l'entreprise.

Selon le rapport CLUSIF de 2014, le BYOD aurait vu son **taux d'interdiction** au sein **des entreprises passer de 38% à 66%**.[13]

Ainsi, selon la CNIL seuls 44 % des possesseurs disent avoir une utilisation « exclusivement personnelle » de leur smartphone.[14]

Or, selon une étude du cabinet américain Gartner, 45 % des entreprises mondiales en 2020 auront renoncées à leurs flottes d'appareils mobiles professionnels.[15]

En l'état actuel du droit, aucune loi ou décret ne régule le BYOD dans les entreprises.

Si les avantages sont nombreux notamment des économies pour l'entreprise qui n'a pas besoin de renouveler ses appareils, et qui développe également une image de modernité, **les risques le sont également avec la sécurité pour les systèmes d'information et la confidentialité des données**.

En effet, l'utilisation des BYOD entraine la disparition de frontières claires entre usage professionnels et privés.

Se posent ainsi trois questions majeures :

- **L'employeur peut-il imposer l'utilisation du BYOD au sein de son entreprise ?**
  Peut-il mettre en œuvre des moyens afin de sécuriser les données professionnelles et le système d'information ?

- **L'employeur peut-il contrôler le matériel personnel d'un collaborateur qu'il utilise à des fins professionnelles ?**

[12] Définition légifrance
[13] Rapport CLUSIF Menaces informatiques et pratiques de sécurité en France, Édition 2014, M. MOURER Lionel, Mme COURTECUISSE Hélène et M. PRISO Serge.
[14] Lettre IP n ° 7 6 2014
[15] Bring Your Own Device: The Facts and the Future, Etude Gartner 2013,David A. Willis

Concernant la première question, selon **l'article L.4121-1 du Code du Travail**, l'employeur se doit de fournir à ses employés les moyens adaptés et nécessaires à l'exécution de leurs tâches professionnelles.

Par conséquent, **l'employeur ne peut imposer à ses salariés** l'utilisation du BYOD. Il **peut néanmoins l'interdire ou l'autoriser.** Dès lors, si il décide de l'autoriser, il peut imposer aux salariés la mise en place de moyens de sécurité concernant les données et applications professionnelles qui doivent néanmoins respecter **la vie privée** des employés qui utilisent des équipements personnels dans le cadre de leur activité professionnelle.

D'un point de vu sécurité des informations professionnelles, il parait donc nécessaire que l'utilisateur accepte d'ajouter des solutions de sécurisation sur son système informatique. A ce titre, l'employeur devra prévoir un budget pour former son personnel à l'utilisation de cette technologie, et mettre en place des outils assurant la sécurité et la confidentialité, tels que le Mobile Device Management (MDM).

Le Mobile Device Management, ou « Gestion de Terminaux Mobiles », est une application permettant la gestion l'entreprise, au niveau du service informatique, d'une flotte d'appareils mobiles, qu'il s'agisse de tablettes, de smartphones voire d'ordinateurs hybrides au format tablette.

En outre, l'employeur doit définir les conditions de contrôle sur toutes les données professionnelles qui sont utilisées par le salarié sur son système informatique personnel utilisé pour son travail, afin d'éviter que la confidentialité des informations sensibles de l'entreprise soit menacée.
Afin d'assurer une sécurité maximale pour les systèmes d'information de l'entreprises, les responsables des systèmes informatiques pourront procéder aux actions suivantes :

- **Limiter à certaines catégories de personnes** uniquement le « droit » au BYOD
- **Limiter le nombre ou le type de terminaux** accessible au BYOD
- **Limiter le nombre ou le type d'usages**
- **Imposer des mesures ou applications particulières** tel que le MDM ou une application de sécurité
- **Imposer la mise en place d'un contrôle de la partie professionnelle** du terminal
- **Définir les règles** du jeu
- **Définir le processus pour demander à bénéficier du BYOD**

Par ailleurs, il leur sera possible de mettre à la charge du salarié les frais d'abonnement et d'utilisation de son terminal, soit les coûts du BYOD, pour les besoins de son activité professionnelle.[16]

En effet, concernant la prise en charge des coûts du BYOD, contrairement au télétravail, aucune réglementation spécifique, n'impose la prise en charge des coûts que pourrait engendrer la pratique du BYOD pour le salarié, notamment lorsque cette pratique est une solution laissée au libre choix du salarié et n'est pas imposée par l'employeur.

[16] Cass. soc. 2 4 2014

Il convient par contre de ne pas :

- **Pratiquer le BYOD par « discrimination »** (l'autoriser uniquement pour certains salariés de manière discriminatoire)
- **Interdire du jour au lendemain ce qui était admis** et qui mettrait en cause la bonne exécution du travail (il est nécessaire dans ce cas de mettre en place un préavis)
- **Autoriser le salarié à travailler hors de ses horaires de travail ou pendant son temps de repos** (cela contrevient à l'obligation de l'employeur de contrôler la durée du travail)

Concernant l'utilisation du matériel informatique par les salariés en dehors du temps de travail, la loi n° 2016-1088 du 8 août 2016, dite « loi travail », fait entrer le droit à la déconnexion dans le code du travail. Il s'agit du droit pour le salarié de se déconnecter des outils numériques mis à sa disposition par l'employeur pour l'exercice de son travail, de manière à respecter ses temps de repos, de congés et sa vie personnelle et familiale. Pour l'employeur, ce droit s'accompagne de la mise en œuvre de dispositifs de régulation et d'actions de formation et de sensibilisation.

