LIVRE BLANC

Olfeo
La sécurité positive en collaboration avec LEXING ALAIN BENSOUSSAN AVOCATS

Maîtrisez vos risques juridiques

Que disent les lois et les jurisprudences sur l'utilisation d'Internet au bureau ? Comment protéger son entreprise dans le respect de ces réglementations ? Comment réagir face aux nouveaux usages : SaaS, HTTPS, nomadisme… Comment garantir la protection des données personnelles ?

SOMMAIRE

PREFACE

L'usage d'Internet au sein des entreprises se complexifie année après année avec le développement des nouveaux usages et des nouvelles menaces qui leurs sont liées : Shadow IT, déchiffrement SSL, Cloud Act, nomadisme, RGPD … Les DSI et les RSSI se posent de nombreuses questions juridiques dans le cadre de leurs missions de protection des intérêts de leurs organisations :

- Qu'avons-nous le droit de filtrer ?
- Faut-il ou peut-on filtrer les accès publics au web ?
- Existe-t-il un régime juridique différent entre les entreprises privées et les acteurs publics ?
- Comment filtrer tout en préservant la vie privée résiduelle des salariés et le respect du RGPD ?
- Peut-on sanctionner un collaborateur sur la foi des données restituées par l'outil de filtrage ?
- L'outil de filtrage est-il autorisé alors qu'il collecte nombreuses données à caractère personnel ? Faut-il informer le personnel, les personnes extérieures, les deux ?
- Quels risques sont engendrés par le développement des applications Saas ?
- En quoi consiste précisément le Cloud Act ?

L'évolution du droit et des usages a amené une modification importante du comportement au sein des entreprises où la question n'est plus « Peut-on filtrer ? » mais « Comment filtrer en toute sécurité pour couvrir toutes les menaces ? ».

La jurisprudence constante et les recommandations des autorités de contrôle comme l'Anssi et la Cnil, confortent ce point, en légitimant la mise en œuvre d'un contrôle des connexions Internet.

Dès lors, il existe trois types d'entreprises ou entités exposées :

- Celles qui prennent encore le risque de ne pas filtrer
- Celles qui filtrent et dont la solution n'est pas mise en œuvre en conformité avec les exigences juridiques de base
- Celles qui, dans un souci de sécurité de leur système d'information, procèdent à un contrôle parfois abusif, au risque d'atteindre la sphère de la vie privée.

Sur le plan organisationnel, on parle par ailleurs de moins en moins de « filtrage » mais « de gestion des droits d'accès et des habilitations ».

L'évolution n'est pas que sémantique. Elle procède d'un vrai changement de paradigme au sein des entreprises ou entités, poussées par leurs obligations de conformité notamment aux dispositions sur la protection des données à caractère personnel.

Maître Polyanna Bigle
Avocat
Directeur du Département Sécurité Numérique
Spécialiste en Droit des Nouvelles Technologies

CHAPITRE I
DROIT DE FILTRER, DROIT DE LOGUER

IL N'Y A PLUS DE DOUTE AUJOURD'HUI, LE FILTRAGE EST ADMIS SUR TOUS LES PLANS : LEGAL, JURISPRUDENTIEL, NORMATIF ET DE BONNES PRATIQUES AINSI QUE SUR LE PLAN DES USAGES.

Cette reconnaissance s'étend naturellement au-delà des frontières hexagonales.

Mais comprendre le droit du filtrage c'est aussi s'intéresser :

- Au droit des logs, car tous les outils de filtrage comportent des logs et fichiers qui seront le cas échéant exploités pour sanctionner un abus
- Au droit des chartes d'usage des systèmes d'information car il ne saurait être question de filtrer sans informer et fixer les règles.

I. LE DROIT DE FILTRER, CADRE LEGAL

Le terme de « filtre » ou de « filtrage », n'est pas inconnu des textes actuels.

On trouve effectivement des références et des renvois exprès à ces termes dans différents documents :

- **Loi dite Hadopi**, la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet précise ainsi que la Haute Autorité, dite l'Hadopi «évalue, en outre, les expérimentations conduites dans le domaine des technologies de reconnaissance des contenus et de **filtrage** par les concepteurs de ces technologies la matière, notamment pour ce qui regarde l'efficacité de telles technologies, dans son rapport annuel prévu à l'article L. 331-14 » ; le rapport Hadopi de février 2013 sur les moyens de lutte contre le streaming et le téléchargement direct illicite énonce que «d'un point de vue technique, la mesure de **filtrage** pourrait passer par l'installation d'un module chez l'utilisateur (plug-in) ».
- **L'arrêté du 27 juin 1989**, relatif à l'enrichissement du vocabulaire de l'informatique dont l'article annexe II définit notamment le **filtrage** comme « mise en correspondance de formes selon un ensemble prédéfini de règles ou de critères ».
- **La circulaire 2004-035 relative à l'usage de l'Internet dans le cadre pédagogique et de protection des mineurs du 18 février 2004** prévoyant « la mise en œuvre d'outils de **filtrage** dans les établissements ou écoles ».
- L'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale qui précise que le filtrage est un des éléments des dispositifs de sécurité des systèmes d'information et des informations traitées par le système lui-même (article 89).

- L'instruction interministérielle n° 901/SGDSN/ANSSI en date du 28 janvier 2015 relative à la protection des systèmes d'information sensibles qui précise que le filtrage, notamment le filtrage applicatif (consistant à inspecter l'en-tête et le contenu des paquets IP), est une des mesures à prendre pour assurer la sécurité des réseaux (objectif 31 et annexe 2).
- Les différents arrêtés, pris en application du code de la défense, fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité[1]. L'annexe I de ces arrêtés fixe les règles de sécurité que les opérateurs d'importance vitale sont tenus de respecter pour protéger leurs systèmes d'information. Parmi ces règles l'une concerne le filtrage, obligeant l'opérateur à mettre en place « des mécanismes de filtrage des flux de données circulant dans ses systèmes d'information d'importance vitale (SIIV) afin de bloquer la circulation des flux inutiles au fonctionnement de ses systèmes et susceptibles de faciliter des attaques informatiques ». L'opérateur doit notamment « définir les règles de filtrage des flux de données (filtrage sur adresse réseau, sur protocole, sur numéro de port, etc.) permettant de limiter autant que possible la circulation des flux aux seuls flux de données nécessaires au fonctionnement et à la sécurité de ses SIIV ».

Le droit Européen reconnaît depuis plus longtemps encore le droit de filtrer :

- **La décision 276/1999 CE du 25 janvier 1999 du Parlement européen et du Conseil** adoptant un plan d'actions communautaires pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la **lutte contre les messages à contenu illicite** et préjudiciable diffusés sur les réseaux mondiaux. Le considérant n°5[2] met en avant le fait que les outils de filtrage constituent des éléments essentiels pour assurer un environnement plus sûr sur Internet[3]. Par ailleurs, ce plan d'action a été prolongé par une période supplémentaire de deux ans, rapportant à six ans la durée de ce plan[4].
- De nombreuses recommandations du **Comité des ministres aux Etats membres** (notamment recommandation 2008-6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des **filtres Internet**, recommandation 2001-8 sur l'autorégulation des cyber-contenus, recommandation 2007-11 sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication).

La **directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union** (dite « directive SRI ») a été implémentée en droit français. Cette directive vise notamment à renforcer les capacités nationales des Etats membres de l'Union Européenne en matière de cybersécurité et à l'instauration de règles européennes communes de cybersécurité dans l'Union pour les prestataires de services numériques. Son article 1 précise en effet que ce texte :

> « a) fixe des obligations à tous les États membres en ce qui concerne l'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

[1] Ces arrêtés datent du 10 juin 2016 pour les secteurs des produits de santé, de la gestion de l'eau et de l'alimentation, du 11 aout 2016 pour les secteurs de l'énergie et des transports du 28 novembre 2016 pour les secteurs de l'audiovisuel et information, des communications électroniques et internet, de l'industrie et des finances, du 10 mars 2017 pour le nucléaire et du 29 mai 2019 pour les activités civiles de l'Etat.

[2] Le considérant n°5 de la décision 276/1999 CE du 25-1-1999 : « Considérant que la promotion de l'autoréglementation de l'industrie et des systèmes de suivi du contenu, le développement des outils de filtrage et des systèmes de classement fournis par l'industrie et une sensibilisation accrue portant sur les services offerts par l'industrie, de même que l'encouragement de la coopération internationale entre toutes les parties concernées, joueront un rôle crucial dans la consolidation de cet environnement sûr et contribueront à lever les obstacles au développement et à la compétitivité de l'industrie concernée ».

[3] Site internet accessible à l'Url www.pointdecontact.net

[4] Décision n° 1151/2003/CE du Parlement européen et du Conseil du 16 juin 2003 modifiant la décision n° 276/1999/CE adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux.

b) institue un groupe de coopération afin de soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance mutuelle ;
c) institue un réseau des centres de réponse aux incidents de sécurité informatiques (ci-après dénommé « réseau des CSIRT ») afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération rapide et effective au niveau opérationnel ;
d) établit des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels et pour les fournisseurs de service numérique ;
e) fixe des obligations aux États membres pour la désignation d'autorités nationales compétentes, de points de contact uniques et de CSIRT chargés de tâches liées à la sécurité des réseaux et des systèmes d'information ».

La **loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité** a transposé cette directive en droit français. Cette loi précise le rôle et les obligations des opérateurs de services essentiels (ci-après « OSE ») et des fournisseurs de services numérique (ci-après « FSN ») en matière de sécurité des réseaux et des systèmes d'information.

L'article 5 de la loi précitée définit les OSE comme des opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services.

La loi définit ensuite les FSN comme toute personne morale qui fournit un service de place de marché en ligne, un service de moteur de recherche en ligne ou un service d'informatique en nuage[5]. Le service d'informatique en nuage vise tout « service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées. »[6]

Dès lors, des sociétés de filtrage pourront être qualifiées de fournisseurs de services numériques lorsqu'elles fournissent un service d'informatique en nuage (i.e. de cloud computing), et entreront donc dans le champ d'application de la directive SRI et de sa loi de transposition.
Seuls les FSN dont les services sont fournis notamment à l'intérieur de l'Union européenne doivent appliquer les dispositions de la loi de transposition de la directive et sous réserve de remplir les deux conditions suivantes, ce qui vise principalement des moyennes et grandes entreprises[7] :

- leur nombre d'employés est supérieur ou égal à 50 ; et
- leur chiffre d'affaires annuel est supérieur à 10 millions d'euros.

Cette loi a été complétée par le **décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique**.

Sont concernés les opérateurs de services essentiels dans les secteurs suivants : l'énergie (électricité, pétrole et gaz), les transports (aérien, ferroviaire, guidé, par voie d'eau, routier), les banques, les infrastructures et marchés financiers, la santé (établissements de soins de santé, y compris les hôpitaux et les cliniques privées), la fourniture et distribution d'eau potable, les infrastructures numériques. Pour les infrastructures numériques, les sous-secteurs concernés sont les suivants :

- les points d'échange internet IXP: service d'interconnexion par appairage pour l'échange de trafic internet ;

[5] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 10.
[6] *Infra*.
[7] Loi n°2018-133 art. 11

- les fournisseurs de services de système de noms de domaines (DNS) : enregistrement et gestion de noms de domaine, hébergement de noms de domaine et service de résolution de noms de domaine ;
- les registres de noms de domaines de haut niveau : attribution des noms de domaine et gestion du registre de noms de domaine de premier niveau et hébergement de zones de premier niveau.

Soumis au contrôle de l'Anssi, les FSN doivent respecter un certain nombre d'obligations que l'on peut regrouper en trois grandes familles :

- l'identification des risques et des systèmes ;
- les mesures techniques et organisationnelles, qui comprennent notamment des mesures destinées à protéger la sécurité du réseau et des systèmes d'information contre les dommages, et notamment les actes malveillants. L'Anssi propose de se référer à son Guide d'hygiène informatique[8] pour la mise en place de ces mesures de sécurité, qui suggère l'installation d'un système de filtrage par catégories d'URLs.
- la gestion et déclaration des incidents. En cas d'incident ayant un impact négatif, l'entreprise devra alors le notifier à l'Anssi.

Au-delà des mots « filtre » et « filtrage », il existe bon nombre de textes qui utilisent d'autres terminologies ou d'autres notions qui sont synonymes de « filtre » ou de « filtrage » :

- **L'article 6 I. – 1 de la loi n°2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique (« LCEN ») retient la formule suivante « **moyens techniques permettant de restreindre l'accès** à certains services de communication au public en ligne ou d'opérer une sélection de ces services »[9]
- Les articles L.331-25 ; L331-26 ; L331-27 ; L335-7-1 et R331-4 du **Code de la propriété intellectuelle** utilisent les termes « **moyens de sécurisation** »[10]
- **L'article L.336-2 du Code de la propriété intellectuelle** vise « toutes mesures propres à prévenir ou à faire **cesser une telle atteinte à un droit d'auteur** ou un droit voisin »
- **Le décret n°2010-1630 du 23 décembre 2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation** destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne
- **L'article 61 de la loi n° 2010-476 du 12 mai 2010 relative à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne** :
  - > « l'arrêt de l'accès à ce service aux personnes mentionnées au 2 du I et, le cas échéant, au 1 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. »
  - > « toute mesure destinée à faire cesser le référencement du site d'un opérateur mentionné au deuxième alinéa du présent article par un moteur de recherche ou un annuaire. »

[8] Anssi, Guide d'hygiène informatique, Renforcer la sécurité de son système d'information en 42 mesures, Septembre 2017, Version 2.0.
[9] LCEN art. 6 I. – 1° : « 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 ».
[10] CPI art. L. 335-12 : « Le titulaire d'un accès à des services de communication au public en ligne doit veiller à ce que cet accès ne soit pas utilisé à des fins de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation des titulaires des droits prévus aux livres Ier et II, lorsqu'elle est requise, en mettant en œuvre les moyens de sécurisation qui lui sont proposés par le fournisseur de cet accès en application du premier alinéa du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

- **L'article L.524-3du Code de la consommation** autorise la DGCCRF à demander à l'autorité judiciaire de prescrire aux hébergeurs ou fournisseurs d'accès à Internet « toutes mesures proportionnées propres à prévenir un dommage ou à faire cesser un dommage causé par le contenu d'un service de communication au public en ligne ».
- **L'article 12 de la loi n° 2014-1353 du 13 novembre 2014** renforçant les dispositions relatives à la lutte contre le terrorisme et la pédopornographie a créé l'article 6-1 de la LCEN, qui prévoit notamment la possibilité pour l'autorité administrative de demander aux hébergeurs et éditeurs de site Internet de retirer les contenus pornographiques de mineurs ou faisant l'apologie du terrorisme, et d'en informer simultanément les fournisseurs d'accès Internet, à qui elle pourra communiquer les adresses électroniques des internautes devant être bloqué à un accès Internet, si le retrait n'a pas été fait sous vingt-quatre heures
- **Un de ses décrets d'application n°2015-125 du 5 février 2015**[11] relatif à la protection des internautes contre les sites provoquant à des actes de terrorisme ou en faisant l'apologie, et les sites diffusant des images et représentation de mineurs à caractère pornographique, pris pour l'application de l'article 6-1 de la loi n °2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique
- S'il concerne expressément les fournisseurs d'accès à Internet, le décret **décrit les modalités de blocage des sites** contrevenant **aux dispositions des articles 227-23 et 421-2-5 du Code pénal** « précise la procédure permettant d'empêcher l'accès des internautes aux sites incitant à la commission d'actes de terrorisme ou en faisant l'apologie et aux sites diffusant des images et représentations de mineurs à caractère pornographique. »

  Il précise notamment que la technique de blocage des sites est celle qui consiste à intervenir sur le nom de domaine.

Depuis la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, le fait de consulter habituellement un site internet mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes, est sanctionné par l'article 421-2-5-1 du code pénal. Bien que ce texte ne renvoie pas directement au filtrage de sites internet, il peut cependant constituer une base juridique à un dispositif mis en œuvre pour filtrer les sites dont la consultation habituelle est prohibée par la loi (dispositif de blocage institué par un employeur ou alerte mise en œuvre dans les établissements d'enseignement par exemple). L'article 706-23 du code de procédure pénale précise que le juge des référés peut prononcer le blocage d'un service de communication au public en ligne pour les faits précités, lorsqu'ils constituent un trouble manifestement illicite, et ce à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir.
Concernant les sites « terroristes » qui pourraient être consultés, des mesures de filtrage peuvent être prises afin de prévenir des comportements de radicalisation. Une alerte automatique pourrait être mise en œuvre afin de transmettre à un service compétent des informations relatives à la consultation de sites internet identifiés comme « radicaux ». Dans l'hypothèse où une telle alerte conduit à collecter et traiter des données à caractère personnel (nom et prénom, horaires et lieux de connexion, etc.) des mesures particulières doivent être prises afin d'assurer la sécurité de ces données et de protéger les droits des personnes. Plus largement, certains services de l'Etat, tels que les préfectures ou encore les référents radicalisation pour l'Education nationale (voir notamment le guide interministériel de prévention de la radicalisation), peuvent intervenir dans la mise en place de certains dispositifs de lutte contre la radicalisation.

[11] Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

CE QU'IL FAUT RETENIR…

NOMBREUX SONT LES TEXTES DE LOI QUI IMPOSENT OU LEGITIMENT LE RECOURS AU FILTRAGE

II. LE DROIT DE FILTRER, CADRE JURISPRUDENTIEL

Le terme de « filtre » ou de « filtrage » est retenu dans plusieurs jugements et arrêts.
Le filtrage a dès les premiers contentieux du web pris un sens tout à fait particulier pour le juge.
L'obligation de filtrage s'est imposée naturellement comme l'une des solutions à l'accès à des contenus/plates-formes illicites dans beaucoup de domaines avec des décisions prises dès l'an 2000 :

- Vente d'objets nazis sur le site yahoo.com accessible depuis la France[12]
- Vente de parfums Christian Dior en dehors de leur réseau de distribution sélectif[13]
- Diffusion de pages à contenus racistes[14]
- Diffusion de propos négationnistes[15]
- Jeux en ligne et paris hippiques[16]
- Site d'hébergement de vidéos (YouTube[17], Dailymotion[18])

Déjà en 2010, **le Président du Tribunal de grande instance de Paris**[19] a ordonné, en application de la loi du 12 mai 2010 relative à la concurrence et à la **régulation du secteur des jeux d'argent et de hasard en ligne**, aux fournisseurs d'accès à Internet, de prendre **« toute mesure de filtrage**, pouvant être obtenue par blocage du nom de domaine, de l'adresse IP connue, de l'URL, ou par analyse du contenu des messages, mises en œuvre alternativement ou éventuellement concomitamment, de manière à ce qu'elles soient suivies de l'effet escompté sur le territoire français ».
La cour d'appel de Paris a reproché à une société de courtage **de ne pas avoir mis en œuvre un filtrage efficace**[20], et le même jour de ne pas avoir détaillé le fonctionnement effectif d'un tel filtrage ni détaillé ses résultats[21]. Dans une décision du 14 décembre 2010, **le Tribunal de Grande Instance de Créteil**[22] a fait injonction à un hébergeur **d'installer sur son site un système de filtrage efficace et immédiat** des vidéos dont la diffusion a été ou sera constatée par l'Institut National de l'Audiovisuel (INA).

