Olfeo France

LIVRE BLANC JURIDIQUE

Co-écrit avec le cabinet d'avocats

Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

Filtrage et Internet au bureau :
Enjeux et cadre juridique en France

3ème édition

SOMMAIRE

PRÉFACE

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

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

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

Maître Éric Barbry

Avocat au Barreau de Paris, Directeur du pôle « Droit du numérique ».

Maître Polyanna Bigle

Avocat au Barreau de Paris, Directeur du département « Sécurité des systèmes d'information et dématérialisation ».

L'usage d'Internet au sein des entreprises et le développement des réseaux sociaux posent un certain nombre de questions :

- Peut-on filtrer ou doit-on filtrer au sein des entreprises ?
- 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 ?
- Le filtrage sur le temps de pause est-il possible ?
- Peut-on sanctionner un collaborateur sur la foi des données restituées par l'outil de filtrage ?
- Peut-on filtrer autre chose que les sites web ?
- Qu'est-ce qui distingue un outil de filtrage d'un autre ?
- Faut-il déclarer son outil à la CNIL ?
- Faut-il informer le personnel, les personnes extérieures, les deux ?

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 ? ».

La jurisprudence la plus récente conforte ce point, en légitimant la mise en œuvre d'un contrôle des connexions Internet.

Dès lors, il existe deux types d'entreprises 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

Sur le plan pratique, on parle par ailleurs de moins en moins de « filtrage » mais « d'administration des accès ».

L'évolution n'est pas que sémantique. Elle procède d'un vrai changement de paradigme au sein des entreprises.

L'objectif n'est plus de « limiter » les accès au web mais de les « organiser ».

Maître Éric Barbry
& Maître Polyanna Bigle

I. LES ASPECTS JURIDIQUES DU FILTRAGE

Il n'y a plus de doute aujourd'hui, le filtrage est admis sur tous les plans :

- Au plan légal
- Au plan jurisprudentiel
- Au plan normatif et des bonnes pratiques
- Et 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 des règles.

I.1 LE DROIT DE FILTRER - ASPECT LÉGAL

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 :

- **Lois dites 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'enregistrement 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 la protection des mineurs du 18 février 2004** prévoyant « la mise en œuvre d'outils de **filtrage** dans les établissements ou écoles »

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**[1] 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. Le considérant n°5 met en avant le fait que les outils de filtrage constituent des éléments essentiels pour assurer un environnement plus sûr sur Internet
- De nombreuses recommandations du **Comité des Ministres aux États 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)

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 »[2]
- 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** »[3]
- **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. »

[1] 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 ».

[2] 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 ».

[3] 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.141-1 VIII 3° du Code de la consommation**, crée par l'article 76 VIII de la loi Hamon du 17 mars 2014, 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 bloqués pour tout 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**[4] 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 représentations 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'appliquant expressément aux 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 à savoir :** « 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.

CE QU'IL FAUT RETENIR…

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

I.2 LE DROIT DE FILTRER - ASPECT 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 :

- Vente d'objets nazis sur le site yahoo.com accessible depuis la France[5]

[4] 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.
[5] CA Paris, 3-9-2010 n°08/12822

- Vente de parfums Christian Dior en dehors de leur réseau de distribution sélectif
- Diffusion de pages à contenus racistes[6]
- Diffusion de propos négationnistes[7]
- Jeux en ligne et paris hippiques[8]
- Site d'hébergement de vidéos (YouTube[9], Dailymotion[10])

Déjà en 2010, **le Président du Tribunal de grande instance de Paris**[11] 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 obtenu, ainsi que les défendeurs l'exposent, 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**[12], et le même jour de ne pas avoir détaillé le fonctionnement effectif d'un tel filtrage ni détaillé ses résultats[13].

Dans une décision du 14 décembre 2010, **le Tribunal de grande instance de Créteil**[14] a fait injonction à un hébergeur **d'installer sur son site un système de filtrage efficace et immédiat** des vidéos dont la diffusion illicite 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 soulevé 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 des hébergeurs 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 à priori d'Internet.**[15].