Les mesures concrètes à mettre en place pour les employeurs sont donc les suivantes :

- **Elaborer une stratégie** permettant la **gestion effective des différentes parties** de l'entreprise au sein desquelles le BYOD est utilisé
- **Adapter leur charte des Systèmes d'information** à ce nouvel usage informatique au sein des entreprises
- **Si besoin, signer des avenants aux contrats** de travail, lorsque des prises en charge de frais sont envisagés par exemple
- **Veiller à ce que les instances représentatives du personnel soient informées** avant d'encadrer ou d'interdire mettre en place le BYOD
- **Gérer efficacement le droit discrétionnaire** de déconnexion de l'employeur concernant les Systèmes d'information des matériels personnels utilisés pour le BYOD

A la seconde question, concernant le contrôle du matériel personnel d'un collaborateur qu'il utilise à des fins professionnelles, la jurisprudence a précisé certains points concernant le BYOD :

- **Une clé USB personnelle connectée** à un **outil informatique mis à la disposition du salarié par l'employeur**, pour l'exécution de son contrat de travail, **est présumée** être utilisée à des fins **professionnelles**, et peut donc être consultée par l'employeur.[17]
  Il en résulte que l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié.

- **Un autre arrêt de la Cour de Cassation**, a estimé que l'employeur ne peut procéder à l'écoute des enregistrements réalisés par la salariée sur son dictaphone personnel en son absence ou sans qu'elle l'ait au moins dûment appelé[18].

  Il résulte de cet arrêt que **l'employeur a bien le droit de consulter les données d'un outil personnel du salarié utilisé à des fins professionnels**, à condition de respecter certaines conditions et notamment **en sa présence**, ou en amenant la preuve qu'il l'a dument appelé avant de procéder à la consultation des données.

[17] Cass soc 12 2 2013 n° 11-28649
[18] Cass-soc 23 05 2012 n° 10-23521

Par ailleurs, il est possible pour l'employeur de prendre connaissance des contenus personnels des salariés, sur autorisation du tribunal.

Ainsi, un employeur est légitime à obtenir du juge l'autorisation d'accéder aux courriers électroniques à caractère privé de son salarié, dès lors existe qu'il justifie de motifs légitimes de suspecter des actes de concurrence déloyale de la part de son salarié [19]

Quoiqu'il en soit, il apparait donc impératif pour l'employeur de prévoir un cadre juridique complet afin d'encadrer l'utilisation du BYOD dans la charte des Systèmes d'information.

Concernant le BYOD, la CNIL s'est également positionnée sur ce sujet en publiant une fiche pratique sur **« les bonnes pratiques » en matière de BYOD** en février 2015[20].

D'après la Commission, la sécurité du système d'information de l'entreprise doit être conciliée avec le respect de la vie privée des employés qui utilisent des équipements personnels dans le cadre de leur activité professionnelle.

La CNIL énumère ainsi les meilleurs pratiques afin de limiter les risques pour la sécurité des données :

- **Identifier les risques**, en tenant compte des spécificités du contexte (quels équipements, quelles applications, quelles données?), et les estimer en termes de gravité et de vraisemblance.
- **Déterminer les mesures à mettre en œuvre et les formaliser dans une politique de sécurité.**
- **Sensibiliser les utilisateurs** aux risques, **formaliser les responsabilités** de chacun et **préciser les précautions à prendre dans une charte** ayant valeur contraignante.
- **Subordonner l'utilisation des équipements personnels à une autorisation** préalable de l'administrateur réseau et/ou de l'employeur.

En plus du BYOD, l'employeur peut également être confronté au BYOS (Bring Your Own Software) ce qui consiste, pour le salarié, à utiliser des logiciels qui n'appartiennent pas à l'entreprise (tels que les services de stockage sur un cloud gratuits pour collaborer sur ou partager des documents volumineux par exemple). En marge du système informatique de l'entreprise peut donc se développer un système informatique fantôme ou « Shadow IT » qu'il est difficile de contrôler. Le BYOS ne fait pas l'objet d'une réglementation spécifique ce qui n'est pas sans poser des difficultés particulières lorsqu'il est question de filtrer. Tout comme pour le BYOD, des mesures concrètes doivent être mises en œuvre par l'employeur et intégrées dans une charte des Systèmes d'information (interdiction de transférer des données professionnelles sur une application autre que celles indiquées par la Direction Informatique).

CE QU'IL FAUT RETENIR

LE BYOD EST UN USAGE INTERESSANT D'UN POINT DE VUE ECONOMIQUE EN PARTICULIER, MAIS IL EST FORTEMENT RECOMMANDE DE BIEN PREVOIR LES CONDITIONS ENCADRANT SON UTILISATION.

[19] Cass soc 23 5 2007 n° 05-17.818.
[20] http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/byod-quelles-sont-les-bonnes-pratiques/

> LA PARTIE PROFESSIONNELLE DU MATERIEL UTILISEE A TITRE PROFESSIONNEL PEUT ETRE CONTROLEE. CECI DEVRA ETRE PREVU DANS LA CHARTE, DE MEME QUE L'OBLIGATION POUR L'EMPLOYE DE METTRE EN EN PLACE DES PREREQUIS TECHNIQUES ET SOLUTIONS TECHNIQUES NECESSAIRES.

A l'inverse du BYOD, une pratique se généralise consistant pour l'employé à utiliser, notamment en dehors de son temps de travail, des matériels professionnels à des fins personnelles. A ce titre, les dispositifs de filtrage peuvent impacter les usages privés des employés en dehors de leur temps de travail (impossibilité de consulter certains sites internet le week-end par exemple). A cet égard, il convient, a minima, que l'employé en soit conscient et qu'il l'ait accepté dans une convention particulière ou dans une charte si la pratique se développe dans l'entreprise.

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 III :
Ne pas filtrer, ne pas loguer : les conséquences

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