Cette jurisprudence en matière de filtrage s'est développée depuis le début des années 2000, en particulier en parallèle du développement de la vente sur Internet, ce qui a posé un certain nombre de problématiques liées à l'accès à des sites illicites. De 2011 à 2014, la position de la jurisprudence en matière de filtrage à l'égard des fournisseurs d'accès à Internet et hébergeur s'est assouplie, avec notamment deux arrêts du même jour de la Cour de cassation. **Il en ressort que les fournisseurs d'accès à Internet ne sont pas astreints à effectuer un contrôle permanent et a priori d'Internet.**[23].

[12] TGI Paris, 22-5-2000.
[13] CA Paris, 3-9-2010 n°08/12822.
[14] TGI Nanterre 24-5-2000.
[15] TGI Paris 20-4-2005, ordonnance de référé Uejf et a. c/ olm llc et a.
[16] TGI Paris, 6-8-2010 RG n°10/56506.
[17] TGI Créteil, 14-12-2010 n°06-12815.
[18] TGI Paris 13-1-2011 n°09-16645.
[19] TGI Paris, 6-8-2010 Président de l'Autorité de régulation des jeux en ligne c/ Neustar et autres, RG n°10/56506.
[20] CA Paris, 3-9-2010 RG n°08/12820, CA Paris, 3 9 2010 RG n°08/12821.
[21] CA Paris, 3-9-2010 RG n°08/12822.
[22] TGI Créteil, 14-12-2010, n°06-12815.
[23] Cass civ-1 7 2012 n° 11-15.165 et 11-15.188

Cette jurisprudence s'inscrit dans la continuité de la jurisprudence européenne[24]. La Cour de justice de l'Union Européenne avait déjà précisé qu'il n'était pas possible de faire injonction à un fournisseur d'accès à internet de mettre en place un système de filtrage de toutes les communications électroniques transitant par ses services, qui s'appliquerait indistinctement à l'égard de toute sa clientèle, et sans limitation dans le temps.

La question de la mise en place des outils de filtrage connaît donc une multitude d'applications jurisprudentielles, à chaque fois que s'est posée la question de mettre en place des mécanismes faisant obstacle à la consultation des sites illicites.

CE QU'IL FAUT RETENIR…

> LES JUGES ORDONNENT COURAMMENT LA TECHNIQUE DE FILTRAGE POUR IMPOSER UNE RESTRICTION D'ACCES

III. LE DROIT DE FILTRER, BONNES PRATIQUES ET NORMES

La Commission Nationale de l'Informatique et des Libertés (CNIL) s'intéresse également au filtrage, notamment aux mesures de filtrage mises en place au sein des entreprises par le biais d'un certain nombre de documents, et en particulier :

- La fiche « Le contrôle de l'utilisation d'internet et de la messagerie électronique », 1er décembre 2015
- Le guide « la sécurité des données à caractère personnel », édition 2018
- Les fiches pratiques « Travail et données personnelles », édition 2018
- L'évaluation des salariés : droits et obligations des employeurs, 11 mai 2011
- La fiche « les outils informatiques au travail », 25 juillet 2018
- L'article de la CNIL sur « l'analyse des flux https : bonnes pratiques et questions », 31 mars 2015

Selon la CNIL[25], si l'utilisation sur les lieux de travail, des outils informatiques à des fins privées est généralement tolérée, elle doit rester raisonnable et ne doit pas affecter la sécurité des réseaux ou la productivité de l'entreprise. Elle précise que rien n'empêche l'employeur de limiter l'accès de ses employés à Internet.

Selon la commission, une telle limitation de l'accès à Internet ne constitue pas par principe une atteinte à la vie privée des employés et se justifie notamment parce que l'usage d'Internet est en général reconnu à condition qu'un tel usage soit, selon elle : raisonnable, ne réduise pas la productivité, ni les « conditions d'accès professionnel au réseau ».

D'un point de vue pratique, la CNIL reconnaît la possibilité de mettre en place des dispositifs de filtrage de sites non autorisés : sites à caractère pédophile, révisionniste, raciste…

[24] CJUE 24-11-2011 aff. C70/10.
[25] CNIL, « Le contrôle de l'utilisation d'internet et de la messagerie électronique », 1-12-2015.

Selon la Commission, l'employeur peut imposer certaines mesures dans l'utilisation des systèmes d'information, justifiées pour la sécurité de l'organisme, telles que : l'interdiction de télécharger des logiciels, de se connecter à des forums « chat », ou d'accéder à une messagerie électronique personnelle, à condition d'en informer les salariés.

En tout état de cause, les instances représentatives du personnel doivent être informées ou consultées avant l'installation d'un dispositif de contrôle de l'activité.

Chaque employé doit être notamment informé :

- Des finalités poursuivies ;
- De la base légale du dispositif ;
- De la durée de conservation des données ;
- Des destinataires des données ;
- De son droit d'opposition pour motif légitime ;
- De ses droits d'accès et de rectification ;
- De la possibilité d'introduire une réclamation auprès de la CNIL.

Elle a rappelé en outre que la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 punit de 5 ans d'emprisonnement et de 300 000 € d'amende l'utilisation, certains dispositifs de captation de données informatiques à l'insu des personnes concernées[26].

Par ailleurs, l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'information) a publié plusieurs documents techniques traitant des outils de filtrage :

- La **note technique portant la Recommandation du 30 Janvier 2013** pour la définition d'une politique de filtrage réseau d'un pare-feu.

  Ce document vise à procurer les éléments organisationnels qui permettent de structurer la base de règles sur lesquelles s'appuie la politique de filtrage réseau appliquée sur un pare-feu d'interconnexion.
  Il est destiné à toutes les personnes ayant pour mission d'élaborer et d'appliquer ou d'administrer des architectures d'interconnexion sécurisées, qui désirent s'assurer que leurs politiques de filtrages réseau appliquées sur les pares-feux sont bien pérennes.

- **La recommandation sur le filtrage des flux HTTPS du 9 octobre 2014** (cf. supra II 3) à laquelle se réfère expressément la CNIL dans son article du 31 mars 2015.

- Les référentiels d'exigences publiés par l'ANSSI et applicables aux prestataires d'audit de la sécurité des systèmes d'information (PASSI), aux prestataires qualifiés en matière de détection des incidents de sécurité (PDIS) et aux prestataires de réponse aux incidents de sécurité (PRIS) prévoient des obligations particulières de filtrage :
  - dans le référentiel applicable aux PASSI, les exigences de l'ANSSI relatives au déroulement d'une prestation d'audit incluent un audit d'architecture consistant en la revue des règles de filtrage et un audit de configuration afin de vérifier la sécurité des configurations des équipements de sécurité « type pare-feu ou relais inverse (filtrant ou non) et leurs règles de filtrage, chiffreurs, etc. » (articles VI.4.1 et VI.4.2 et annexe 3) ;

[26] Fiche pratique Cnil Keylogger : dispositifs de cyber surveillance particulièrement intrusifs, 20 mars 2013.

- le filtrage est au cœur du référentiel applicable aux PDIS dans la mesure où le système d'information du service de détection des incidents de sécurité (service assurant la gestion des incidents, événements et notification au sens de l'article II.1) est organisé en zones de confiance, cloisonnées entre elles par des mécanismes de filtrage, d'authentification et de contrôle d'accès (article II.2). Le filtrage constitue donc un dispositif essentiel afin d'assurer le respect des exigences relatives à la protection de l'information (articles II.3, IV.2.2, IV.3.10 et suivants), la politique de filtrage devant être maintenue à jour en permanence (articles IV.3.7) ;
- le référentiel applicable aux PRIS prévoit de nombreuses exigences relatives au déroulement d'une prestation de réponse aux incidents de sécurité. A ce titre un plan de remédiation (visant à limiter la compromission, enrayer l'activité de l'attaquant et durcir la sécurité du système d'information de la victime) doit être élaboré et devant prévoir un « durcissement de la politique de filtrage » (article VI.6.6). La politique de filtrage est d'ailleurs un prérequis que le commanditaire de l'audit doit fournir au prestataire avant la réalisation de la prestation (annexe 4).

- La note technique « Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu » du 4 août 2016.

  Ce document, qui a pour objectif de proposer un cadre permettant d'assainir la politique de filtrage réseau d'un pare-feu d'interconnexion dont la maîtrise ou la compréhension n'est plus garantie, s'inscrit dans la suite logique de la note technique précitée de 2013. Avec cette note technique, l'ANSSI souhaite s'assurer que les politiques de filtrage, qui jouent un rôle primordial dans la sécurisation des systèmes d'information, soient maitrisées afin d'éviter toute perte de leur contrôle. Une perte de contrôle d'une politique de filtrage d'un pare-feu entrainerait l'autorisation de flux illégitimes. Finalement, maintenir une politique de filtrage compréhensible et cohérente permettrait de réduire les coûts de maintenance du système d'information.

- Guide relatif aux recommandations de sécurisation d'un pare-feu Stormshield Network Security du 27 décembre 2017 (version 2.7.2).

  Ce document a pour objectif de présenter les bonnes pratiques relatives au déploiement sécurisé des pares-feux Stormshield Network Security (SNS), et traitent notamment de la politique de filtrage réseau.

CE QU'IL FAUT RETENIR…

> LE FILTRAGE FAIT ASSUREMENT PARTIE DE CE QU'IL EST CONVENU D'APPELER LES « BONNES PRATIQUES » EN TERMES DE MANAGEMENT DU SYSTEME D'INFORMATION ET DE SA SECURITE.

IV. LE FILTRAGE ET LES USAGES

Le « droit » ne se limite pas aux textes de loi, jurisprudences et normes.

Les tribunaux, lorsqu'ils ont à trancher un litige, s'attachent souvent à étudier les usages au sein même des entreprises. Ces usages donnent en quelque sorte un indice sur la pertinence et la récurrence d'un phénomène.

Or, force est de constater que le filtrage fait l'objet d'un usage réel, voir intensif.

CE QU'IL FAUT RETENIR…

90% DES ENTREPRISES FILTRENT… ET VOUS ?

V. LE DROIT DE LOGUER

Les logs ou les traces sont un corollaire technique des outils de filtrage. Ces outils permettent en effet non seulement de restreindre ou de contrôler des accès à des sites web sur Internet, mais ils permettent également de tracer de manière individuelle ou collective l'usage de l'Internet.

De fait, à côté de l'interrogation légitime relative au droit de filtrer, on peut s'interroger sur le cadre juridique afférent au droit de loguer.

Le droit ne connaît pas le mot « log » mais il retient des notions approchantes comme :

- Les « données relatives au trafic »[27]
- Les « **données de connexion** », pour lesquelles il convient de préciser que la durée de conservation n'a pas été modifiée par le décret du 24 décembre 2014[28]
- Les « **données de nature à permettre l'identification** » prévus à l'article 6 II de la LCEN et énumérées au sein du décret n° 2011-219 du 25 février 2011 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 [29]

La Commission européenne a présenté le 10 janvier 2017 une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, dit « règlement e-privacy »[30].

L'un des objectifs du règlement est d'étendre les règles de protection de la vie privée à des nouveaux services de communications interpersonnelles sur Internet non soumis au cadre réglementaire de l'Union européenne, à savoir la directive « vie privée et communications électroniques »[31]. Le règlement e-privacy précise que la notion de « service de communications interpersonnelles » comprend notamment les « services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service »[32].

[27] CPCE art. L. 34-1 et R. 10-12 et suivants, concernant notamment la gestion des données de trafic par les opérateurs de communications électroniques et assimilés.
[28] Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
[29] Article 6 II de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication de données, modifié par le décret 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.
[30] Proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, 10 janvier 2017.
[31] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.
[32] Proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, 10 janvier 2017, article 4.

Le règlement e-privacy s'applique aux données de communications électroniques « traitées en relation avec la fourniture et l'utilisation de services de communications électroniques dans l'Union, que le traitement ait lieu ou non dans l'Union »[33]. Le règlement s'applique :

- au contenu des données de communications électroniques : « le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son » ;
- aux métadonnées de communications électroniques[34] : « les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les **données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil** produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.»

Les logs ou traces entrent donc dans le champ d'application de la proposition de règlement e-privacy.

Aux termes de l'article 5 de la proposition de règlement, les données de communications électroniques sont confidentielles. Les fournisseurs de services seront tenus d'effacer le contenu de communications électroniques ou anonymiser les données après réception du contenu par le destinataire, ainsi que les métadonnées de communications électroniques lorsqu'elles ne seront plus nécessaires pour assurer la communication[35]

Le projet de règlement interdit l'utilisation des capacités de traitement et de stockage des équipements terminaux et la collecte d'informations provenant des équipements terminaux des utilisateurs finaux. Cette utilisation et collecte sont toutefois autorisées s'ils sont nécessaires à la communication électronique, à la fourniture d'un service de la société d'information, pour mesurer des résultats d'audience sur le Web ou si l'utilisateur final a donné son consentement[36]. La définition de l'utilisateur final couvre les personnes physiques et les personnes morales.

Il en est de même de la jurisprudence :

Dans **un arrêt du 9 juillet 2008**, **la Cour de Cassation**[37] a retenu que les **connexions à Internet** étaient présumées professionnelles : l'employeur peut donc rechercher ces données et ce, hors de la présence de l'employé.
Cette solution a été confirmée mot pour mot dans des arrêts rendus par la **Cour de cassation** le 9 **février 2010**[38] et par la **Cour d'Appel d'Aix en Provence** le **22 février 2013**[39], ainsi qu'implicitement dans un **arrêt du 10 mai 2012** de **la Cour de Cassation** confirmant l'arrêt d'appel.[40]

[33] Proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, 10 janvier 2017, considérant 9.
[34] Proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, 10 janvier 2017, article 4.
[35] Proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, 10 janvier 2017, article 7.
[36] Proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, 10 janvier 2017, article 8.
[37] 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 ».
[38] Cass soc 9-2-2010 n°08-45.253 M. X c/ association Relais jeunes Charpennes : « 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.»
[39] CA Aix en Provence 22 -02-2013 n° 11-09.553 « (…) les connections établies par M. X... sur son site internet pendant son temps de travail et grâce à l'outil informatique mis à la disposition de l'intéressé par son employeur; de sorte que ces connections sont présumées avoir un caractère professionnel et que l'employeur peut les rechercher hors sa présence. »
[40] Cass-soc 10 05 2012 n° 11-11.252

Ces décisions sont devenues la jurisprudence constante consistant à donner **une place résiduelle à la vie privée de l'employé sur son lieu de travail**. Avant de présumer professionnelles les connexions Internet, la haute juridiction avait déjà posé cette présomption pour les dossiers et fichiers informatiques présents sur le poste de travail de l'employé (sauf s'ils sont clairement identifiés comme personnels).

La **Cour de cassation** a apporté une précision importante concernant les connexions Internet de son salarié. Ainsi dans **l'arrêt du 10 mai 2012** précité, elle précise que « si l'employeur peut toujours consulter les fichiers qui n'ont pas été identifiés comme personnels par le salarié, il ne peut toutefois les produire dans une procédure judiciaire, si leur contenu relève de la vie privée sans l'accord de ce dernier. »[41].

La Cour de cassation casse et annule un arrêt de la cour d'appel aux motifs que le fait pour un salarié de se connecter 800 fois en un mois, dont 200 fois en sept jours, à des sites à caractère pornographique depuis un ordinateur mis à sa disposition par son employeur et strictement affecté à un usage professionnel, justifie son licenciement pour cause réelle et sérieuse[42].

Cependant, par un arrêt du même jour, la Cour de cassation a considéré que le licenciement d'un salarié était dépourvu de cause réelle et sérieuse au motif que l'employeur n'avait pas rapporté la preuve que le salarié est bien l'auteur des connexions internet litigieuses[43]. … D'où l'importance de « loguer » les connexions à internet[44].

Ainsi que pour la CNIL :

La CNIL qui utilise les termes de « fichiers logs » ou « fichier de journalisation »[45] a publié un certain nombre de documents relatifs aux logs et notamment :

- **Les fiches pratiques « Travail et données personnelles »**, édition 2018, fait également référence aux fichiers « logs » (les logs de connexion ne doivent pas être conservés plus de 6 mois) ou de journalisation à propos des informations personnelles des utilisateurs auxquelles les DSI ont accès en raison de leurs fonctions ;

- **Le « guide de sécurité des données à caractère personnel », édition 2018**, la fiche n°4 porte sur « Tracer les accès et gérer les incidents ». Cette fiche explique les mesures que doit mettre en place un DSI « Afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit enregistrer les évènements pertinents et garantir que ces enregistrements ne peuvent être altérés. Dans tous les cas, il ne faut pas conserver ces éléments pendant une durée excessive. »

Sont ainsi énumérées les précautions suivantes, qualifiées d'élémentaires par la CNIL :

---

[42] Cass. Soc., 3 octobre 2018, n° 17-13.089.
[43] Cass. Soc., 3 octobre 2018, n° 16-23.968.
[44] On rappellera toutefois que la directive 2006/24 du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques prévoyait l'obligation des fournisseurs de services de communications électroniques accessibles au public ou des réseaux publics de communications de conserver les données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques. Toutefois, cette directive a été invalidé par un arrêt de la CJUE du 8 avril 201444 au motif que « l'ingérence que comporte l'obligation générale de conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel n'était pas limitée au strict nécessaire »[44].

[45] Les fiches pratiques « Travail et données personnelles », édition 2018.

- « **Prévoir un système de journalisation** (c'est-à-dire un enregistrement dans des « fichiers journaux ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important).

- La journalisation doit concerner, au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion.

- Dans certains cas, il peut être nécessaire de **conserver également le détail des actions effectuées par l'utilisateur**, les types de données consultées et la référence de l'enregistrement concerné. »

VI. LE DROIT DES CHARTES D'UTILISATION DES SYSTEMES D'INFORMATION

En quelques années la charte des systèmes d'information s'est imposée comme un élément fondamental en termes de maîtrise des risques liés à l'utilisation par les salariés du matériel et des services informatiques et Internet, mis à leur disposition à des fins professionnelles.

La charte définit les conditions générales d'utilisation par le personnel, du système d'information et de communication et notamment des accès internet, des réseaux et des services multimédias au sein d'une organisation.

La jurisprudence reconnaît une valeur juridique à part entière à ces chartes dont la violation peut aboutir à une sanction du salarié et même justifier son licenciement.

- **Depuis plus de dix ans, la jurisprudence constante y compris de la Cour de cassation, a eu l'occasion de reconnaître la force contraignante d'une charte**.
- Ainsi par un **arrêt du 21 décembre 2006**, la Cour de cassation a considéré que la tentative de connexion sur le poste informatique du directeur de la société, par emprunt du mot de passe d'un autre salarié, constituait « **un comportement contraire à l'obligation de respect de la charte informatique en vigueur** dans l'entreprise, rendait impossible son maintien dans l'entreprise pendant la durée du préavis et constituait une faute grave »[46].
- Dans un arrêt rendu le **15 décembre 2010, la Chambre sociale de la Cour de cassation** a affirmé que la détention de 480 fichiers pornographiques **en violation de la charte informatique** de l'entreprise justifiait le licenciement d'un salarié[47].
- Dans un arrêt rendu le **19 janvier 2012**, **la Cour d'appel de Paris** a relevé que le salarié avait procédé à un usage anormal de l'outil informatique qui lui était confié, en installant des logiciels sur le poste de travail alors que cela était formellement **interdit par la charte informatique**[48].
- A 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 employeur** arguant notamment lui avoir payé de très nombreuses heures de présence sans contrepartie d'un travail effectif.

46 Cass soc. 21-12-2006 n°05-41.165.
47 Cass. soc. 15-12-2010 n° 09-42.691. CA Metz, 10-5-2017, n°17/00255.
48 CA Paris, pôle 6 ch. 5, 19-1-2012 RG n° 07-01754.