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'ACCÈS

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

I.3 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 :

- **Les fiches de synthèse « Cybersurveillance sur les lieux de travail »** du 11 février 2002
- **Le rapport de la CNIL** « **La cybersurveillance sur les lieux de travail** » édition mars 2004
- **Le guide « la sécurité des données à caractère personnel** », édition 2010
- **Le guide pratique de la CNIL** « **pour les employeurs et les salariés** », édition 2010 dont la fiche n°6 porte sur le « Contrôle de l'utilisation d'Internet et de la messagerie »
- **L'évaluation des salariés : droits et obligations des employeurs,** 11 mai 2011
- **La fiche « les outils informatiques au travail** », janvier 2013
- **La fiche pratique Keylogger** : des dispositifs de cybersurveillance particulièrement intrusifs du 20 mars 2013
- **L'article de la CNIL sur « l'analyse des flux https : bonnes pratiques et questions »** du 31 mars 2015

Dans son guide pratique pour les employeurs et les salariés[16], la CNIL considère que s'il n'est pas possible d'interdire « de manière générale et absolue » l'utilisation d'Internet à des fins non professionnelles, en se référant notamment au contexte de développement des moyens de communication ainsi qu'au contexte jurisprudentiel actuel, rien n'empêche l'employeur de limiter notamment 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…

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.

[16] Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2010 p. 18, voir également le rapport de la CNIL « La cybersurveillance sur les lieux de travail », édition mars 2004, p. 12.

Chaque employé doit être notamment informé :

- Des finalités poursuivies
- Des destinataires des données
- De son droit d'opposition pour motif légitime
- De ses droits d'accès et de rectification

La CNIL a également encadré l'utilisation des keyloggers, qui tracent tous les caractères saisis sur un clavier par un utilisateur sur son ordinateur. Ils permettent ainsi à un employeur de connaître les mots saisis lors de la rédaction d'un email, d'un échange sur messagerie instantanée ou de la consultation d'un site Internet.

Elle a ainsi considéré que ce dispositif portait une atteinte excessive à la vie privée des salariés concernés, et qu'il était dès lors, illicite au regard de la loi Informatique et Libertés.

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 de certains dispositifs de captation de données informatiques à l'insu des personnes concernées.[17]

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

- La **note technique portant sur 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 pare-feu 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.

CE QU'IL FAUT RETENIR…

LE FILTRAGE FAIT ASSURÉMENT PARTIE DE CE QU'IL EST CONVENU D'APPELER LES « BONNES PRATIQUES » EN TERMES DE MANAGEMENT DU SYSTÈME D'INFORMATION ET DE SÉCURITÉ

[17] Fiche pratique CNIL Keylogger : dispositifs de cybersurveillance particulièrement intrusifs, 20 mars 2013.

I.4 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…

80% DES ENTREPRISES FILTRENT… ET VOUS ?

I.5 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** »[18]
- 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[19]
- Il est par ailleurs possible qu'un arrêt de la CJUE remette en cause celui du 8 février 2014 qui avait invalidé la directive européenne de 2006 sur la conservation des données[20]
- Les « **données de nature à permettre l'identification** » prévues 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[21]

[18] 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.
[19] Décret n°2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.
[20] CJUE C- 293/12 et C-594/12 du 8 3 2014 invalidant la directive 2006/24/CE sur la conservation des données de l'Union européenne.
[21] 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.

Il en est de même de la jurisprudence :

Dans **un arrêt du 9 juillet 2008**, **la Cour de cassation**[22] 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**[23] et par la **Cour d'appel d'Aix en Provence** dans un arrêt du **22 février 2013**[24], ainsi qu'implicitement dans un **arrêt du 10 mai 2012** de **la Cour de cassation** en confirmant l'arrêt d'appel.[25]

Ces décisions présentent une avancée jurisprudentielle essentielle, et s'inscrivent dans l'actuelle tendance jurisprudentielle 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).