- Dans le même sens, il a été reproché à un salarié d'avoir envoyé à ses collaborateurs et via sa messagerie professionnelle, un courriel portant préjudice à l'image du groupe, alors même que la charte informatique de l'entreprise interdisait « la diffusion d'informations ou de propos de nature à porter préjudice, de façon délibérée, à l'image du groupe ou de ses partenaires commerciaux ». Dans ce contexte, le licenciement était fondé sur une cause réelle et sérieuse[49].

Une charte informatique déployée comme un règlement intérieur est reconnue juridiquement opposable aux salariés.

Depuis longtemps la CNIL préconise une « charte informatique » comme le document qui pourra préciser les règles à respecter en matière de protection des données et les sanctions encourues en cas de non-respect de celles-ci, de sécurité informatique, mais aussi celles relatives à l'utilisation des moyens informatiques et de télécommunications ((téléphonie, messagerie électronique ou encore Internet)[50]. C'est encore plus vrai avec le Règlement Général sur la Protection des Données Personnelles (RGPD) qui impose de mettre en œuvre des mesures organisationnelles et juridiques pour s'assurer en interne cette protection[51] : même si la charte d'usage des systèmes d'information et de communication n'est pas visée expressément, elle est un élément majeur de ces mesures et des documents « d'accountability ».

Dans un certain nombre de documents, la Commission rappelle la nécessité d'informer les institutions représentatives du personnel et les salariés de la mise en place de moyens de contrôle de leur activité, notamment :

- **Les fiches « Travail et données personnelles »**, édition 2018 dont la fiche « Les outils informatiques au travail » prévoit notamment que l'information des employés sur les outils informatiques mis en place sur les lieux de travail afin de contrôler leurs activités peut se faire notamment par une charte informatique, annexée ou non au règlement intérieur.

- **La fiche « Le contrôle de l'utilisation d'internet et de la messagerie électronique »**, 1er décembre 2015. La CNIL recommande ainsi de « porter à la connaissance des salariés (par exemple dans une charte) le principe retenu pour différencier les courriers électroniques professionnels et personnels (qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé, etc.) »

- **Le guide « La sécurité des données personnelles », édition 2018**, comporte la fiche n°1 Sensibiliser les utilisateurs », dans laquelle sont listées les précautions élémentaires à mettre en œuvre pour sécuriser un système d'information. Au titre de ces précautions élémentaires figure la rédaction d'une charte informatique et son incorporation au règlement intérieur.

D'autres autorités préconisent l'utilisation de chartes. Il en est ainsi de **l'Hadopi** qui recommande que **la charte informatique mentionne expressément l'interdiction de la contrefaçon**.

De même, **l'ANSSI, dans sa recommandation sur les flux https du 9 novembre 2014**[52] **ainsi que dans son Mooc SecNumAcademie**[53], prévoit la mise en place d'une charte d'utilisation des moyens informatiques et de communication électronique pour les employés et également une charte administrateur pour l'accès aux données cryptées.

49 CA Toulouse, 29 09 2017, n° 2017/824.
50 Cnil, Guide « La sécurité des données personnelles », Edition 2018.
51 Règlement n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, articles 24, 25, 28, 32.
52 Recommandation de l'ANSSI Flux HTTPS n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.
53 https://secnumacademie.gouv.fr/

Au-delà de la nécessité de définir des règles du jeu dans l'entreprise, **le phénomène des chartes s'est vu renforcé par l'adoption d'un certain nombre de référentiels ou de normes** telles que la **norme 27001** relative au management de la sécurité du SI et le **référentiel général de sécurité** (RGS), dans sa version 2.0 publiée par arrêté du Premier ministre du **13 juin 2014** et applicable depuis le **1er juillet 2014**, qui préconisent l'adoption d'une charte informatique.

Selon l'étude 2014 sur les menaces informatiques et les pratiques de sécurité en France réalisée par le CLUSIF (Club de la sécurité de l'information français), le nombre d'entreprises ayant formalisé leur politique des Systèmes d'information est resté stable depuis 2010 (64 % en 2014 contre 63 % en 2012 et 2010).

Pourtant, les incidents liés aux systèmes d'information se sont multipliés depuis ces dernières années et notamment celles dues à une défaillance au sein même de l'entreprise, les pannes d'origines internes étant passées de 25 % à 35 % entre 2012 et 2014[54].

CE QU'IL FAUT RETENIR…

> LA CHARTE INFORMATIQUE PERMET DE FIXER LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION. ELLE EST OPPOSABLE AUX SALARIES EN CAS DE LITIGE SI ELLE EST DEPLOYEE COMME UN REGLEMENT INTERIEUR

VII. LE CLOUD ACT

Le 22 mars 2018, le Congrès des Etats-Unis a adopté le « Clarifying Lawful Overseas Use of Data », autrement appelé le « Cloud Act »[55], réformant le « Stored Communications Act » de 1986.

APPLICABILITE DU CLOUD ACT

Le Cloud Act permet aux organes gouvernementaux américains (qui réunissent tant les départements fédéraux, tels que la CIA, la NSA ou le FBI, que les services locaux des états, et leurs sous-divisions politiques)[56] de requérir la communication de données hébergées aux Etats-Unis ou en dehors auprès de prestataires de services de communications électroniques ou de services informatiques à distance.

> Procédure

Il est important de rappeler que ces prestataires peuvent volontairement communiquer le contenu d'une communication à un organisme des forces de l'ordre, s'ils ont obtenu le consentement de leur client ou abonné, ou s'ils ont obtenu ce contenu par inadvertance et que ce contenu serait susceptible de porter sur la commission d'un crime[57].

[54]Rapport CLUSIF Menaces informatiques et pratiques de sécurité en France, Édition 2014, M. MOURER Lionel, Mme COURTECUISSE Hélène et M. PRISO Serge.

[56] United States Code, Titlte 18, Ch. 121 : STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS, §2711. Definitions for chapter, (4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.

[57] United States Code, Titlte 18, Ch. 121 : STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS, §2702. Voluntary disclosure of customer communications or records : « A provider described in subsection (a) may divulge the contents of a communication (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the

Ces organes gouvernementaux peuvent demander la communication de données sous certaines conditions.

- Sur la base d'un mandat délivré par un tribunal compétent conformément à la procédure pénale américaine (fédérale ou régionale). Dans ce cas, le client ou abonné concerné n'en sera pas préalablement informé.
- Sur la base d'une « assignation administrative », autorisée par une loi fédérale ou régionale ou par un grand jury fédéral ou régional.
- Sur la base d'une assignation à comparaître.
- Sur la base d'une ordonnance d'un tribunal, il sera tenu de notifier préalablement le client ou l'abonné concerné[58].

Dans ces trois derniers cas, le client ou l'abonné devra être préalablement informé par l'organe requérant.

Sur quels motifs ?

Selon la Cloud Act, les demandes de communication des organes gouvernementaux doivent poursuivre un objectif précis, celui de protéger la sécurité publique et de lutter contre la criminalité, y compris le terrorisme[59].
Le champ d'application de cette loi apparait donc très large, et ne semble pas limité aux enquêtes pénales ou aux actions contre le terrorisme ce qui n'est pas sans rappeler le Patriot Act.
Le Patriot Act, adopté par les Etats-Unis le 26 octobre 2001, et dont l'objectif était de lutter contre le terrorisme[60], a fait l'objet d'une importante polémique ces dernières années. Une enquête[61] a en effet révélé que le FBI avait utilisé cette loi pour d'autres finalités que la lutte contre le terrorisme. Sur le fondement de la section 215 du Patriot Act, les agences gouvernementales demandaient aux opérateurs de téléphonie de leur fournir l'intégralité des métadonnées téléphoniques de leurs clients américains. Ainsi en 2013, sur 11 129 demandes de requêtes fondées sur le Patriot Act, seules 51 concernaient le terrorisme.
En réponse à cet écart de conduite, le Sénat a voté, le 2 juin 2015, le « USA Freedom Act » visant à modifier certaines dispositions du Patriot Act. Ainsi, la section 215 du Patriot Act a été supprimée afin d'empêcher la collecte de masse des données téléphoniques des citoyens américains.

Prestataires

Les personnes susceptibles de répondre à une requête de communication de la part d'un organe gouvernemental américain sont les « provider of electronic communication service or remote

subscriber in the case of remote computing service; (7) to a law enforcement agency (A) if the contents (i) were inadvertently obtained by the service provider and (ii) appear to pertain to the commission of a crime ».

[58] United States Code, Titlte 18, Ch. 121 : STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS, §2703. Required disclosure of customer communications or records.

[59] Cloud Act (H.R. 4943), Sec. 2 Congressional findings : « to protect public safety and combat serious crime, including terrorism ».

[60] H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[61] Article « Peekaboo, I see you : Government Authority Intended for Terrorism is Used for Other Purposes, MarkJaycox, Electronic Frontier Fondation.

computing service ». Dès lors, sont concernés les fournisseurs de services de communications électroniques ou de services informatiques à distance[62].

Sont définies dans le Code des Etats-Unis (« US Code »*)* les activités de ces prestataires :

- Les services de communications électroniques sont définis comme « tout service qui permet à l'utilisateur de ce service d'envoyer ou de recevoir des communications filaires ou électroniques »[63] - ce qui vise aussi les opérateurs de téléphonie ;

  En comparaison, l'article 34-1 du code des postes et communications électroniques français ne vise que « 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 ».

- La fourniture de services informatiques à distance consiste dans « la fourniture au public de capacité de service de stockage informatique ou de services de traitements au moyen d'un système de communication électronique »[64].

Concrètement, cela vise notamment :

- les fournisseurs d'accès à internet ;
- les fournisseurs de messagerie électronique ;
- les prestataires qui proposent des solutions d'hébergement dans le cloud.

Les sociétés qui développent un service de filtrage des flux de navigation web sont des éditeurs de logiciels. Toutefois, ces prestataires peuvent déployer leurs services de filtrage de deux façons :

- mode *on-premise*, dans l'infrastructure du client ;
- mode hébergé (SaaS), dans une infrastructure tierce accessible via Internet. Le filtrage sera alors positionné dans le cloud.

Ainsi, les prestataires de services proposant des services de filtrage des flux de navigation web via la technologie du *cloud computing* pourront donc être qualifiés de fournisseurs de services cloud au sens du Cloud Act.

Extraterritorialité

Le Cloud Act a vocation à s'appliquer à un fournisseur de service enregistré sur le territoire américain quel que soit le lieu de localisation des données. Les fournisseurs de services qui relèvent de la compétence des Etats-Unis sont concernés[65] : les sociétés « contrôlées » par des sociétés enregistrées aux Etats-Unis[66]...

[62] United States Code, Bill S. 2383, Section 3, §2713 : « a provider of electronic communication service or remote computing service ».
[63] United States Code, Title 18, Ch. 119, §2510 (15) : « electronic communication service means any service which provides to users thereof the ability to send or receive wire or electronic communications ».
[64] United States Code, Title 18, Ch. 121 : STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS, §2711. Definitions for chapter, (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.
[65] United States Code, Bill S. 2383, Section 2 Congressional Findings : « Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism. Such

Au-delà de cette première hypothèse, la question de savoir si un fournisseur de service étranger peut tout de même être soumis à la compétence des Etats-Unis est plus délicate. En effet, il convient de prendre en considération la coutume américaine consistant à faire appliquer leur droit de manière extraterritoriale. A plusieurs reprises, des entreprises européennes se sont vues sanctionner par les Etats-Unis sur la base de lois extraterritoriales[67].

Le rapport parlementaire Gauvain du 26 juin 2019 souligne que la prudence s'impose, notamment pour les sociétés ayant leur siège social en dehors du territoire américain et n'étant pas contrôlées par une société enregistrée aux Etats-Unis, mais qui proposent au marché américain des services de communications électroniques ou des services informatiques à distance[68]. Dans ce cas, il n'est pas impossible que le Cloud Act soit finalement interprété de sorte à ce que ces sociétés relèvent de la compétence des Etats-Unis. Partant de ce principe, les dispositions du Cloud Act leur seraient applicables.

Nature des données

Le Cloud Act permet aux organes gouvernementaux américains de requérir la communication de données susceptibles de les intéresser, indépendamment de la localisation de ces données. Selon le Cloud Act, les données concernées sont « les contenus de communications électroniques et tous enregistrements et autres informations relatives à un client ou abonné »[69]. Dès lors, les données susceptibles d'être concernées sont de tous les types, et concernent tant les personnes physiques que les personnes morales.

EXCEPTIONS

Procédure de recours

Un recours pour les prestataires concernés si l'application du Cloud Act entre en conflit avec les lois d'un Etat étranger ayant conclu un accord (« executive agreement ») avec les Etats-Unis. La conclusion d'un tel accord implique que l'Etat considéré soit admis au rang des pays qualifiés (« qualifying foreign government »). Or, actuellement, aucun « executive agreement » n'est à ce jour entré en vigueur.

Le recours prévu par le Cloud Act aux fins d'annulation ou de modification des demandes de communication formées par les organes gouvernementaux[70] nécessite la réunion des deux conditions suivantes :

- le client ou l'abonné du prestataire concerné n'est pas un ressortissant américain (n'est pas « United States Person ») et ne réside pas aux Etats-Unis, et
- le prestataire risque de violer la loi étrangère en conflit avec le Cloud Act d'un pays étranger qualifié (« qualifying foreign government »).

---

efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States ».

[66] Afin de préciser la notion de contrôle, un parallèle peut être fait avec le code de commerce français qui définit notamment les notions de filiales, de participation et de sociétés contrôlées : Article L233-1, article L233-2, article L233-3, et article L233-4 du Code de commerce.

[67] En 2014, BNP-Paribas a été condamnée à 9 milliards de dollars d'amende pour ne pas avoir respecté l'embargo avec Cuba et l'Iran.

[68] Rapport parlementaire « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale », Raphaël Gauvain, 26 juin 2019, page 29-30.

[69] United States Code, Bill S. 2383, Section 2383, §2713 : « the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber ».

[70] United States Code, Bill S. 2383, Section 3, §2713, (2) Motion to quash or modify.

La définition de « United States Person »[71] vise notamment tout citoyen ou ressortissant des Etats-Unis, tout étranger ayant une résidence permanente aux Etats-Unis ou encore toute société enregistrée aux Etats-Unis.

Que l'on se rassure, le Cloud Act n'a pas vocation à s'appliquer aux sociétés françaises offrant leurs services uniquement à des clients français ou européens.

La question de savoir quelle solution vont apporter les juridictions américaines aux conflits de lois avec des Etats non qualifiés reste entière.

Réciprocité du Cloud Act

Le Cloud Act offre la possibilité aux gouvernements étrangers, grâce à un « executive agreement » conclu au préalable avec les Etats-Unis, d'avoir accès à certains types de données sur le territoire américain.

Les gouvernements étrangers peuvent demander des informations directement auprès de tout fournisseur de services de communications électroniques ou de services informatiques à distance basé aux Etats-Unis.
La demande de communication émise par le gouvernement étranger doit avoir pour objet l'obtention d'informations relatives à la prévention et à la détection des crimes graves, y compris le terrorisme, ainsi qu'aux enquêtes et aux poursuites en la matière.

Toutefois, la demande de communication ne doit pas concerner un ressortissant américain (« United States Person ») ou une personne qui réside aux Etats-Unis. Les gouvernements étrangers ne pourront pas non plus cibler une personne n'ayant pas la nationalité américaine et ne résidant pas aux Etats-Unis si l'unique objectif est d'obtenir des informations relatives à une personne de nationalité américaine ou résidante aux Etats-Unis.

Cloud Act et RGPD

Le « Cloud Act » semble entrer en conflit direct avec les dispositions du RGPD, ce dernier prévoyant à l'article 48[72] qu'en l'absence de convention internationale applicable, une décision d'une juridiction ou d'une autorité administrative d'un pays tiers à l'Union européenne ne peut imposer un transfert de données à caractère personnel. Toutefois, il est possible de déroger aux dispositions de cet article si «le transfert est nécessaire pour des motifs importants d'intérêt public »[73]. Les motifs importants d'intérêt public doivent être pris en considération au regard du droit en vigueur dans l'Union européenne.

Dès lors, si la requête concerne des données personnelles, y faire droit sur le seul fondement du Cloud Act constituerait une violation du RGPD[74] et représente un risque réel de sanctions pour le prestataire

[71] United States Code, Bill S. 2383, Section 2523 : « the term "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States. ».
[72] Règlement Général sur la Protection des Données, 25 mai 2018, article 48 : « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre ».
[73] Règlement Général sur la Protection des Données, 25 mai 2018, article 49.
[74] Le Groupe de l'article 29 l'indiquait déjà dans son Avis 05/2012 sur l'informatique en nuage en date du 1-7-2012.

concerné, en application de l'article 83 du RGPD[75]. C'est vraisemblablement là le principal argument à l'application du Cloud Act en Europe.

La perspective d'un Cloud Act européen

La Commission européenne travaille à un projet de règlement et de directive qui institueraient un « cloud act européen »[76].
La Commission souhaite proposer une nouvelle réglementation permettant aux autorités policières et judiciaires d'obtenir plus facilement et plus rapidement les preuves électroniques (tels que les courriels ou documents se trouvant sur le cloud), dont elles ont besoin pour la bonne conduite de leurs enquêtes à l'encontre des criminels et terroristes.

Un conflit de loi certain

Il apparaît cependant que le cloud act européen, s'il était adopté, porte intrinsèquement le risque d'un conflit de loi. Si un prestataire recevait concomitamment ou successivement des injonctions contraires d'un juge américain et d'un juge d'un Etat européen, la coopération judiciaire s'avèrera difficile en France d'après le rapport parlementaire précité.

Le prestataire concerné devra alors faire un choix[77] :

- user de recours coûteux pour faire valoir sa bonne foi et ne pas compromettre sa position vis-à-vis de chacun des deux juges. A noter toutefois que les prestataires les plus compétitifs sur le cloud étant américains, on peut penser que l'avantage serait clairement pour le juge américain ;
- ou quitter le marché européen. Suite à l'application du RGPD le 25 mai 2018, certaines entreprises américaines ont déjà fait ce choix avec leurs clients européens.

Un projet de règlement ou directive européen fait sens à l'heure où les conventions internationales font de plus de plus défaut. Cependant, cette règlementation européenne est toujours au stade des propositions et apparait donc insuffisante face aux champions américains du cloud public à bas coût.

Réaction française

De son côté, le député français Raphaël Gauvain a rédigé un rapport visant à rétablir la souveraineté de la France et de l'Europe et de protéger les entreprises des lois et mesures à portée extraterritoriale[78]. Parmi les nombreuses mesures proposées, le rapport souhaite renforcer les outils européens de protection des entreprises européennes face aux demandes des autorités administratives et judiciaires étrangères.

[75] Amende administrative pouvant s'élever à 20.000.000 € ou 4% du CA annuel mondial.
[76] https://ec.europa.eu/commission/presscorner/detail/fr/IP_18_3343
[77] Eric Le Quellenec, cabinet Alain Bensoussan, Article « Vers l'adoption prochaine d'un Cloud act européen ? », 23 août 2018.
[78] Rapport parlementaire, « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale », Raphaël Gauvain, 26 juin 2019.

CHAPITRE II
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, l'accès au web en situation de mobilité, la multiplication des applications SAAS, le développement du télétravail, ou encore la présence d'appareils 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.

I. LES RESEAUX SOCIAUX ET L'ENTREPRISE

Aujourd'hui les réseaux sociaux font partie intégrante du mode de vie des salariés tant au titre de leur vie privée, que comme outils de travail mais aussi comme moyen mi-professionnel-mi-privé de tisser des « réseaux »[79].

Les réseaux sociaux s'intègrent pleinement à l'environnement de travail sous différentes formes comme par exemple :

- Travail en réseaux (networking)
- Prospection commerciale
- Travail en communauté (hubworking)
- Dans les recrutements
- Web TV d'entreprise (ex : Chaine Youtube)
- Communication produit, institutionnelle ou Marque employeur (LinkedIn, Facebook, Twitter, Instagram…)
- Mise en contact professionnelle via plusieurs plates-formes
- Réseau social d'entreprise
- 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 organisation afin d'attirer des prospects, fidéliser les clients…

[79] On peut commencer à parler de sphère mi- professionnelle mi- privée ne faisant que renforcer la complexité du sujet : comment par exemple traiter le cas de salariés qui échangent des messages instantanés pour organiser un pot de départ d'un collègue, ou s'inviter au restaurant d'entreprise ? Que dire de l'application web de gestion des notes ou des tâches ? Les notes électroniques peuvent-elles être traitées comme des cahiers de notes papier personnels ?

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

Toutefois, les propos et informations 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 protection des données personnelles, les incriminations relatives aux STAD[80] 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. Autre phénomène, le développement des « fakenews » ou « fausses nouvelles », auxquels la loi française est préparée depuis longtemps[81].

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 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 ?

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

Mais l'entreprise, 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 professionnelles.

La jurisprudence affluente en la matière s'est stabilisée :

- 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 Facebook[82]. La Cour d'Appel de Reims a constaté que les propos tenus par l'apprenti sur Facebook « auxquels ont accès nombre

[80] Système de traitement automatisé de données

[81] Article 27 de la loi de 1881 sur la Liberté de la presse: « La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros.Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation.» La Loi n°2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information vient enrichir l'interdiction sur le périmètre électoral.

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

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.

- La Cour d'appel de Lyon, le 24 mars 2014 retient la faute sérieuse pour des propos injurieux tenus sur un mur Facebook en libre accès[83].

- De la même manière, la Cour d'Appel d'Aix-en-Provence, le 27 mars 2015, considère que la faute grave était caractérisée pour des insultes sur un mur Facebook dont l'accès n'avait pas été cantonné aux seuls « amis » acceptés, de sorte qu'elles étaient potentiellement visibles par la clientèle ou par d'autres salariés de l'entreprise[84]. Elle a jugé de même, bien que le profil du salarié ne fût pas public, mais qu'il comportait un nombre « d'amis » (179 en l'espèce) dont l'importance ne permettait pas de caractériser une sphère privée d'échanges[85].

- Toutefois la jurisprudence s'est assouplie lorsque les propos injurieux ou diffamatoires du salarié ne sont accessibles qu'à un nombre restreint de personnes qui ont été validées au préalable par le teneur du compte : tout est dans l'art de paramétrer les fonctionnalités de publication (public, amis, groupe, …) : « ayant constaté que les propos avaient été diffusés sur le compte ouvert par la salariée sur le site Facebook et qu'ils n'avaient été accessibles qu'à des personnes agréées par cette dernière et peu nombreuses, à savoir un groupe fermé composé de 14 personnes, de sorte qu'ils relevaient d'une conversation de nature privée, la cour d'appel a pu retenir que ces propos ne caractérisaient pas une faute grave[86].

On peut déduire de cette jurisprudence que le licenciement d'un salarié pour injures publiques ou diffamation pour des propos émis sur un réseau social, ne serait justifié qu'après avoir apprécié le nombre de personnes ayant accès au compte, par exemple en utilisant le faisceau d'indices suivant :

- le caractère ouvert ou non du compte ;
- le nombre de personnes ayant une visibilité sur les propos ;
- le contrôle des personnes ayant accès aux propos

… ce qui pose une difficulté majeure pour l'employeur pour obtenir licitement les informations de compte personnel d'un salarié…

La jurisprudence a également donné droit aux employeurs qui avaient licencié leur salarié pour avoir passé trop de temps sur les réseaux sociaux à partir du système d'information de l'entreprise :

- 41 heures de connexion à des fins non professionnelles sur internet en un mois justifient un licenciement pour faute grave du salarié[87] ;
- L'employeur qui avait constaté plus de 800 connexions internet sans rapport avec son activité professionnelle constituaient des manquements graves du salarié à ses obligations découlant du contrat de travail, était admis à licencier le salarié pour faute grave[88] ;
- La salariée qui s'est connectée plus de 10 000 fois, pendant son temps de travail, sur une période d'un mois, à des sites extraprofessionnels, et notamment des réseaux sociaux

[83] CA Lyon, 24 mars 2014, n° 13-03463.
[84] CA Aix-en-Provence, 27 mars 2015, n° 13-20847
[85] CA Aix-en-Provence, 5 février 2016, n° 14- 13717
[86] Cass. soc., 12 septembre 2018, n°16-11690. Cass. 1re civ., 10 avril 2013, n° 11-19.530 : l'injure publique n'est pas constituée dans la situation d'un salarié qui avait émis des propos injurieux accessibles seulement à des personnes agréées en nombre restreint et ayant une communauté d'intérêts.
[87] Cass. soc., 18 mars 2009, n° 07-44247.
[88] Cass. soc., 21 septembre 2011, n°10-14869.

constitue une utilisation particulièrement abusive d'internet et est constitutive d'une faute grave[89].

- La Cour d'Appel admet qu'un employeur puisse licencier son salarié qui se connecte de manière très fréquente à son compte Facebook durant les heures de travail[90].

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

Sur ce sujet, l'entreprise doit faire preuve d'imagination car les interdictions « traditionnelles » ne sauraient seules les protéger :

- **Interdire l'accès aux réseaux sociaux** durant le temps de travail quel que soit le matériel utilisé, ce qui ne limitera toutefois pas le risque de propos injurieux ou diffamatoires. **La publication d'informations sur des réseaux sociaux à titre professionnel ou à titre privé, au sujet de certaines activités de l'entreprise** (projets spécifiques, activités, résultats financiers, etc…) peut être interdite. 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. De plus, afin d'éviter la propagation des fake news, l'entreprise pourra imposer aux salariés de vérifier avant toute publication, les sources et le contenu de l'information.

Il appartient à l'employeur de définir les règles du jeu quant à l'utilisation des réseaux sociaux et des services web depuis le lieu de travail ou à partir des ressources 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 ET L'AUTORISER A REALISER TELLE OU TELLE OPERATION OU LUI INTERDIRE TELLE OU TELLE AUTRE.

II. LES ACCES INVITES AU RESEAU INTERNET DE L'ENTREPRISE

L'accès à un public tiers au web se développe de plus en plus.
Hier limitée aux cybercafés et à quelques aéroports pionniers dans le domaine des hot-spot (points d'accès sans-fil), aujourd'hui l'accès public au web est partout : salons, restaurants, points d'information public mais aussi gares et hôtels.

[89] Cass. soc., 26 février 2013 n°11-27372.
[90] CA Pau, 13 juin 2013, n°11-02759.

Cette pratique qui s'étend dans les entreprises et administrations permet d'autoriser l'accès à Internet aux visiteurs extérieurs via leurs Wi-Fi. Il est souvent appelé Wi-Fi « invité » ou « visiteur ». Il peut s'agir de prestataires, de clients, de candidats ou encore de partenaires de l'entreprise qui viennent pour la première fois ou occasionnellement et dont le matériel utilisé n'est pas maitrisé par le service informatique.

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**[91]. 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[92].

- **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 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 :

- L'accès limité par un mot de passe complexe et modifié régulièrement et application des recommandations de sécurité de l'Anssi[93] ;

- **La limitation de l'accès à certains sites et services**, par conséquent, mettre en œuvre un système de filtrage

[91] 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. »
[92] CPCE, art ; D98.
[93] Recommandations de sécurité relatives aux réseaux Wi-Fi No DAT-NT-005/ANSSI/SDE/NP du 9 septembre 2013. Voir également pour les établissements de santé : Guide pratique spécifique pour la mise en place d'un accès Wifi Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

- 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

III. LE SHADOW IT

La multiplication des applications SAAS (opérées dans le Cloud) à fait émerger des nouveaux usages dans les entreprises.

Le « shadow IT » se définit comme l'utilisation et/ou le téléchargement par un salarié au sein de l'entreprise d'applications et logiciels informatiques non homologuées par la direction des systèmes d'information (DSI), c'est-à-dire installés à l'insu de celle-ci ou sans sa consultation préalable. Sur le cloud, sont principalement concernées le partage de données et le transfert de fichiers (exemple : l'application Dropbox).

Omniprésent dans les entreprises aujourd'hui, le phénomène du shadow IT s'explique notamment par les raisons suivantes :

- la tendance à la libéralisation de l'usage des nouvelles technologies en entreprise ;
- l'entrée sur le marché du travail des « digital native », qui font preuve d'un haut niveau d'exigence vis-à-vis des applications informatiques ;
- la difficulté de certains DSI à s'adapter aux besoins réels des utilisateurs et à surveiller les réseaux ;
- les possibilités d'implantation de solutions de plus en plus simples et rapides.

Dès lors, l'achat de logiciels passe de moins en moins par les services informatiques qui en portent pourtant la responsabilité. Les entités métiers (exemple : marketing, comptabilité, ressources humaines…) choisissent et souscrivent directement à des services en ligne (gratuitement ou en souscrivant à un abonnement payant). Ces entités métiers sont aptes à juger de la couverture fonctionnelle de ces applications mais n'ont généralement pas les compétences pour juger les conséquences techniques, juridiques ou les risques qui peuvent découler de leurs utilisations.

Le shadow IT emporte un certain nombre de conséquences préjudiciables pour la société concernée. Tout d'abord, il est susceptible de perturber le fonctionnement de son système d'information dans la mesure où il n'existe aucune garantie d'interopérabilité et de cohérence entre celui-ci et les applications utilisées par les salariés. Au contraire, elles peuvent engendrer une consommation importante de la bande passante, un ralentissement des réseaux et des bugs quelconques, ce qui ajoute inéluctablement du travail à la DSI et lui inflige un important coût financier.

Au-delà de ces aspects, le Shadow IT expose la société à des risques non négligeables en termes de sécurité, à plus forte raison s'agissant du recours à des applications en mode SaaS. En effet, il est impossible pour la DSI d'expertiser au préalable les prestataires concernés, ce qui s'avère problématique compte tenu de leur grande diversité et de la grande disparité de leurs offres en termes de qualité. En outre, la DSI ne peut en aucun cas sécuriser des applications dont elle n'a même pas connaissance.

Par conséquent, les services SaaS développés par l'intermédiaire du Shadow IT posent ainsi le problème du risque d'infection par des malware, de fuites de données liés à un hébergement des données non sécurisé ou à l'interconnexion avec le SI, ou encore des violations de confidentialité.

Cette négligence peut également avoir des conséquences juridiques importantes. Par exemple, dans le secteur de la santé, l'envoi de données réglementées à des hébergeurs non habilités est un acte préjudiciable, ou encore, la transmission de données personnelles à des entités situées en dehors de l'Union européenne, sans s'assurer que ces entités sont en conformité avec le RGPD et sans en informer au préalable les personnes concernées etc.

Dans le cas d'un prestataire Saas européen hébergé chez un prestataire US (AWS, …) les données recueillies sont par ailleurs soumises au Cloud Act.

Il s'avère aujourd'hui complexe pour une direction des systèmes d'information de prétendre mettre fin au Shadow IT, étant entendu que des mesures prohibitives pourraient s'avérer bloquantes pour l'activité des salariés et faire l'objet de mesures de contournement. Au contraire, il paraît opportun d'essayer « d'accompagner » le Shadow IT par le biais de mesures telles que :

- la sécurisation accrue du système d'information de l'entreprise, ce qui passe notamment par une amélioration du contrôle du droit d'accès aux applications, l'instauration d'un système de surveillance du trafic réseau et des audits réguliers pour mesurer l'ampleur du Shadow IT
- la sensibilisation et la formation des salariés autour des impératifs de sécurité et des risques générés par le Shadow IT ;
- la planification de règles de gouvernance, indispensables compte tenu de la hausse des cas de recours au mode SaaS. A ce titre, il convient de mettre en avant le rôle consultatif et la force de proposition de la DSI tout en impliquant les différents services dans la politique informatique compte tenu de leurs compétences.

A titre d'exemple, la coopération entre les métiers et les directeurs des services d'information pourrait se formaliser avec une charte permettant de faciliter les échanges et de capitaliser les bonnes pratiques.

Par conséquent, choisir une application sans avoir vérifié au préalable sa conformité aux différentes règlementations applicables, et notamment en matière de protection des données, fait peser sur l'entreprise des risques de sécurité non négligeables : aucune garantie sur le niveau de sécurité du logiciel et des infrastructures.

Il est à noter que lorsqu'il est proposé en Saas, le proxy et le filtrage de contenu occupent une place particulière. En effet en tant qu'outil d'interception du flux web, il accède à tout le contenu web entrant et sortant de l'entreprise. S'il est compromis ou si le prestataire du proxy Saas n'est pas de confiance, toutes les démarches pour lutter contre le shadow IT auront été vaines. Le proxy Saas occupe donc une place particulièrement sensible dans la chaine de confiance, il convient donc de le sélectionner avec une attention particulière.

Ou se porte donc la responsabilité ?

Le premier dont la responsabilité sera recherchée est l'employeur. La responsabilité de l'employeur peut être engagée sur le fondement des lois dites « Hadopi »[94].

L'article L. 336-3 du Code de la propriété intellectuelle issu des lois Hadopi prévoit, en effet, 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 I et II lorsqu'elle est requise ».

L'obligation qui consiste à veiller à ce que l'utilisation des outils ne permette pas de réaliser des actes contrefaçon porte sur « la personne titulaire d'un accès » autrement dit sur l'employeur, car c'est bien lui qui techniquement et juridiquement « dispose » des accès à internet et les met à dispositions de ses salariés ou faisant partie du personnel.

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. Les personnels des métiers informatiques, qu'ils soient directeurs de la sécurité des Systèmes d'information ou administrateurs, peuvent être responsables en cas d'incompétence professionnelle ou de négligence fautive.

Les droits dont disposent le salarié ou l'agent et les circonstances d'utilisation sont également pris en compte par le juge.

À titre d'exemple, un administrateur système réseau d'une association a été licencié pour faute grave après que son employeur ait découvert, par hasard, au cours d'un audit du réseau du système informatique de l'association, la présence de fichiers en provenance d'internet sur le poste de l'administrateur indiquant un téléchargement 24h24 et 7 jours/7 ce qui portait à environ 6 Go d'images, de sons, de vidéos et de progiciels stockés sur son disque dur.

De même, la Cour d'appel de Versailles a jugé qu'était constitutive d'une faute grave le fait d'installer un logiciel permettant le téléchargement illégal d'œuvres musicales à partir de l'adresse IP d'une étude d'huissier de justice, le licenciement en découlant étant dès lors justifié[95].

CE QU'IL FAUT RETENIR

LE RECOURS AUX APPLICATIONS SAAS COMPORTE DE MULTIPLES AVANTAGES : FACILITE DE MISE EN ŒUVRE ET D'EXPLOITATION, EVOLUTIONS FONCTIONNELLES PLUS RAPIDES, ETC… IL PERMET AUSSI DE MODERNISER LE SYSTEME D'INFORMATION AFIN DE FOURNIR AUX UTILISATEURS DES APPLICATIONS PLUS FACILES D'ACCES ET PLUS INNOVANTES. PLUS LES BESOINS DES UTILISATEURS SONT PRIS EN CONSIDERATION, MOINS ILS AURONT TENDANCE A SE SOUSTRAIRE AUX APPLICATIONS ET SERVICES MIS A LEUR DISPOSITION AU PROFIT DE CEUX QU'ILS UTILISENT A TITRE PERSONNEL. SI L'ENTREPRISE NEGLIGE DE REPONDRE AUX BESOINS DES UTILISATEURS, ELLE S'EXPOSE AU SHADOW IT ET A TOUS LES PROBLEMES QU'ILS ENTRAINENT : FAILLE DE SECURITE, DIFFUSION D'INFORMATIONS CONFIDENTIELLES, ILLEGALITE SUR LE STOCKAGE DES DONNEES, … MIEUX VAUT PREVENIR QUE GUERIR.

[94] Il s'agit de la loi Création et Internet favorisant la diffusion et la protection de la création sur internet du 12-6-2009 et de la loi relative à la protection pénale de la propriété littéraire et artistique sur internet du 15-9-2009.

[95] CA Versailles, 31-3-2011, n° 09-00742.

III. 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, commerces en ligne, échanges dématérialisés avec signature électronique de contrats avec les fournisseurs…

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.

Deux traitements de déchiffrement des flux HTTPS peuvent être envisagés par une entreprise :

- le traitement des flux HTTPS sortants : cas dans lequel le déchiffrement HTTPS permet la lecture en clair des requêtes initiées par les employés, depuis le système d'information de l'entreprise, destinées à établir un canal sécurisé avec des serveurs web externes ;
- le traitement des flux HTTPS entrants : cas dans lequel le déchiffrement HTTPS permet la lecture en clair des requêtes initiées par les serveurs web externes et destinées à des serveurs web hébergés au sein du système d'information 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 **note de l'ANSSI**[96] sur le décryptage des flux https apporte des 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 », 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 tels 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 871-1 à L 871-7 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

En conséquence, la mise en œuvre par un employeur d'une solution de déchiffrement d flux HTTPS est susceptible de violer la liberté individuelle des employés.

Plus précisément, le déchiffrement d'un flux chiffré, en particulier lorsqu'il concerne la sphère personnelle sur le lieu de travail, pourrait porter atteinte au secret des correspondances privées, à la protection des données à caractère personnel ou encore à la vie privée des utilisateurs en dehors et dans le cadre du 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.

[96] ANSSI, « Recommandation de sécurité concernant l'analyse des flux HTTPS », n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.

Le code du travail encadre spécifiquement l'information des salariés. A ce titre, il est prévu que « le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés »[97].
Cette disposition est complétée par l'article L.1222-4 du même code.

Il résulte de ces dispositions que, lors de la mise en œuvre d'un mécanisme de déchiffrement HTTPS, l'employeur devra consulter les instances représentatives du personnel, informer les employés et trouver un équilibre entre le respect de leur vie privée et de leurs correspondances avec les exigences de sécurisation du système d'information de l'entreprise. Une attention particulière devra être portée à la recherche d'une solution proportionnée aux objectifs de l'entreprise.

Bien que l'Anssi se soit prononcée en faveur de la légalité de ce procédé, elle l'encadre au travers d'exigences techniques couplées à des recommandations juridiques[98].

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

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

- D'informer les salariés sur la nature des mesures informatiques prises sur le réseau informatique de l'entité et en recueillant leur consentement individuel sur la charte informatique ainsi qu'en consultant les instances représentatives du personnel
- Mettre en place d'un outil de déchiffrement proportionnel et nécessaire par rapport aux finalités annoncées par l'employeur (telles que la sécurité du réseau, la protection des données sensibles de l'entité) qui imposent que les mesures prises soient justifiées par la nature de la tâche et proportionnées à la finalité
- Assurer la sécurité des données déchiffrées par rapport à la protection des données à caractère personnel
- Contrôler l'accès aux outils de déchiffrement (logiciels de déchiffrement, clés de chiffrement des matériels ou des utilisateurs) en particulier lorsqu'une mauvaise utilisation peut engager la responsabilité d'un tiers (salarié notamment). Les accès aux clés de chiffrement notamment lorsqu'il s'agit d'un accès au séquestre des clés des utilisateurs doivent être journalisées et être prévu dans la charte informatique de l'entité
- Faire valider par la direction des systèmes d'information voire une autorité de niveau supérieur
- 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

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 moins intrusifs

[97] C.trav. art. L2323-47 al.3.
[98] Anssi, Recommandation de sécurité concernant l'analyse des flux HTTPS, 9 11 2014.