Cependant, la **Cour de cassation** a apporté une précision importante concernant les connexions Internet des salariés. 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. »

Ainsi que pour la CNIL :

La CNIL qui utilise les termes de « fichiers logs » ou « fichiers de journalisation »[26] a publié un certain nombre de documents relatifs aux logs et notamment :

- **Les fiches de synthèse « Cybersurveillance sur les lieux de travail » du 11 février 2002** où elle utilise les termes de « fichiers logs ou de journalisation »[27]

- **Le rapport de la CNIL « La cybersurveillance sur les lieux de travail », édition mars 2004** où dans son introduction la CNIL précise la nécessité de procéder à une journalisation, c'est-à-dire à l'enregistrement des actions de chaque utilisateur sur le système pendant une durée définie ;

- **Le guide pratique de la CNIL « pour les employeurs et les salariés »**, **édition 2010**, fait également référence aux fichiers « logs » 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 2010**, la fiche n° 8 porte sur « La traçabilité et la gestion des incidents ». Cette fiche explique les mesures que doit mettre en place un DSI « Afin d'être en mesure d'identifier à postériori un accès frauduleux à des données personnelles, une utilisation abusive de telles données, ou de déterminer

[22] 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.»

[23] 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.»

[24] 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. »

[25] Cass-soc 10 05 2012 n° 11-11.252

[27] Rapport de la CNIL « La cybersurveillance sur les lieux de travail », édition mars 2004.

[27] Rapport de la CNIL « La cybersurveillance sur les lieux de travail », édition mars 2004.

l'origine d'un incident, il convient d'enregistrer les actions effectuées sur le système informatique.
Pour ce faire, le responsable d'un système informatique doit mettre en place un dispositif adapté aux risques associés à son système. Celui-ci doit enregistrer les évènements pertinents, garantir que ces enregistrements ne peuvent être altérés, et dans tous les cas conserver ces éléments pendant une durée non excessive ».

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

- « **Prévoir un système de journalisation** (c'est-à-dire un enregistrement dans des «fichiers de log») 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 dérogatoire, ou demande de la CNIL, de conserver ces informations pour une durée plus longue)

- **Prévoir au minimum la journalisation des accès des utilisateurs** incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion. Le format de l'horodatage doit de préférence prendre comme référence le temps UTC10

- Dans certains cas, il peut être nécessaire de **conserver également le détail des actions effectuées par l'utilisateur**, telles que les données consultées par exemple. »

I.6 LE DROIT DES CHARTES D'UTILISATION DES SYSTÈMES 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, des services informatiques et d'Internet mis à leur disposition à des fins professionnelles.

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.

- **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 »[28]

- 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[29]

- 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 son poste de travail alors que cela était formellement **interdit par la charte informatique**[30]

[28] Cass. soc. 21 12 2006 n°05-41.165.
[29] Cass. soc. 15 12 2010 n° 09-42.691.
[30] CA Paris, pôle 6 ch. 5, 19-1-2012 RG n° 07-01754.

- 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**[31] 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.

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

Pour la CNIL, une « charte informatique » est un document qui pourra préciser les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'Internet[32].

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 de synthèse « Cybersurveillance sur les lieux de travail » du 11 février 2002**

- **Le guide pratique de la CNIL « pour les employeurs et les salariés »**, édition 2010 dont la fiche n°6 porte sur le « Contrôle de l'utilisation d'Internet et de la messagerie ».
  La CNIL recommande ainsi de « porter à la connaissance des salariés (par exemple dans une charte) le principe retenu pour différencier les e-mails professionnels des e-mails personnels (qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé, etc.) »

- **Le guide « La sécurité des données personnelles », édition 2010**, comporte la fiche n°3 « Gestion des habilitations et sensibilisation des 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

- **La fiche « les outils informatiques au travail** » de janvier 2013, qui 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 par une charte informatique, annexée ou non au règlement intérieur

D'autres autorités que la CNIL préconisent l'existence 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**[33], prévoit la mise en place d'une charte d'utilisation des moyens informatiques et de communication électronique pour les employés et également d'une charte administrateur pour l'accès aux données cryptées.

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 récente 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),

[31] CA D'AIX RN Provence 13/01/2015, RG n°10/2106
[32] CNIL « Cybersurveillance sur les lieux de travail « 11 2 2002.
[33] Recommandation de l'ANSSI Flux HTTPS n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.

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'origine interne étant passées de 25 % à 35 % entre 2012 et 2014[34].

CE QU'IL FAUT RETENIR…

LA CHARTE INFORMATIQUE PERMET DE FIXER LES RÈGLES D'UTILISATION DU SYSTÈME D'INFORMATION. ELLE EST OPPOSABLE AUX SALARIÉS EN CAS DE LITIGE SI ELLE EST DÉPLOYÉE COMME UN RÈGLEMENT INTÉRIEUR

[34]Rapport CLUSIF « Menaces informatiques et pratiques de sécurité en France », édition 2014, M. MOURER Lionel, Mme COURTECUISSE Hélène et M. PRISO Serge.

II. LES USAGES PARTICULIERS DU FILTRAGE

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

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

II.1 LES RÉSEAUX SOCIAUX ET L'ENTREPRISE

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

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

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

- Travail en réseau (networking)
- Travail en communauté (hubworking)
- Web TV d'entreprise
- Communication 2.0 (Facebook…)
- Mise en contact professionnelle via plusieurs plates-formes
- Tweeter et blogs 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 ou un groupe sur les réseaux sociaux présentant leur entreprise afin d'attirer des prospects, fidéliser les clients…

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

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

En outre, la création d'applications dédiées aux salariés d'une entreprise permet de renforcer le sentiment d'appartenance à l'entreprise et constitue un moyen de socialisation[35].

Toutefois, les propos pouvant être publiés par les collaborateurs sur ces plates-formes ainsi que leur utilisation sur le lieu de travail constituent un risque juridique important. En effet, si beaucoup de législations leur sont applicables, notamment la législation relative aux droits d'auteur, la loi Informatique et Libertés, les incriminations relatives aux STAD[36] ou encore la loi pour la confiance

[35] Article « Les réseaux sociaux en entreprise : un potentiel inexploité qui fait saliver. » sur le site emergenceweb.com.
[36] Système de traitement automatisé de données.

dans l'économie numérique, bien d'autres règles s'appliquent à l'utilisation d'Internet telles que la liberté d'expression et les limites qui sont les siennes : diffamation, injure, dénigrement, concurrence déloyale, pour ne citer que les principales.

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

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

De nombreuses jurisprudences ont vu le jour en la matière :

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

  Le Conseil de prud'hommes[37] **décide** que le licenciement pour faute grave des deux salariées est fondé, considérant que « [l'un des salariés] a choisi dans le paramètre de son compte de partager sa page Facebook avec « ses amis et leurs amis », permettant ainsi un accès ouvert notamment aux salariés ou anciens salariés de la société. (…) ce mode d'accès ouvert à Facebook dépasse la sphère privée (…) la production aux débats de la page mentionnant les propos incriminés constitue un mode de preuve licite du caractère bien fondé du licenciement ». Les salariés ont interjeté appel

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

  Elle précise **concernant le réseau social Facebook** qu'il « **doit être considéré au regard de sa finalité et de son organisation, comme un espace public**. Elle ajoute en outre « qu'il appartient en conséquence à celui qui souhaite conserver la confidentialité de ses propos tenus sur Facebook, soit **d'adopter les fonctionnalités idoines offertes par ce site**, soit de s'assurer préalablement auprès de son interlocuteur qu'il a limité l'accès à son «mur»[38]

- **La Chambre correctionnelle du Tribunal de grande instance de Paris, le 17 Janvier 2012,** a également condamné un représentant du personnel et un délégué syndical pour **injure publique sur Facebook**.[39]

[37] CPH Boulogne-Billancourt, 19 nov. 2010, n°10-853
[38] CA de Besançon, 15 nov. 2011, n°10-02642
[39] TGI 17 ch correctionnelle 17 Janvier 2012

- **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[40]. La Cour d'appel de Reims a constaté que les propos tenus par l'apprenti sur Facebook « auxquels ont accès nombre d'internautes sont manifestement insultants » et que celui-ci s'était « prêté sans réserve aux commentaires pour le moins désobligeants de ses correspondants ». La Cour a donc relevé que cette attitude était « manifestement fautive » et avait occasionné un préjudice à l'employeur.