- **La présence, ou tout du moins la convocation[99] du salarié concerné** en cas de connaissance de contenus considérés comme personnels ou privés[100]

Par conséquent, l'Anssi préconise que la mise en place d'un dispositif de déchiffrement soit encadrée juridiquement :

- par la charte d'utilisation des moyens informatiques et de communications électroniques rédigées par l'employeur, après consultation des instances représentatives du personnel ;
- par une autorisation expresse de l'administrateur à accéder aux contenus déchiffrés moyennant le respect d'une obligation de confidentialité ;
- par une PSSSI envisageant le déchiffrement et éventuellement le cas des sous-traitants.

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** (sur les catégories de personnes impactées par la solution, la nature de l'analyse réalisée, les données conservées, les modalités d'investigation, les sites faisant l'objet d'une liste blanche, l'existence de dispositifs permettant une utilisation personnelle qui ne serait pas soumis à l'analyse des flux), par exemple dans la charte d'utilisation des moyens informatiques. L'information doit aussi préciser les raisons de cette mesure (identification de logiciels malveillants, protection du patrimoine informationnel, détection de flux sortants anormaux)
- Une **gestion stricte des droits d'accès des administrateurs aux courriers électroniques**, lesquels sont présumés avoir un caractère professionnel sauf s'ils sont identifiés comme étant personnels
- Une **minimisation des traces conservées** (ex : fichier malveillant, source, destination, et non identifiants et mots de passe)
- Une **protection des données d'alertes extraites 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 Internet sécurisés ne devant pas être déchiffrés par l'employeur comme par exemple les sites d'organismes de sécurité sociale, mutuelle, laboratoires d'analyses médicales, …

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. CELLE-CI SOIT CONFORME AUX BONNES PRATIQUES DE L'ANSSI ET DE LA CNIL ET QU'ELLE SOIT REALISEE DANS LE RESPECT DU SECRET DES CORRESPONDANCES ET DE LA VIE PRIVEE

[99] Cass, Soc 17 6 2009 n° pourvoi 08-40274.
[100] Cass, Soc 17 5 2005, n° pourvoi 03-40017.

IV. NOMADISME, MOBILITE ET TELETRAVAIL

De plus en plus d'employés ont l'occasion de travailler hors du bureau régulièrement : démocratisation du télétravail, déplacements professionnels etc.
Répondre à un mail sur le quai de la gare via son téléphone mobile, mettre à jour un fichier via sa tablette dans les transports, sont autant de cas d'usages de mobilité qui peuvent concerner les salariés d'une entreprise. Le développement des applications cloud et des services associés, ainsi que l'accès à des WIFI public permettent effectivement aux salariés de travailler partout. En situation de nomadisme, ils accèdent au système d'information de leur entreprise et à Internet. Mais l'accès au bureau dématérialisé via la connexion réseau est fréquemment plus vulnérable que dans l'entreprise.

Par conséquent, la sécurisation de la flotte de devices et la protection du système d'information est un défi pour la DSI. Les enjeux liés à la sécurité et à la confidentialité des données deviennent des sujets de plus en plus critiques.

Des questions se posent :

- L'entreprise est-elle responsable juridiquement des usages internet de ses collaborateurs en situation de nomadisme et de mobilité ?
- Comment réagir en cas de faille de sécurité sur le matériel professionnel d'un salarié, utilisé en dehors de son lieu de travail ?

LE TELETRAVAIL, N'EST PAS JURIDIQUEMENT LE TRAVAIL A DISTANCE

Avant la loi n°2012-387 du 22 mars 2012, il convenait de se référer à l'Accord National Interprofessionnel du 19 juillet 2005 sur le télétravail[101].

La loi n°2012-387 du 22 mars 2012 introduit dans le code du travail les articles L1222-9, L 1222-10 et L1222-11, qui sont en cohérence avec l'Accord National Interprofessionnel du 19 juillet 2005 et qui sont donc désormais applicables aux employeurs et salariés.

La spécificité du télétravail réside dans le fait que le travail est exécuté dans des locaux qui ne sont pas ceux de l'employeur induisant un transfert de responsabilité issue de l'utilisation des moyens informatiques et de communication électronique à la charge des utilisateurs, ce qui a amené à préciser des règles spécifiques au sein de la charte des systèmes d'information.

Le télétravail est défini à l'article L1222-9 du Code du travail comme :

> « toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information et de la communication dans le cadre d'un contrat de travail ou d'un avenant à celui-ci. »

L'article L.1222-10 du Code du travail prévoit des obligations à la charge de l'employeur qui doivent être reprises dans une charte des systèmes d'information et dans un guide sur le télétravail.

Enfin, l'article L. 1222-11 du Code du travail prévoit la mise en place du télétravail lors de circonstances exceptionnelles.

[101] Cet Accord National Interprofessionnel a fait l'objet de deux arrêtés du 30 mai 2006 et du 15 juin 2006 le rendant obligatoire pour tous les employeurs et tous les salariés compris dans son champ d'application

L'Accord National Interprofessionnel du 19 juillet 2005 prévoit d'autres obligations non reprises par la loi n°2012-387 du 22 mars 2012, mais qui continuent néanmoins à s'appliquer :

- l'assurance (audit du contrat d'habitation salarié),
- la sécurité (règles d'hygiène et de sécurité notamment des équipements),
- audit du bail du salarié (vérification que pas d'interdiction d'utilisation des locaux à des fins professionnelles),
- la santé (exigences relatives aux écrans de visualisation, conditions d'ambiance de travail …),
- frais liés à l'activité,
- protection des données,
- l'accès à la formation…

Il conviendra de préciser toutes les règles relatives à ces dispositions dans le guide du télétravail ou dans la charte des systèmes d'information le cas échéant.

Les obligations édictées au sein de la charte des systèmes d'information ont pour objectif de garantir que l'utilisateur fait un usage des moyens informatiques et de communication électronique conforme à la responsabilité qui lui est transférée par le fait d'accomplir son travail à domicile.

Les moyens informatiques et de communication électronique se retrouvent en effet en la possession et sous la garde de l'utilisateur, ce qui n'est pas le cas lorsque le travail est effectué dans les locaux de l'employeur.

De ce fait, l'utilisateur est soumis à une responsabilité accrue et peut se voir sanctionner en cas de non-respect des règles édictées dans la charte des systèmes d'information.

MOBILITE ET TRAVAIL A DISTANCE

La charte informatique de l'entreprise devra également prévoir les situations de mobilité de ses salariés, en dehors des cas de télétravail. A cet égard, dans le cadre de ses déplacements professionnels, et quel que soit leur durée ou leur fréquence, l'utilisateur devra assurer la garde et la responsabilité des moyens informatiques et de communication électronique.

En effet, il convient d'imposer à l'utilisateur un niveau de surveillance et de confidentialité renforcée et d'exiger qu'il adopte une attitude de prudence et de réserve au regard des informations et des ressources du système d'information de l'entreprise qu'il pourrait être amené à manipuler ou à échanger.

La charte informatique peut également prévoir que l'utilisateur doit veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens, les utiliser ou accéder à leurs contenus.

En cas de perte ou de vol de matériels personnels, utilisés pour un usage professionnel, l'utilisateur devra en informer sans délai l'établissement et mettre en œuvre les démarches nécessaires, notamment pour empêcher l'accès aux données professionnelles accessibles via le terminal concerné.

Il est primordial de sensibiliser les salariés aux enjeux de sécurité informatique liés à la mobilité et au télétravail.

L'Anssi a publié un guide « Recommandations sur le nomadisme numérique »[102] afin d'aider les entreprises à mettre en place des mesures techniques de sécurité encadrant la mobilité et le

[102] Anssi, Guide « Recommandations sur le nomadisme numérique », 17 10 2018.

télétravail. Ce guide conseille notamment de prendre en compte dans la politique de sécurité des systèmes d'information (PSSI) :

- l'ouverture du système d'information de l'entité pour les accès distants ;
- la maîtrise des nouveaux flux liés au nomadisme ;
- la maîtrise des équipements de connexion des utilisateurs.

Le guide liste les nombreux risques liés au nomadisme et propose des bonnes pratiques afin de les limiter, notamment :

- Intégrer le nomadisme dans la politique de sécurité des systèmes d'informations de l'entité ;
- Réaliser l'inventaire des activités des utilisateurs compatibles avec le nomadisme ;
- Maîtriser la gestion des utilisateurs nomades ;
- Maîtriser l'équipement d'accès de l'utilisateur nomade ;
- Mettre en œuvre une solution de chiffrement de disque sur les équipements d'accès nomade ;
- Sensibiliser et former les utilisateurs nomades ;
- Mettre en œuvre des matériels et des logiciels disposant d'un visa de sécurité de l'ANSSI;
- Respecter les recommandations du guide d'administration sécurisée de l'ANSSI pour le SI de l'entité incluant le SI nomadisme ;
- Intégrer une politique de MCO et MCS[103] pour le SI nomadisme ;
- Prévoir une supervision de l'état du parc des équipements d'accès nomade ;
- Mettre en place une journalisation des différents éléments du SI nomadisme en suivant les recommandations du guide de l'ANSSI ;
- Mettre en place un système d'analyse et de corrélation d'évènements du SI nomadisme ;
- Mettre en œuvre une sonde de détection dans le SI nomadisme.

V.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[104].

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 2018, l'usage des équipements personnels BYOD est interdit pour 72% des entreprises[105]. L'Anssi dans ses recommandations en matière de nomadisme et dans son Mooc SecNumAcadémie, déconseille fortement de l'autoriser :
« L'utilisation d'équipements personnels par l'utilisateur (AVEC 3 en français ou BYOD 4 en anglais) pour se connecter au SI de l'entité est donc à proscrire. Cela est justifié entre autres pour les raisons suivantes: l'impossibilité de garantir le niveau de sécurité de l'équipement personnel ; la multiplication des environnements utilisateur, qui rend la gestion du cycle de vie des applications difficile (navigateurs Web, interfaces homme-machine, etc.) ; la complexité de l'investigation en cas d'incidents. »

[103] Maintien en condition opérationnelle / Maintien en condition de sécurité.
[104] Définition Légifrance.
[105] Rapport CLUSIF « Menaces informatiques et pratiques de sécurité en France », Édition 2018, M. MOURER Lionel, M. MONEGER Stéphane et M. NOTIN Jérôme.

Selon une étude réalisée par Verizon, une entreprise sur trois admet qu'elle a déjà subi une intrusion à cause d'un terminal de sa flotte mobile[106].

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

Légifrance donne toutefois une définition de cette pratique dans son « Vocabulaire de l'informatique et des télécommunications » : « se dit de l'utilisation, dans un cadre professionnel, d'un matériel personnel tel qu'un téléphone multifonction ou un ordinateur ».
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 appareils en BYOD entraine la disparition de frontières claires entre usages 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 ?

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, s'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 :

[106] Rapport Verizon, « Mobile Security Index », 2019.

- 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[107].

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.

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, par exemple prévoir le mode de navigation « privée », l'obligation de créer des répertoires marqués professionnels, de marquer les contacts pro/personnels, rappeler le droit à la déconnexion professionnelle, …
- **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

[107] Cass. soc. 2 4 2014.

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[108].
- Il en résulte que l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié.
- Toutefois, une décision plus récente de la Cour de cassation vient tempérer la jurisprudence : dans cet arrêt, la chambre sociale confirme la décision de la Cour d'appel de Nouméa (12 novembre 2015) qui avait décidé d'écarter "l'existence de toute faute commise par le salarié concernant la copie, invoquée par l'employeur, de fichiers du serveur de l'entreprise au moyen de sa clé USB personnelle" et considéré que « le seul fait que le salarié n'obtempère pas, sur le champ, à l'injonction que lui a fait l'employeur de lui remettre sa clé USB personnelle afin de vérifier son contenu, ne constitue pas en soi un comportement fautif »[109]. La Cour d'appel avait souverainement estimé que le grief imputé par l'employeur au salarié d'appropriation sur sa clé USB personnelle d'informations à caractère confidentiel n'était pas établi. A charge maintenant pour l'employeur d'établir que le salarié s'est effectivement approprié des fichiers confidentiels sur sa clé USB personnelle s'il souhaite pouvoir contourner le refus du salarié de remettre sa clé USB.
- **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[110].

  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 professionnelles**, 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.

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[111].

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 2019[112].

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 :

[108] Cass soc., 12 2 2013, n° 11-28649
[109] Cass. soc. 5 07 2017, n° 16-12.386.
[110] Cass.-soc., 23 05 2012, n° 10-23521
[111] Cass soc 23 5 2007 n° 05-17.818.
[112] http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/byod-quelles-sont-les-bonnes-pratiques/

- **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.
- Cloisonner les parties de l'outil personnel ayant vocation à être utilisées dans un cadre professionnel (création d'une « bulle de sécurité »).
- Contrôler l'accès distant par un dispositif d'authentification robuste de l'utilisateur (si possible à l'aide d'un certificat électronique, d'une carte à puce, etc.).
- Mettre en place des mesures de chiffrement des flux d'informations (VPN, HTTPS, etc.).
- Prévoir une **procédure en cas de panne/perte du terminal personnel** (information de l'administrateur réseau, mise à disposition d'un équipement alternatif professionnel, effacement à distance des données professionnelles stockées sur le terminal personnel).
- Exiger le **respect de mesures de sécurité élémentaires** telles que le verrouillage du terminal avec un mot de passe conforme aux bonnes pratiques et l'utilisation d'un antivirus à jour.

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 gratuit 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.
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.

CHAPITRE 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.

I. 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

II. QUELS 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**[113], 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

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

- De **conserver les données d'identification** énumérées au sein du décret n °2011-219 du 25 février 2011[114] 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

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

Le risque civil

[114] Décret modifié par le Décret n ° 2014-1576 du 24 12 2014

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 L336-3 précité, exclut dorénavant la sanction pénale : » Le manquement de la personne titulaire de l'accès à l'obligation définie 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. »

Mais l'article général 121-2 du Code pénal reste applicable et 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 (fournisseur de moyens), pour des accès illicites, par ses organes ou représentants et pour le compte de l'entreprise :

- 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[115]. 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

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

- 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

III. QUI EST RESPONSABLE ?

LA RESPONSABILITE DE L'EMPLOYEUR

Sur le plan 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.

La Cour d'appel d'Aix-en-Provence a condamné une personne pour contrefaçon de marque ainsi que son entreprise aux motifs que le site internet litigieux a été créé sur le lieu de travail du salarié avec les moyens informatiques que son employeur lui a fournis. L'entreprise a été déclarée responsable en sa qualité de commettant de la création par son salarié d'un site internet personnel illicite[116].

Dans le même sens, le TGI de Marseille a condamné l'employeur d'un salarié ayant créé un site Internet litigieux, pour avoir mis à disposition de son salarié les moyens techniques nécessaires à la mise en ligne du site en question, peu importe que le salarié ait agi en dehors de ses attributions professionnelles[117].

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[118] :

[116] Aix-en-Provence, 13 3 2006, n° 03/15440.
[117] TGI Marseille, 11 6 2003.
[118] Cass. ass. plén. 19-5-1988 pourvoi n° 87-82654.

- 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 faisant jurisprudence retenant la responsabilité de l'employeur au motif principal que[119] :

- « 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 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 milite 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.

Sur le plan 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 ?

[119] CA Aix-en-Provence 2e ch. 13-3-2006.

- **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**[120] » 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

[120] 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. ».

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 :

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 expresse 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[121]) ?

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 :

- 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**[122], 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[123].

La jurisprudence a estimé que dans ce cas **la faute personnelle n'est « pas dépourvue de tout lien avec le service »**[124]

Le premier dont la responsabilité sera recherchée est l'employeur

[121] Code pénal, art. 227-23 et 227-28-1
[122] CE 26 juill. 1918, Épx Lemonnier.
[123] Dalloz encyclopédie « Répertoire de la responsabilité de la puissance publique -Faute des agents et responsabilité administrative » – Jean-Pierre DUBOIS – avril 2014.
[124] CE 18 nov. 1949, Demoiselle Mimeur, Lebon 492 ; JCP 1950. II. 5286, concl. Gazier).

LA 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
- 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[125].

[125] Cass soc 15 12 2010 n ° 08-42486

- **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[126].
- **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[127].

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

- Constitue une faute grave l'usage à titre personnel de l'outil informatique mis à sa disposition par l'employeur à des fins personnelles en violation du règlement intérieur de l'entreprise et de la charte informatique qui y est annexée par un administrateur système chargé de faire respecter ces règles. Le contrôle du disque dur dénommé « Perso » ayant permis de constater cet usage abusif est licite : cette dénomination ne peut conférer un caractère personnel à l'intégralité des données qu'il contient[128].

- Une violation délibérée et répétée de la charte informatique en vigueur au sein de l'entreprise (qui en l'espèce proscrit la connexion à certains sites ludiques) justifie le licenciement de la salariée pour faute grave[129].

- Dans un arrêt plus récent du 22 février 2018, la Cour européenne des droits de l'homme a confirmé la radiation d'un employé aux motifs que son employeur avait accédé à son poste de travail et y avait découvert, dans un répertoire « données personnelles », notamment 1 562 fichiers à caractère pornographique. L'employé a saisi le conseil des prud'hommes d'Amiens pour que son licenciement soit déclaré dénué de toute cause réelle et sérieuse. Le conseil a estimé que la décision de l'employeur était justifiée, les fichiers n'ayant pas été dûment identifiés comme « privé » en référence à la charte informatique. La Cour d'appel et la Cour de cassation ont toutes deux confirmé cette décision[130].

- La Cour d'appel de Rouen constate que le règlement intérieur et la charte relative à l'utilisation des systèmes d'information applicables au sein de la société rappellent en des termes généraux que les moyens mis à disposition par l'employeur ont un usage professionnel. En l'espèce, le salarié reconnaît avoir transféré à plusieurs reprises des courriels

[126] Cass soc 15 12 2010 n ° 09-42.691
[127] CA Versailles 31-5-2011 Mickael P. c/ Mireille B.P.
[128] CA Paris 10 04 2014, n°11/04388.
[129] CA Aix en Provence, 13 01 2015 RG 1 0/2106.
[130] Cour européenne des droits de l'homme, 5ème section, arrêt du 22 février 2018, M. X. / France.

professionnels sur sa boîte personnelle. Toutefois, cela ne suffit pas à établir le grief, le licenciement est jugé sans cause réelle et sérieuse[131].

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[132], 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[133], 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[134], 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 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.

[131] CA de Rouen, 31-12-2019 n° 16/04938.
[132] CA Nîmes 26 07 2016 n° 15/04114.
[133] CA Aix-en-Provence 8 juillet 2016 n° 2016/473.
[134] CA Nancy 22 juillet 2016 n° 14/00624.

ROLE ET RESPONSABILITE DES ADMINISTRATEURS / DSI

Le rôle des administrateurs

Comme le précise la CNIL dans sa fiche **« Travail et données personnelles »**[135], 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 »[136], 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. »[137].

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[138]. 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[139]. En revanche, si un fichier est identifié comme personnel, l'employeur ne peut y avoir accès « qu'en présence du salarié ou si celui-ci

[135] CNIL, Fiche « Travail et données personnelles », édition 2018.
[136] Fiche pratique CNIL « Peut-on accéder à l'ordinateur d'un salarié en vacances », 19 juillet 2010.
[137] Recommandation de l'ANSSI Flux HTTPS n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.
[138] Cass. 18-3-2003.
[139] Cass. 18-10-2006.

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**[140].

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[141] 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.

- Le tribunal correctionnel d'Annecy en date du 4 décembre 2015 a condamné un administrateur qui s'est introduit et maintenu frauduleusement dans le système d'information de l'entreprise, de manière intentionnelle. Il a accédé à des serveurs et consulté des fichiers sans lien avec sa fonction, s'y est maintenu dans une intention autre que celle d'exécuter son travail habituel, et a consulté les emails de sa DRH. Il l'a fait en toute connaissance de cause et en violation de la charte informatique de l'entreprise. Selon le tribunal, l'interception, l'utilisation et le détournement de la correspondance électronique de mauvaise foi sont caractérisés[142].

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

[140] 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 ».
[141] CA Paris 22e ch. C 4-10-2007 RG 03/12345.
[142] Tribunal correctionnel d'Annecy, 4 décembre 2015.

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. 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[143], 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 » (par exemple en répondant à un message s'affichant à l'écran)

- **Tracer les opérations de maintenance** : l'utilisateur doit pouvoir constater si la prise de main à distance est en cours et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

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

[143] CNIL, Guide « La sécurité des données à caractère personnel », Fiche n°5 « Sécuriser les postes de travail », Edition 2018.

CHAPITRE IV
PLAN DE DEPLOIEMENT D'UNE SOLUTION DE FILTRAGE

I. ETAPE 1 : LE CHOIX DE LA SOLUTION

Une solution de filtrage pertinente doit être capable de proposer :

- Des **catégories adéquates qui correspondent au droit pénal** du pays et segmentées en fonction des habitudes de navigation des utilisateurs
- Un **taux de reconnaissance** du web élevé (aptitude à reconnaître les sites visités par les utilisateurs)
- Une **qualité du classement** pertinente (choix de la bonne catégorie pour un site au regard de la législation et de la culture du pays)
- **Une protection optimale grâce au filtrage par liste blanche**, en n'autorise l'accès aux seuls sites ayant été reconnus et préalablement qualifiés.

LE BON CHOIX DES CATEGORIES

La législation, les habitudes de navigation ou encore les centres d'intérêts varient d'un pays à un autre.

Or, il est important de s'assurer que la solution de filtrage que l'on souhaite mettre en place permette à l'entreprise de se défendre conformément au droit pénal applicable dans le(s) pays dans le(s)quel(s) elle donne accès à Internet. Pour cela la solution de filtrage doit permettre d'exclure précisément les sites et protocoles illicites.

De même il est indispensable que celle-ci prenne en compte les centres d'intérêts extra-professionnels des internautes afin d'apporter une simplicité de création des politiques de filtrage et que celles-ci soient efficaces.

Il faut savoir choisir un outil adapté à son besoin et répondant aux obligations légales et qui collecte des données non discriminatoires

L'IMPORTANCE DU TAUX DE RECONNAISSANCE

En effet, si les URL référencées ne correspondent pas à l'usage du web tel qu'il est fait par l'organisation, cette base ne sera pas pertinente quelle que soit sa taille. Le taux de reconnaissance est l'indicateur le plus fiable pour mesurer l'efficacité d'un outil de filtrage.

Les solutions américaines à vocation mondiale embarquent des bases très volumineuses mais qui incluent les sites les plus regardés dans le monde avec une très grosse proportion de sites anglo-saxons.

Pour le marché français, des sites français comme « tf1.fr » ou « fnac.com » seront référencés mais pas forcément des sites à audience plus locale comme des pages pornographiques sur des blogs français.
Il est intéressant de noter que les 100.000 premiers sites regardés de France représentent 98% du trafic et que 70% d'entre eux sont francophones.

LA QUALITE DU CLASSEMENT : LES SITES DANS LES BONNES CATEGORIES

Le troisième critère d'évaluation est la qualité de classement. L'analyse automatique à base de mots clés ou d'intelligence artificielle conduit trop souvent à des évaluations erronées comme des faux positifs qui se traduisent par du sur-filtrage et donc à un mécontentement des utilisateurs.

Il est important que le classement effectué par l'éditeur soit juste, c'est-à-dire que le site soit classé dans la catégorie dont il est le plus proche. Des pages différentes d'un même site peuvent d'ailleurs être classées dans des catégories différentes (exemple : les portails sont par nature multi-catégories).

L'appréciation de l'appartenance d'un site à une catégorie plutôt qu'à une autre nécessite :

- **Une analyse humaine** (nous avons vu que les techniques d'intelligence artificielle ne sont pas encore assez performantes)

- **Un jugement de valeur** qui soit basé sur un référentiel culturel très proche de l'entreprise utilisatrice

Ce dernier point est très important et favorise aussi les solutions locales. Des éditeurs américains peuvent, par exemple, classer des syndicats dans la catégorie terrorisme/activisme car c'est sincèrement dans cette catégorie que leur jugement de valeur les place. L'impact de ces erreurs de classement peut se traduire, au minimum par du temps pour reclasser certains sites et au pire par des difficultés sociales.

LE FILTRAGE PAR LISTE BLANCHE POUR CREER UN ENVIRONNEMENT DE CONFIANCE

Enfin, la mise en place de politique d'accès de type « liste blanche », c'est-à-dire limiter l'accès aux seules catégories ou sites explicitement autorisés, garantit une protection optimale. L'environnement de confiance ainsi déterminé **offre le plus haut niveau de sécurisation** puisque tous les contenus autorisés auront préalablement fait l'objet d'une analyse.

L'Anssi recommande ce mode de fonctionnement pour les organisations ayant les plus hauts niveaux d'exigence, telles que les OIV (opérateurs d'importance vitale).

Néanmoins, cette approche nécessite une parfaite connaissance des habitudes de navigation pour offrir un taux de reconnaissance des sites visités extrêmement élevé.

L'utilisation du filtrage est non seulement légale mais apparaît dans bien des cas comme étant imposée par la loi.

Sa mise en œuvre doit s'inscrire dans le respect des obligations légales que constituent principalement :

- Le droit de la protection des données
- Le droit du travail

II. ETAPE 2 : LE RESPECT DU DROIT DE LA PROTECTION DES DONNEES PERSONNELLES

LES PRINCIPES DE LA LOI INFORMATIQUE ET LIBERTES

La Loi Informatique et Libertés, vise ce que l'on nomme les données à caractère personnel et les traitements de données à caractère personnel.

Suite à l'adoption du Règlement général sur la protection des données personnelles, entré en vigueur le 25 mai 2018, l'adaptation du droit français au nouveau cadre européen s'est faite en plusieurs étapes:

- modifications de la loi « Informatique et Libertés », par la loi du 20 juin 2018, puis de son décret d'application, par décret du 1er août 2018 ;
- réécriture et mise en cohérence de cette loi, par ordonnance du 12 décembre 2018 ;
- élaboration d'un nouveau décret d'application de la loi, daté du 29 mai 2019 et entré en vigueur le 1er juin.

Ainsi, la loi Informatique et Libertés du 6 janvier 1978 est en vigueur dans une nouvelle rédaction depuis le 1er juin 2019. Elle comporte notamment les dispositions relatives aux « marges de manœuvre nationales » autorisées par le Règlement général sur la protection des données que le législateur a choisi d'exercer.

En vertu **de l'article 2 alinéa 2 et 3 de la loi Informatique et Libertés** :

- **Constitue un fichier de données à caractère personnel : « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.** »

Sauf dispositions contraires, dans le cadre de la présente loi s'appliquent les définitions de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016 (cf. ci-après).**L'article 6 I de ladite loi** précise également des **interdictions en matière de collecte ou de traitement de certaines données** :

- « Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. » »

En application **de l'article 4 de la loi Informatique et Libertés,** les données à caractère personnel doivent être :

- **Traitées de manière licite, loyale**
- Collectées pour des **finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités
- **Adéquates, pertinentes** et, au regard des finalités pour lesquelles elles sont traitées, **limitées** à ce qui est nécessaire
- **Exactes** et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder
- **Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées**.
- Traitées de façon à garantir une **sécurité appropriée** des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées

Dans la mesure où les outils de filtrage permettent d'identifier les comportements de personnes physiques, les informations qu'ils comportent constituent bien des données à caractère personnel au sens de la loi.

Les données des outils de filtrage peuvent être collectées, saisies, enregistrées, consultées, éditées. Elles font donc l'objet d'un traitement.

Par conséquent, un dispositif de filtrage constitue un traitement soumis à la législation relative à la protection des données à caractère personnel.

LES PRINCIPES DU REGLEMENT RGPD

Le Parlement européen a adopté le 14 avril 2016 le règlement général sur la protection des données personnelles 2016/679 (dit « RGPD »). L'objectif du règlement est d'instaurer des mécanismes visant à assurer une application cohérente de la législation en matière de protection des données dans l'ensemble de l'Union européenne. Ce règlement est applicable depuis le 25 mai 2018.

Quatre grands principes structurent le règlement RGPD (articles 5 et 6) :

- le principe de légalité, les données à caractère personnel devant être traitées de manière licite, loyale et transparente au regard de la personne concernée
- le principe de finalité, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités
- le principe de légitimité, les données traitées doivent être exactes, adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Ces données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées
- le principe de proportionnalité, les traitements doivent être proportionnés au regard de la finalité

L'article 4 du RGPD reprend des termes similaires à ceux du droit français pour définir la notion de donnée à caractère personnel qui renvoie alors à « toute information se rapportant à une personne physique identifiée ou identifiable (est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale) ».

Ce même article 4 défini le terme de traitement « comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ». Comme pour la définition de la notion de données à caractère personnel, la définition de ce type de traitement en droit européen est aussi très proche de la définition de la loi française.

LES ACTIONS PREALABLES A METTRE EN ŒUVRE

Schématiquement, pour qu'un outil de filtrage soit mis en œuvre conformément à la loi Informatique et Libertés et/ou au RGPD, les grandes règles doivent être respectées :

- Le droit des personnes
- Tenue du registre de traitements
- L'analyse d'impact
- La sécurité des données

Le droit des personnes

Tant la loi Informatique et Libertés que le RGPD prévoit des obligations relatives au droit des personnes.

Les personnes concernées par un traitement de données à caractère personnel disposent de plusieurs droits au titre de la loi Informatique et libertés et du RGPD :

- Le droit à l'information
- Le droit d'accès
- Le droit d'opposition
- Le droit de rectification
- Le droit à l'effacement
- Le droit à la limitation du traitement
- Le droit à la portabilité des données

La personne dont les données à caractère personnel font l'objet d'un traitement doit être informée, au plus tard au moment de la collecte des données[144] :

- De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant
- Le cas échéant, les coordonnées du délégué à la protection des données
- De la finalité poursuivie par le traitement ainsi que la base juridique du traitement
- Lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers
- Les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent
- Le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

En plus des informations ci-dessus, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :

- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données
- lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci
- le droit d'introduire une réclamation auprès d'une autorité de contrôle
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un

[144] Règlement général sur la protection des données personnelles 2016/679, 14-04-2016, article 13. .

contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données

- l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Cette information peut être réalisée par le biais de la charte lorsqu'il s'agit d'employés par exemple.

Les entités responsables du traitement devront mettre en place une procédure afin de garantir aux personnes concernées l'exercice de leur droit d'accès, de rectification et d'opposition. Ces entités devront aussi prévoir les procédures permettant l'effacement et la portabilité des données à caractère personnel, ainsi que la limitation du traitement.

Au titre du droit d'accès, la personne concernée peut demander l'accès auxdites données à caractère personnel ainsi qu'aux informations suivantes[145] :

- « La confirmation que des données à caractère personnel les concernant font ou ne font pas l'objet d'un traitement

- Des informations relatives aux finalités du traitement ou catégories de données à caractère personnel traitées et les destinataires ou catégories de destinataires auxquels les données sont communiquées

- Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée

- L'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement

- Le droit d'introduire une réclamation auprès d'une autorité de contrôle

- Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source

- L'existence d'une prise de décision automatisée, y compris un profilage

Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées en ce qui concerne ce transfert

- Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement

Ces droits ont pour but « d'encourager la transparence dans l'exploitation des données à caractère personnel »[146].

[145] Règlement général sur la protection des données personnelles 2016/679, 14-04-2016, article 15.
[146] Alain Bensoussan, « Informatique, télécoms, internet » éd. 2014, n°1639.

L'établissement d'un registre

Le RGPD prévoit un allègement des obligations en matière de formalités préalables. La logique de formalités préalables laisse la place à celle de responsabilisation des acteurs.

Ainsi, le RGPD a fait disparaitre les formalités déclaratives auprès de la CNIL au bénéfice de l'obligation de tenir un registre dans les conditions de l'article 30 du règlement. Il conviendra également d'appliquer un nouveau principe, le principe de responsabilité (accountability) selon lequel le responsable du traitement est responsable du respect des principes essentiels du RGPD et doit être en mesure de démontrer que ceux-ci sont respectés (article 5).

Le responsable de traitement comptant au moins 250 employés, devra ainsi tenir un registre des activités de traitement contenant l'identité et les coordonnées du responsable de traitement, les finalités, les catégories de personnes concernées, les catégories de données, l'existence ou non d'un transfert international, les délais prévus pour l'effacement et une description générale des mesures de sécurité techniques et organisationnelles qui ont été prises.

Une analyse d'impact préalable

L'article 35 du RGPD obligera le responsable de traitement à effectuer, avant la mise en œuvre du traitement, une analyse d'impact « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

L'analyse d'impact sera en particulier requise en cas « d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ».

La CNIL a publié une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise[147] et une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise[148].

Parmi les opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, la CNIL mentionne les « traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés ». Elle implique les outils de filtrage en visant « dispositif de cyber surveillance tels que ceux procédant à une analyse des flux de courriels sortants afin de détecter d'éventuelles fuites d'information (dispositifs dits de Data Loss Prevention) ».

En effet, les dispositifs de filtrage peuvent déboucher sur un traitement automatisé de données à caractère personnel qui procède à une « évaluation systématique et approfondie » des connexions internet[149] ; de surcroît, sur le fondement de ce traitement des décisions juridiques concernant directement les salariés peuvent être prises (sanction par exemple).

L'article 35 détaille les modalités de l'analyse d'impact. Cette dernière devra au moins contenir :

[147] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf
[148] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf
[149] Cf art. 35.3.a RGPD

- une description générale des traitements envisagés et des finalités
- l'évaluation de la nécessité et de la proportionnalité des opérations de traitement
- l'évaluation des risques pour les droits et libertés des personnes concernées
- les mesures envisagées pour faire face aux risques.

La sécurité des données

Le principe de sécurité et de confidentialité des données prévoit une obligation de sécurité des données à caractère personnel.

Au titre de la loi Informatique et Libertés [150], le responsable d'un traitement de données à caractère personnel est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès. Des mesures de sécurité et de confidentialité adéquates devront donc être prises (mot de passe, sécurisation des accès physique et logique ainsi que des liaisons…).

La CNIL dispose d'une gamme de pouvoirs élargie pour vérifier que les dispositions de la loi Informatique et Libertés sont respectées. En cas de non-respect des dispositions, la CNIL peut sanctionner le responsable du traitement.

Cette obligation de sécurité des données et des traitements est reprise par les articles 25 et 32 à 34 du RGPD qui imposent la mise en œuvre de « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » telles que la pseudonymisation, l'anonymisation ou la minimisation des données par exemple.

Le principe de minimisation vise à s'assurer que les données traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

L'application de ce principe au filtrage renvoie à ce que, dans l'hypothèse où un traitement de données à caractère personnel est mis en œuvre afin d'identifier le comportement d'une personne, ne doivent être traitées que des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du dispositif de filtrage (exemple : identité, fonctions et coordonnées de la personne concernée et faits signalés par le dispositif automatique de filtrage). La sécurité de ce dispositif sera d'autant plus renforcée si les données traitées sont anonymisées.

De surcroît, l'article 25-1 impose l'obligation de Privacy by design. Ce principe signifie que les aspects de protection des données doivent être pris en compte dès la conception d'un traitement et maintenus en conformité tout au long du cycle de vie de la solution qui assure le traitement. Le Privacy by design est un gage de confiance vis-à-vis des salariés et des partenaires.

A titre d'exemple, il convient de prendre les mesures qui garantissent, par défaut, que les données à caractère personnel traitées au titre du filtrage ne sont rendues accessibles qu'à un nombre déterminé et restreint de personnes (dès la conception et tout au long du cycle de vie de traitement).

LES POUVOIRS DE LA CNIL

La loi Informatique et Libertés telle que modifiée par le RGPD instaurent de nombreux pouvoirs pour la CNIL.

[150] Loi n° 78-17 du 6 1 1978, art.121.

L'article 8 de la loi Informatique et Libertés fixe les missions générales de la CNIL, à savoir :

- « Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations et peut, à cette fin, apporter une information adaptée aux collectivités territoriales, à leurs groupements et aux petites et moyennes entreprises. »
- « Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France. »

L'article 16 de la loi Informatique et libertés précise les pouvoirs de la CNIL en matière de sanction :

« La formation restreinte prend les mesures et prononce les sanctions à l'encontre des responsables de traitements ou des sous-traitants qui ne respectent pas les obligations découlant du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi. »

L'article 19 de la loi Informatique et Libertés définit les modalités de contrôle de la mise en œuvre des traitements.

Aux termes de l'article 33 du RGPD et en cas de violation de données à caractère personnel, le responsable du traitement doit notifier la violation en question à la CNIL si cette violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Aux termes de l'article 34 de la loi Informatique et Libertés, cette obligation de notification n'est applicable qu'aux fournisseurs au public de services de communications électroniques. Cette obligation s'applique donc à tous responsables de traitement, y compris aux sous-traitants qui effectuent un traitement de données à caractère personnel.

LES SANCTIONS

Aux termes de l'article 20 de la Loi Informatique et Libertés, lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant de la règlementation en matière de protection des données personnelles, le président de la CNIL peut, après lui avoir adressé un avertissement ou en complément d'une mise en demeure, saisir la formation restreinte de la CNIL en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes :

- Un rappel à l'ordre
- Une injonction de mettre en conformité le traitement avec les obligations du RGPD ou de la Loi Informatique et Libertés, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte
- La limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du même RGPD ou de la Loi Informatique et Libertés
- Le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée
- La suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale
- La suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes

- Une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du RGPD, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires).

Le non-respect des obligations de la loi Informatique et Libertés constitue également des infractions et peut conduire les tribunaux à prononcer des sanctions pénales.

La sanction encourue varie en fonction de l'obligation non respectée et peut être une contravention ou un délit. La peine maximale encourue est de 5 ans d'emprisonnement et 300 000 euros d'amende[151].

Pour les personnes morales, l'amende encourue est le quintuple de celui prévu pour les personnes physiques.

La loi pour une République numérique intègre[152], comme le RGPD, le principe de proportionnalité du montant de la sanction pécuniaire par rapport à la gravité des manquements commis et aux avantages tirés de ces manquements.

En application des articles 83 et 84 du RGPD, la CNIL pourra imposer, en cas de non-respect du règlement, une amende administrative de 10 000 000 d'euros ou 2% du chiffre d'affaires annuel mondial dans les cas suivants :

- absence de protection des données dès la conception et protection des données par défaut
- absence de représentant établi dans l'union
- absence de registre des activités de traitement
- absence de coopération avec l'autorité de contrôle
- absence de notification à l'autorité de contrôle ou à la personne concernée d'une violation des données
- absence d'analyse d'impact.

L'amende administrative pourra s'élever à 20 000 000 d'euros ou 4% du chiffre d'affaires annuel mondial dans les cas suivants :

- non-respect des principes de base d'un traitement (licéité, loyauté, légitimité, adéquation et pertinence des données, consentement, données sensibles, etc.)
- non-respect du droit des personnes
- non-respect des règles relatives aux transferts de données à caractère personnel.