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

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

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

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

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

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

Il appartient à l'employeur de définir les règles du jeu quant à l'utilisation des réseaux sociaux et des services web 2.0 depuis le lieu de travail. À charge pour lui d'interdire, de tolérer ou de 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 ACCÈS AU WEB AVEC UNE GRANULARITÉ TELLE QUE L'ON PEUT PARAMÉTRER L'OUTIL DE MANIÈRE À AUTORISER TELLE PERSONNE À ACCÉDER À TELLE PLATE-FORME WEB 2.0 ET L'AUTORISER À RÉALISER TELLE OU TELLE OPÉRATION OU LUI INTERDIRE TELLE OU TELLE AUTRE

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

II.2 LES ACCÈS INVITÉS AU RÉSEAU INTERNET DE L'ENTREPRISE

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

Hier limité aux cybercafés et à quelques aéroports pionniers dans le domaine des hotspots, aujourd'hui l'accès public au web est partout : salons, hôtels, restaurants, points d'information publics.

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

Il faut ici rappeler deux réalités juridiques :

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

  En langue naturelle cela signifie que les hotspots professionnels sont soumis aux mêmes obligations que les hotspots mis à disposition par les opérateurs de télécommunications notamment en termes **d'identification des utilisateurs et de conservation des données de trafic**.

  Les entreprises, offrant un réseau interne ouvert au public au sein de l'entreprise, sont considérés comme fournisseur de **réseau interne ouvert au public**[41]. Ces réseaux **ne sont pas soumis à l'obligation de se déclarer opérateurs auprès de l'ARCEP**, seuls les réseaux ouverts au public sont soumis à l'obligation de déclaration[42].

- **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 invités ?

[41] CPCE : l'article 32définit 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. »
[42] CPCE, art ; D98.

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

- **La limitation de l'accès à certains sites et services**, par conséquent, il est nécessaire de mettre en œuvre un système de filtrage
- **La conservation des données** de connexion
- **Une charte Wi-Fi** présentant à 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 ACCÈS PUBLIC PEUT VOIR SA RESPONSABILITÉ ENGAGÉE DU FAIT DES ACCÈS ILLICITES DES TIERS

II.3 LES FLUX SÉCURISÉS : HTTPS, FTPS…

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

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

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

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

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

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 dans l'entreprise à son insu.

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'un déchiffrement d'un flux chiffré y compris de nature personnelle sur le lieu de travail, notamment au regard des référentiels légaux applicables en 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

À 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.

À ce titre, une toute récente **note de l'ANSSI**[43] sur le déchiffrement des flux https apporte de nouvelles précisions sur ce point, où elle qualifie notamment les risques juridiques du déchiffrement de flux HTTPS :

Elle définit en premier lieu le protocole HTTPS qui est « la déclinaison sécurisée de HTTP encapsulé à l'aide d'un protocole de niveau inférieur nommé TLS, 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 déchiffrement contient des risques dans la mesure où cette opération conduit à rompre la sécurité d'une transmission chiffrée et à faire apparaître 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 déchiffrement de flux cryptés et notamment :

- **Les articles 100 et suivants du Code de procédure pénale** qui imposent une obligation légale de déchiffrement dans le cadre spécifique des interceptions judiciaires
- **Les articles L. 241-1 à L. 245-3 du Code de la sécurité intérieure** qui autorisent cet usage dans le cadre des interceptions de sécurité
- **L'article 230-1 du Code de procédure pénale** qui autorise le déchiffrement 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** qui garantit le secret des correspondances privées

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

- **Les articles 226-16 à 226-24 du code pénal** prévoient la protection des données à caractère personnel