LE SAVIEZ-VOUS ?

L'OUTIL DE FILTRAGE DOIT FAIRE L'OBJET D'UNE ANALYSE D'IMPACT PREALABLE ET INSCRIT AU REGISTRE DES TRAITEMENTS. L'ACCES AUX DONNEES DE L'OUTIL DOIT ETRE SECURISE.

[151] Code pénal, art. 226-16 et suivants.
[152] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, article 65.

III. ETAPE 3 : LE RESPECT DU DROIT DU TRAVAIL

La mise en place d'une solution de filtrage constitue à la fois :

- **Un outil de contrôle** de l'activité des employés, et doit à ce titre **être porté à leur connaissance**[153]
- Une nouvelle technologie introduite au sein de l'entreprise, et doit en conséquence faire l'objet **d'une consultation des institutions représentatives du personnel**[154]

SIMPLE « DOCUMENT » D'INFORMATION ET/OU CHARTE INFORMATIQUE ?

Dès lors que l'outil de filtrage engendre la collecte des données à caractère personnel, un document doit être rédigé pour informer les salariés de la mise en place de cet outil.

Il n'existe pas de présentation obligatoire quant à la forme permettant d'assurer une telle information.

Ce document peut être une charte communément appelée « charte d'usage des systèmes d'information » ou « charte informatique ».

Cependant, implémenter au sein de l'entreprise ou de l'établissement une telle charte peut nécessiter plus de temps.

La mise à disposition d'un simple document d'information

Dans le but de simplifier ces démarches d'information, il est possible de rédiger un document présentant à minima la nouvelle technologie, les objectifs recherchés, les règles d'utilisation ainsi que la durée de conservation des données collectées.

L'implémentation de ce document simplifié consiste pour l'employeur à respecter les démarches minimums suivantes :

- **Transmettre le document à chaque salarié** individuellement à travers par exemple une note de service, un courrier accompagnant la fiche de paie, un lien inséré sur le site intranet de l'entreprise ou de l'établissement, un outil de diffusion de charte qui permet d'afficher celle-ci à la première connexion Internet du collaborateur…
- **Afficher le document** à une place accessible sur le lieu de travail
- Le comité social et économique est informé et consulté sur les questions intéressant l'organisation, la gestion et la marche générale de l'entreprise, notamment sur « l'introduction de nouvelles technologies, tout aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail »[155] (cela concerne les entreprises d'au moins cinquante salariés)

[153] C. trav. art. L. 1222-4. : « Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »
[154] Code du travail, article L2312-8 4°.
[155] Code du travail, article L2312-8 4°.

Le texte modifié clarifie bien l'étendue de l'information et la consultation du comité social et économique.

Par ailleurs, le comité social et économique est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés[156].

Il convient de préciser qu'un avis négatif du comité social et économique ne fait pas obstacle à la mise en place de la solution, toutefois, le défaut de consultation ou la consultation irrégulière sont constitutifs du délit d'entrave. A défaut d'accord, le CSE est réputé avoir été consulté et avoir rendu un avis négatif à l'expiration d'un délai d'un mois[157].

Si cette démarche simplifiée permet de mettre en place rapidement l'outil de filtrage, le document ainsi implémenté n'est pas opposable à l'employé en ce sens qu'il ne permet pas à l'employeur d'utiliser les informations résultant de l'utilisation de l'outil de filtrage pour prendre une sanction à l'égard du personnel.

La mise en place de la charte d'usage des systèmes d'information ou charte informatique

Dans le but de rendre une charte d'usage des systèmes d'information opposable aux employés et donc « efficace » juridiquement, une procédure d'implémentation spécifique doit alors être suivie.
Eu égard à son objet, consistant notamment à poser des obligations générales et permanentes concernant les conditions d'utilisation des équipements de travail et à la sécurité au sein de l'entreprise, elle doit être considérée comme une adjonction au règlement intérieur[158], si un tel règlement existe déjà.

L'opposabilité de la charte

Pour être opposable aux salariés, la Charte doit être déployée de la même manière qu'un règlement intérieur, dans le respect du code du travail.

Le Droit français établit clairement qu'une charte déployée comme un règlement intérieur est considérée comme tel. Ce document s'impose donc à tous les utilisateurs soumis au règlement intérieur et doit être diffusé comme suit (article L1321-5 du Code du travail) :

- individuellement, avec le bulletin de salaire ou grâce à un outil de diffusion individuelle de la Charte en ligne par exemple,
- collectivement, à une place facilement accessible sur le lieu de travail et/ou sur l'intranet.

La charte informatique est destinée à être diffusé auprès de tous les utilisateurs des ressources informatiques : dès son adoption, à l'arrivée d'un collaborateur et dès sa mise à jour.

Les démarches supplémentaires à destination des entreprises et des administrations employant des agents de droit privé :

[156] Code du travail, article L2312-38.
[157] C. trav. art L2312-16.
[158] C. trav. art. L. 1321-5.

Plus généralement, comme prévu par les articles R1321-2 et R1321-4 du Code du travail, si les salariés dépendent du code du travail, il est également nécessaire de :

- déposer la Charte au Greffe du Conseil des prud'hommes,
- transmettre la Charte à l'Inspection du travail en deux exemplaires.

L'Anssi propose un guide pour accompagner petites et moyennes entreprises (PME) et des entreprises de taille intermédiaire (ETI) dans l'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques avec huit points clés minimum.

Ainsi, les principes suivants doivent respectés dans la mise en œuvre de la charte :

Le principe de discussion collective **en la soumettant à l'avis du comité social et économique**[159] .

Le dossier de présentation au Comité d'entreprise abordera notamment les fondements législatifs et jurisprudentiels de la Charte Internet, son champ d'application, ses principes, ainsi que son déploiement.
Dans l'hypothèse où l'employeur ne requiert pas l'avis du comité social et économique sur l'implémentation d'une charte informatique, cette dernière sera alors inopposable aux salariés.

Un avis négatif n'empêche pas la mise en place de la Charte, en revanche l'absence de consultation constitue un délit d'entrave selon l'article L2317-1du code du travail.

Le principe de transparence et loyauté

Les collaborateurs doivent être informés des moyens de contrôle et de surveillance mis en œuvre : la charte permet cette transparence. Une sensibilisation complémentaire est recommandée.
Aucune information concernant personnellement un collaborateur ne peut être collectée par un dispositif dont l'intéressé n'a pas été préalablement informé.

Le principe de proportionnalité

La charte doit trouver un juste équilibre entre le droit des collaborateurs de disposer sur le lieu de travail et avec les outils informatiques de l'entreprise d'une « vie privée résiduelle », et le droit de contrôle et de surveillance de l'employeur afin de garantir la sécurité des systèmes d'information et limiter ses responsabilités.

Le principe de lisibilité

La charte doit être compréhensible et comprise par tous les collaborateurs quels que soient leur statut et leurs fonctions. Il en va de sa bonne application.

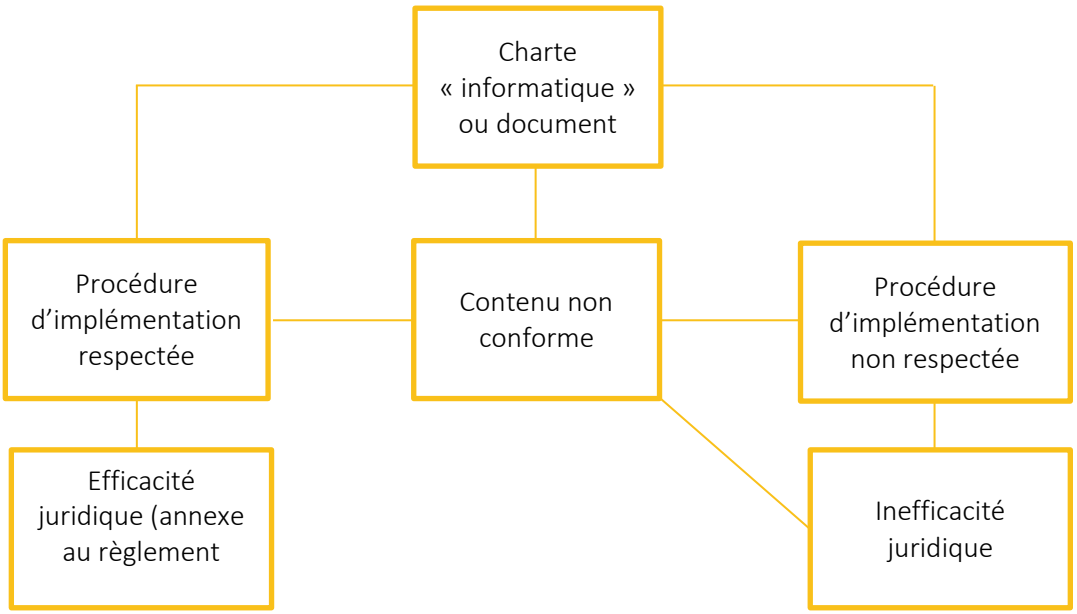
Il est souvent recommandé de prévoir un Livret Technique explicitant les règles techniques, un Guide Juridique explicitant les règles de droit (les textes et la jurisprudence), voire également un FAQ.
Il est également obligatoire de l'afficher à une place convenable et aisément accessible dans les lieux de travail ainsi que dans les locaux et à la porte des locaux où se fait l'embauche.[160]

[159] C. trav. art. L. 1321-4.
[160] C. trav. art. R. 1321-1.

- **Pour les entreprises et les administrations qui emploient des agents de droit privé,** deux étapes supplémentaires sont nécessaires :

  > **La déposer au greffe du conseil de prud'hommes** du ressort du siège social de l'entreprise[161]

  > **La transmettre à l'inspecteur du travail en deux exemplaires**[162]



La modification de la charte

A chaque modification de la Charte, l'ensemble de cette procédure doit être à nouveau déployée.
Pour le Livret Technique ou Guide Juridique, l'avantage non négligeable de ces différents documents est qu'ils n'ont pas besoin d'être soumis aux Instances Représentatives du Personnel.
En ce qui concerne les personnes tierces à l'entreprise qui ont accès à Internet, la charte informatique, constituant une annexe au règlement intérieur, n'est pas par principe opposable aux tiers qui ne sont pas des salariés de l'entreprise.

Dans la catégorie des tiers, il faut distinguer entre :

- **Les tiers intervenant sous contrat de prestations** (exemple : contrat de sous-traitance sur place)

- **Les tiers** pour lesquels il n'y a **pas** nécessairement **de contrat** (par exemple intervention occasionnelle d'un travailleur indépendant)

Concernant les premiers, il est nécessaire d'insérer une clause dans le contrat de prestation de service visant la charte informatique, à charge pour l'employeur principal de la personne de faire respecter la charte.

Concernant les seconds, la seule solution est l'acceptation individuelle de la charte informatique.

[161] C. trav. art. R. 1321-2.
[162] C. trav. art. R. 1321-4.

La procédure d'acceptation individuelle peut être :

- Ecrite
- Par voie électronique suite à l'ouverture d'une session informatique, le cas échéant

Idéalement, il est conseillé de rédiger à côté de la charte du système d'information applicable aux salariés/agents, une « charte des droits d'accès » pour les tiers de l'entreprise. La charte des droits d'accès est un document quasi-identique à la charte informatique mais adaptée aux utilisateurs tiers de l'entreprise et qui prévoit notamment des sanctions adaptées pour cette catégorie d'utilisateurs en cas de non-respect de la charte.

L'adoption d'une charte à destination des personnels ne règle cependant pas tous les problèmes.
Elle ne règle pas le problème des conditions dans lesquelles les personnels des directions informatiques et particulièrement les administrateurs systèmes peuvent ou non déployer les outils, les paramétrer, ou encore accorder à telle ou telle personne une dérogation temporaire ou définitive.

La particularité des chartes dans le secteur public

Le dépôt de la charte informatique au greffe du conseil des prud'hommes est sa transmission à l'inspecteur du travail ne concerne que les personnes soumises au Code du travail.

La procédure d'implémentation d'une charte informatique dans l'administration n'est pas homogène. Elle dépend de la catégorie d'utilisateur au sein de l'administration et de la fonction publique à laquelle il appartient (fonction publique de l'Etat, fonction publique territoriale, fonction publique hospitalière).

Il existe de multiples statuts au sein des organismes publics. Il ne sera abordé ci-dessous que la procédure d'implémentation relative aux agents titulaires de l'Etat (fonctionnaires) et aux agents non titulaires de l'Etat (agents contractuels).

S'agissant des agents titulaires de l'Etat, ces derniers sont notamment soumis à :

- La loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et son article 4 dispose que : « le fonctionnaire est, vis à vis de l'administration dans une situation statutaire et réglementaire ». Leur situation est donc régie de façon statutaire et réglementaire

  En conséquence, leur situation est modifiable par le législateur ou l'autorité administrative détenant le pouvoir réglementaire. Leurs droits et avantages peuvent donc être accrus et leurs obligations et sujétions aggravées en fonction des exigences de l'intérêt général et des besoins du service, et ce par voie législative ou réglementaire

- La loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat

L'article 28 de la loi n°83-634 « portant droits et obligations des fonctionnaires » dispose que :

- « Tout fonctionnaire, quel que soit son rang dans la hiérarchie, est responsable de l'exécution des tâches qui lui sont confiées. Il doit se conformer aux instructions de son supérieur

hiérarchique, sauf dans le cas où l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public

- Il n'est dégagé d'aucune des responsabilités qui lui incombent par la responsabilité propre de ses subordonnés. »

Ce principe d'obéissance est ainsi associé à un principe de la responsabilité du fonctionnaire dans la mesure des tâches et des prérogatives qui lui sont confiées.
L'obéissance hiérarchique impose au fonctionnaire de se soumettre aux mesures prises par le chef de service pour le fonctionnement et l'organisation du service qu'elles soient générales (circulaires, instructions, notes de service...) ou particulières (comme les décisions d'affectation).

La jurisprudence reconnaît au chef de service un pouvoir autonome d'organisation dans le respect de la hiérarchie des normes :

- « Considérant que si, même dans le cas où les ministres ne tiennent d'aucune disposition législative un pouvoir réglementaire, il leur appartient, comme à tout chef de service, de prendre les mesures nécessaires au bon fonctionnement de l'administration placée sous leur autorité [...] dans la mesure où l'exige l'intérêt du service »[163].

L'acte réglementaire est un acte :

- Général
- Impersonnel ou non nominatif
- Visant une fonction, une institution, ou une situation[164]

En l'espèce une charte informatique a vocation à entrer dans la catégorie de l'acte réglementaire, dans la mesure où elle s'applique :

- De manière générale
- Sans distinguer les catégories de destinataires
- A toutes personnes placées dans la situation d'utilisateur des Systèmes d'information

La charte informatique ne doit pas comporter de disposition manifestement illégale, ou compromettante gravement un intérêt public. En conséquence, la charte devrait s'imposer au fonctionnaire, en tant qu'acte réglementaire pris dans le cadre de l'organisation du service.

Cependant, dans le cas où l'acte réglementaire affecterait les droits et obligations statutaires des fonctionnaires ou les prérogatives dont ils bénéficient de par leur appartenance à leur corps, il pourrait faire l'objet d'un recours pour excès de pouvoir « ouvert même sans texte contre tout acte administratif et qui a pour effet d'assurer, conformément aux principes généraux du droit, le respect de la légalité »[165].

La charte doit être adoptée après consultation du comité technique[166] et le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail[167]. Ces comités n'ont qu'un pouvoir consultatif et la décision revient en dernier ressort à l'autorité hiérarchiquement compétente. Néanmoins, leur

[163] CE sec.7-2-1936 n° 433211 Jamart.
[164] Jurisclasseur administratif, fascicule 106-10 Notion d'acte administratif n°10.
[165] CE sec. 17-2-1950 n° 86949 Dame Lamotte.
[166] Article 15 de la loi n°84-16 du 11 janvier 1984.
[167] Article 16 de la loi n°84-16 du 11 janvier 1984.

consultation étant obligatoire dans le cadre d'une charte informatique, le défaut de consultation entacherait la charte d'illégalité.

S'agissant des agents contractuels de l'Etat, ces derniers ne sont pas des fonctionnaires car leur mission prend nécessairement fin, soit par une cessation d'emploi dans la fonction publique, soit par une poursuite d'emploi dans la fonction publique à la suite d'une intégration.

Un agent lié à l'administration peut être un agent public ou un salarié de droit privé.

S'il s'agit d'un agent public, le droit applicable est le droit est le droit public et le juge compétent pour connaître de tout litige est le juge administratif.

Les agents publics non titulaires sont soumis au décret n°86-83 du 17 janvier 1986, et notamment aux articles 43, 43-1, 43-2, 44 du titre relatif à la suspension et la discipline.

Selon les dispositions desdits articles, l'agent non titulaire est soumis, à l'obligation d'obéir aux instructions qui lui sont données, sauf en ce qui concerne les ordres manifestement illégaux et de nature à compromettre l'ordre public[168].

En conséquence, l'agent non titulaire devra se conformer à la charte informatique, de la même manière que le fonctionnaire.

S'il s'agit d'un agent de droit privé, sa situation s'apparente à celle d'un salarié travaillant dans une entreprise. Il est soumis au Code du travail. La procédure d'implémentation de la charte est la même que celle relative aux salariés.

La particularité du personnel informatique

L'ANSSI a publié un guide sur les « Recommandations relatives à l'administration sécurisée des systèmes d'information » le 24 avril 2018. Elle préconise notamment de prévoir une charte informatique spécifique applicable aux administrateurs.

Cette charte devra notamment appeler les administrateurs à la vigilance vis-à-vis des ressources d'administration mises à leur disposition et sur les conduites à tenir en cas de compromission avérée ou suspectée, de perte ou de vol.

Ainsi, les meilleures pratiques en la matière consistent donc à côté de la charte destinée à l'ensemble des personnels, à adopter une charte spécifique dite « charte administrateur » ou encore « charte des droits d'administration ».

Il apparaît nécessaire de responsabiliser l'administrateur aussi bien par la technologie (filtrage, contrôle des accès et des usages) que par un encadrement de la règle du jeu sur un plan contractuel.
La charte administrateur est un complément indispensable à la charte des utilisateurs car si tout administrateur est un utilisateur, tous les utilisateurs ne sont pas des administrateurs ou dotés de droits d'administration.

De fait, il convient de déterminer les droits et obligations des administrateurs et des personnes disposant d'un droit d'administration : ils doivent pouvoir être protégés de tous risques d'atteintes à la vie privée mais également pouvoir être sanctionnées en cas d'abus des moyens dont ils disposent.

[168] Jursiclasseur Administratif Fascicule 193 Agents non titulaires n°65.

La charte administrateur ne repose sur aucune réglementation en particulier, et s'inscrit dans le cadre de la meilleure pratique du moment dans le domaine de la responsabilisation des acteurs de la sécurité des Systèmes d'information.

Le guide de la CNIL « La sécurité des données personnelles », édition 2018 préconise d'adopter une politique spécifique de mots de passe pour les administrateurs et de limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées. En particulier, limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent.

La charte administrateur, faisant l'objet d'une acceptation par l'administrateur, doit nécessairement aborder au minima les thématiques suivantes : les prérogatives, les engagements et les responsabilités de l'administrateur.

Elle permet également de responsabiliser les administrateurs pour leur propre usage étant rappelé que la jurisprudence a déjà sanctionné :

- Un administrateur du réseau informatique pour la présence de fichiers en provenance d'Internet approchant les 6 GO d'images, de sons, de vidéos et de progiciels laissant présager un téléchargement 24h/24 et 7 jours/7 depuis le poste administrateur[169]
- Un administrateur réseau pour atteinte à un système de traitement automatisé de données alors même que l'accès a été rendu possible du fait de sa fonction d'administrateur[170].

LES AUTRES CHARTES SPECIFIQUES A CERTAINS GROUPES DE PERSONNES

Il pourra parfois être nécessaire de prévoir des règles spécifiques à certaines catégories de personnes : les développeurs, les managers (ou la hiérarchie), les personnes extérieures à l'établissement.

Ces personnes n'ont pas les mêmes accès au système d'information (par exemple un accès plus étendu pour les développeurs ou les manager) soit comme personnes extérieures qui ne sont pas soumises au règlement intérieur de l'établissement mais celui de leur propre employeur ou aucun s'il s'agit d'un professionnel indépendant. Ces règles pourront se traduire par des Chartes spécifiques.

CE QU'IL FAUT RETENIR

ADOPTER UNE CHARTE QUI INTEGRE LE FILTRAGE. LA CHARTE NE SE DECLARE PAS A LA CNIL.

LA PROTECTION DES LANCEURS D'ALERTE

La personne, administrateur ou non, en charge de la gestion du filtrage et des éventuelles alertes mises en œuvre peut être confrontée à une situation la conduisant à dénoncer des faits, notamment répréhensibles, à son supérieur hiérarchique ou à une autorité tierce à l'entreprise (exemple : signalement d'un délit commis sur internet). Dans cette hypothèse ladite personne pourrait être qualifiée de lanceur d'alerte. Un régime spécial de protection doit alors s'appliquer conformément à la

[169] CA Paris 22ème chambre, 4 10 2007.
[170] TGI Rennes 21 2 2008 n°03-52216.

loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Un lanceur d'alerte est « une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance » (article 6 de la loi n° 2016-1691).

Le lanceur d'alerte bénéficie d'un régime de protection particulier :

- il n'est pas pénalement responsable s'il « porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte » (article 122-9 du code pénal);
- les procédures mises en œuvre pour recueillir les alertes doivent garantir une stricte confidentialité de l'identité du lanceur d'alerte, des personnes visées par l'alerte et des informations recueillies par l'ensemble des destinataires de l'alerte (article 9 de la loi n° 2016-1691);
- le lanceur d'alerte « ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour avoir signalé une alerte » (article 10 de la loi n° 2016-1691).
- L'article 8 de la loi n° 2016-1691 précise enfin que « le signalement d'une alerte est porté à la connaissance du supérieur hiérarchique, direct ou indirect, de l'employeur ou d'un référent désigné par celui-ci ».
- Si le supérieur ne prend aucune mesure dans un délai raisonnable afin de traiter l'alerte, l'alerte peut être adressée à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. En dernier ressort, l'alerte pourra être rendue publique.

IV. ETAPE 4 : L'ADMINISTRATION ET PARAMETRAGE DE LA SOLUTION

Une fois l'implémentation juridique de la mise en œuvre des outils de filtrage traitée (droit du travail et protection des données personnelles en particulier), encore faut-il que les modalités d'utilisation même de la solution soient respectueuses des dispositions réglementaires.

Plusieurs autres zones de risque juridique sont ici à traiter :

- Le niveau de paramétrage et la qualité des listes d'exclusions
- Le traitement égalitaire des utilisateurs
- L'utilisation précontentieuse ou contentieuse des éléments issus des de filtrage utilisés.

LE NIVEAU DE PARAMETRAGE ET LA QUALITE DES LISTES D'EXCLUSION

Sur la première problématique, il faut rappeler que la constitution de listes d'exclusions n'est pas un acte aussi anodin qu'il n'y paraît.
S'il est normal, voire obligatoire d'interdire l'accès à un certain nombre de contenus (pédopornographie, racisme, révisionnisme, terrorisme, contrefaçon…) certaines restrictions portent en elle l'essence même d'une discrimination.
Ainsi, créer des listes d'exclusion autour de thématiques telles que l'homosexualité pourrait être considéré comme attentatoire aux libertés les plus fondamentales des individus voire discriminatoires ou encore homophobes.

LE TRAITEMENT EGALITAIRE DES UTILISATEURS

Sur la seconde problématique, qui découle de la première, il est essentiel d'assurer le même niveau de paramétrage de la solution pour tous les utilisateurs occupant un même poste, afin de ne pas discriminer les utilisateurs.
Cependant, si de par l'utilisation qu'il fait d'Internet, un utilisateur mettait en péril la sécurité du système d'information de l'entreprise ou de l'établissement, ce motif pourrait justifier une éventuelle intervention de l'administrateur visant à limiter les accès Internet de cet utilisateur.
Sur ce point, il conviendra d'avoir préalablement informé l'employé de cette possibilité, par exemple en prévoyant un paragraphe spécifique dans la charte « utilisateur » à cet effet.

LA CONSERVATION DES PREUVES

Sur la troisième problématique, il faut préciser que le droit de la preuve en matière précontentieuse ou contentieuse est un droit extrêmement rigoureux qui ne laisse la place à aucun doute particulièrement quand il s'agit de sanctionner un employé en application du code du travail.
Les conditions dans lesquelles ces éléments de preuve peuvent être apportés doivent être rigoureusement définies au sein de l'entreprise, dans ce que l'on peut appeler un guide de maintien des preuves.
Ce guide est destiné à centraliser l'ensemble des meilleures pratiques en la matière (appel à un huissier, saisine des autorités compétentes, présence du personnel lors d'opérations de contrôle, conditions dans lesquelles des copies peuvent être réalisées…) et doit donc comporter des mentions particulières s'agissant des informations et données traitées à travers les outils de filtrage.

SENSIBILISEZ VOS COLLABORATEURS

Conformément au principe d'accountability du RGPD, il est fortement conseillé aux entreprises mettant en œuvre des traitements de données personnelles de proposer à ses collaborateurs des formations sur la règlementation en matière de protection des données afin de les sensibiliser et de leur permettre de mieux appréhender les problématiques de protection des données dans leur relation avec les clients, fournisseurs, prestataires de l'entreprise. Cela peut se matérialiser par le suivi d'une formation à travers des parcours de sensibilisation.

V. ETAPE 5 : LA GESTION DES LOGS

Il convient de regarder une combinaison de dispositions afin de répondre précisément à la question de savoir si l'employeur doit conserver les données relatives à l'utilisation d'Internet par ses salariés.

Cette difficulté résulte en particulier de la combinaison des dispositions :

- Du Code des postes et des communications électroniques, modifié par la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant disposition diverses relatives à la sécurité et aux contrôles frontaliers
- De l'article 6 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 et son décret d'application du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne[171]

Ces dispositions visent en partie les mêmes acteurs, dont le fournisseur d'accès, mais selon des approches différentes, qui ne coïncident pas.
L'article 6-I.-1 de la LCEN fait référence notamment aux « personnes dont l'activité est d'offrir un accès aux services de communication ».[172]

De son côté, l'article L. 34-1 du Code des postes et communications électroniques vise :

- Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, dans son alinéa 1er
- Mais également les acteurs « assimilés » à des opérateurs de communications électroniques 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, à l'alinéa 3 du paragraphe II

La définition de l'opérateur telle que prévue par l'article L. 34-1 du Code des postes et communications électroniques apparaît donc beaucoup plus large que celle posée à l'article 6 de la LCEN et il est difficile de déterminer les frontières de la notion de fournisseur d'accès.

Ces difficultés d'interprétation sont d'ailleurs accentuées par l'incertitude persistante quant au champ d'application desdits textes, et leur applicabilité aux employeurs.
Comme il a déjà été précisé, la question n'est en effet toujours pas tranchée s'agissant de la qualification possible de fournisseur d'accès d'un employeur donnant accès à Internet à ses employés, comme le rappelle la jurisprudence[173].

En pratique, afin de préserver sa responsabilité et donc pouvoir de contrôle et de direction, l'employeur doit être capable de retrouver a posteriori si l'origine d'un dommage ou d'un acte illicite ou contrevenant à la charte des Systèmes d'information, provenait de son organisation interne.

Dans ce contexte, et en l'absence de réponse jurisprudentielle claire, il est possible de relever que :

- Le décret n° 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne du 25 février 2011 : portant application de l'article 6 de la loi n° 2004-575 du 25 juin 2004 pour la confiance dans l'économie numérique prévoit dans son article 3 une durée d'un an à compter du jour de la création des contenus
- La CNIL préconise une durée de conservation de six mois s'agissant de la conservation de données permettant le contrôle par l'employeur de l'utilisation d'Internet faite par ses employés (logs de connexions)[174]

[171] Décret modifié par le Décret n ° 2014-1576 du 24 12 2014
[172] Renvoyant à la LCEN, art 6 I.1°
[173] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005.
[174] CNIL, Fiche « Le contrôle de l'utilisation d'internet et de la messagerie électronique », 1er décembre 2015.

Aux termes du **décret n° 2011-219 relatif à la conservation et à la communication des données**, les fournisseurs d'accès à Internet doivent conserver **pendant un an** à compter du jour de la création des contenus, pour chaque connexion de leurs abonnés, les données suivantes :

- L'identifiant de la connexion
- L'identifiant attribué par les fournisseurs d'accès à Internet à l'abonné
- L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès
- Les dates et heures de début et de fin de la connexion
- Les caractéristiques de la ligne de l'abonné

Les fournisseurs d'accès à Internet et les fournisseurs d'hébergement doivent aussi **conserver pendant un an** à compter du jour de la résiliation d'un contrat ou de la fermeture d'un compte par un utilisateur, les informations fournies lors de sa souscription ou lors sa création à savoir :

- Au moment de la création du compte, l'identifiant de cette connexion
- Les nom et prénom ou la raison sociale
- Les adresses postales associées
- Les pseudonymes utilisés
- Les adresses de courrier électronique ou de comptes associés
- Les numéros de téléphone
- Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour

Enfin, lorsque la souscription d'un contrat ou d'un compte est payante, les fournisseurs d'accès à Internet et les fournisseurs d'hébergement doivent **conserver pendant un an** à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement, les informations suivantes :

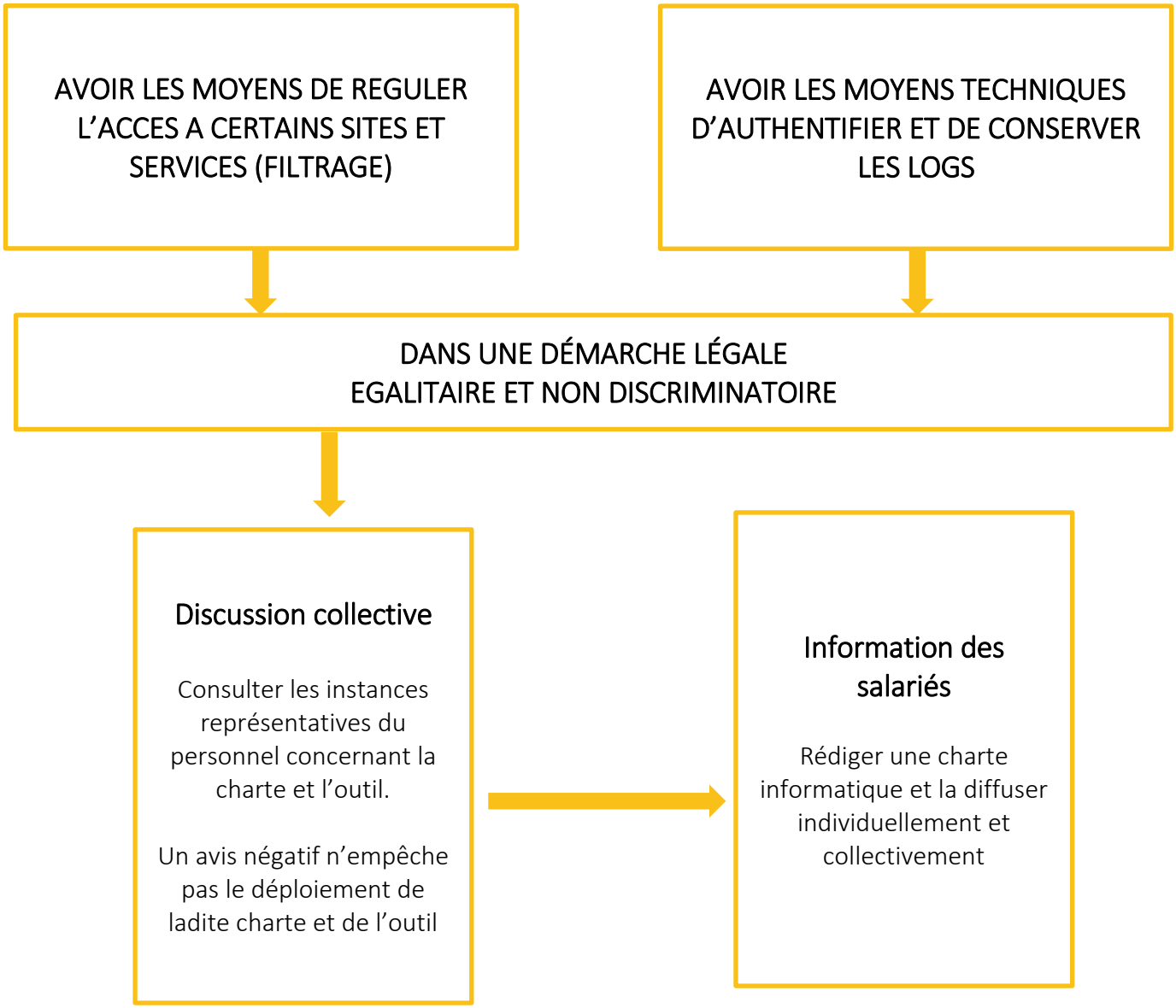
- Le type de paiement utilisé
- La référence du paiement
- Le montant
- Date et heure de la transaction

VI. ETAPE 6 : LE MAINTIEN EN CONDITIONS OPERATIONNELLES

Il est indispensable d'assurer un maintien en conditions opérationnelles de la solution de filtrage et de sa conformité au droit. Il s'agit en particulier de s'assurer de la conformité légale du paramétrage et des procédures permettant d'assurer l'utilisation précontentieuse ou contentieuse des éléments issus des outils de filtrage mis en œuvre.

VII. LES REGLES D'OR DU FILTRAGE

COMMENT PROTEGER SON ORGANISATION DE L'USAGE D'INTERNET CONFORMEMENT AU DROIT ?



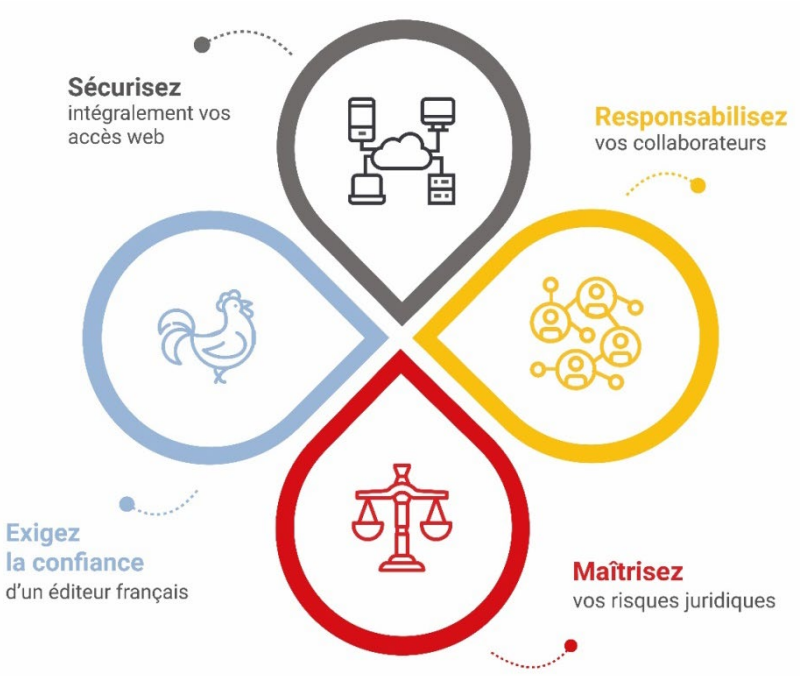
* Registre des traitements à partir du 25 mai 2018 (entrée en vigueur du RGPD)

A PROPOS D'OLFEO

Nous accompagnons depuis plus de 16 ans les entreprises exigeantes dans la sécurisation de leur flux web. Grâce à notre connaissance extrêmement fine des besoins des organisations françaises, nous avons développé une passerelle de sécurité web disruptive, basée sur une vision globale, et pas uniquement technologique.

Nos solutions allient :

- La sécurisation intégrale de vos accès web grâce à des solutions technologiques de haut niveau et une base de données d'une qualité inégalée,
- La responsabilisation de vos collaborateurs en les rendant acteurs de votre politique de sécurité,
- La protection juridique totale grâce à l'intégration des lois Françaises & européennes (droit pénal, droit social, RGPD, etc.),
- La confiance d'un éditeur français pour assurer la proximité et la souveraineté de vos données.



C'est ce que l'on appelle, la sécurité positive.
Notre solution a aujourd'hui été adoptée par 1000 clients et a obtenu de nombreux labels notamment : « Utilisé par les armées françaises » ou « France Cybersecurity ».

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

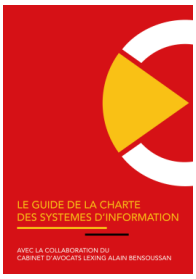
- Proxy avancé & déchiffrement HTTPS
- Filtrage web
- Filtrage applicatif
- Antivirus web
- Portail public
- Filtrage DNS
- Nomadisme
- Campus

POUR ALLER PLUS LOIN

Découvrez nos autres livres blancs :

Responsabilisez vos collaborateurs

Sécurisez intégralement vos accès web



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 ? …

https://www.olfeo.com/fr/telechargement-guide-charte-SI

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

Maître Polyanna Bigle du cabinet d'avocats Alain Bensoussan Lexing, Avocate et Directeur du Département Sécurité Numérique a réalisé plusieurs mises à jour de ce guide (co-auteur d'origine : Maître Eric Barbry, Avocat).

Maître Polyanna Bigle

Avocat au Barreau de Paris
Directeur du Département « Sécurité Numérique »
Spécialiste en droit des nouvelles technologies, de l'informatique et de la communication

Depuis sa création en 1978, le cabinet Lexing Alain Bensoussan Avocats est entièrement dédié au droit des technologies avancées. Ce choix précurseur lui a permis de se maintenir de façon durable à la pointe de son secteur et des meilleures pratiques juridiques dans les domaines notamment de l'informatique, des télécoms, d'internet, de la propriété intellectuelle, de la protection des données personnelles et de l'IA.

Novateur dans son organisation, sa gestion et son système qualité, le cabinet s'appuie sur une équipe d'avocats technologues qui associent la connaissance des secteurs techniques à celle du droit spécifique qui s'y applique, et apportent leur savoir-faire dans tous les axes d'exercice de leur métier : le pilotage de projets juridiques ; le conseil, l'audit et l'assistance ; le précontentieux, le contentieux et l'arbitrage ; l'infogérance juridique.

Par-delà ses activités propres à l'international, le cabinet s'est développé à l'étranger dès 1992 puis a créé le réseau Lexing®, premier réseau international d'avocats spécialisés en droit des nouvelles technologies, comprenant actuellement une trentaine de cabinets d'avocats sur les 5 continents.

Le cabinet est régulièrement distingué par de nombreux prix pour sa stratégie d'innovation,

Olfeo

CONTACTEZ-NOUS

- 4 rue de ventadour
  75001 Paris
  +33(0) 969 390 999

contact@olfeo.com

www.olfeo.com