- **Les articles 226-1 à 226-7 du code pénal** protègent également la vie privée des salariés en dehors de leur cadre de travail

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

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

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

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

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

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

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

Cette possibilité devra être toutefois justifiée par deux finalités :

- **L'impossibilité d'assurer le bon fonctionnement du système d'informations** et de maintenir les conditions de sécurité informatique par d'autres moyens

- **La présence, ou tout du moins la convocation[44] du salarié concerné** en cas de connaissance de contenus considérés comme personnels ou privés[45]

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

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

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

- **Une information précise** des salariés
- **Une gestion stricte des droits d'accès des administrateurs** aux courriers électroniques
- **Une minimisation des traces** conservées
- **Une protection des données d'alerte 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 à la vie privée des employés en sélectionnant une liste blanche de sites Internet sécurisés ne devant pas être déchiffrés par l'employeur, comme par exemple les sites d'organismes de sécurité sociale, mutuelles, laboratoires d'analyses médicales…

LE SAVIEZ-VOUS?

LE DÉCHIFFREMENT DE FLUX HTTPS DOIT ÊTRE STRICTEMENT ENCADRÉ PAR L'EMPLOYEUR AFIN DE NE PAS ENTRAÎNER UNE VIOLATION DES DROITS DE PROPRIÉTÉ INTELLECTUELLE ET DES DROITS RELATIFS AUX DONNÉES À CARACTÈRE PERSONNEL

II.4 LE FILTRAGE ÉTENDU

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

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

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

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

LE SAVIEZ-VOUS ?

LE FILTRAGE URL EST UN PREMIER REMPART TECHNIQUE POUR PROTÉGER JURIDIQUEMENT L'ENTREPRISE MAIS EST INSUFFISANT
POUR ÊTRE EFFICACE LE FILTRAGE DOIT ÊTRE ÉTENDU À L'ENSEMBLE DES FLUX ET PROTOCOLES

II.5 BYOD (BRING YOUR OWN DEVICE)

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.[46]

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

Selon le rapport CLUSIF de 2014, le BYOD aurait vu son **taux d'interdiction** au sein **des entreprises passer de 38% à 66%** ![47]

Ainsi, selon la CNIL, seuls 44 % des possesseurs disent avoir une utilisation « exclusivement personnelle » de leur smartphone.[48]

Or, selon une étude du cabinet américain Gartner, en 2020, 45 % des entreprises mondiales auront renoncé à leur flotte d'appareils mobiles professionnels.[49]

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

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

En effet, l'utilisation du BYOD entraîne la disparition des frontières claires entre usage professionnel et usage privé.

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. Ceux-ci doivent néanmoins respecter **la vie privée** des employés qui utilisent des équipements personnels dans le cadre de leur activité professionnelle.

[46] Définition Légifrance
[47] Rapport CLUSIF « Menaces informatiques et pratiques de sécurité en France », édition 2014, M. MOURER Lionel, Mme COURTECUISSE Hélène et M. PRISO Serge.
[48] Lettre IP n° 7 6 2014
[49] Bring Your Own Device: The Facts and the Future, étude Gartner 2013, David A. Willis.

D'un point de vue sécurité des informations professionnelles, il paraît donc nécessaire que l'utilisateur accepte d'ajouter des solutions de sécurisation sur son système informatique. À 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 par 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'entreprise, les responsables des systèmes informatiques pourront procéder aux actions suivantes :

- **Limiter à certaines catégories de personnes uniquement** le « droit » au BYOD
- **Limiter le nombre ou le type de terminaux** accessibles 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** d'utilisation du BYOD
- **Définir le processus** à suivre pour 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.[50]

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)
- Ne pas encourager **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)

[50] Cass. soc. 2 4 2014

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

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

À 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.[51]
  Il en résulte que l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié.

- **Un autre arrêt de la Cour de cassation** a estimé que l'employeur ne peut procéder à l'écoute des enregistrements réalisés par la salariée sur son dictaphone personnel en son absence ou sans qu'elle l'ait au moins dûment appelé.[52]

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

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.[53]

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

Concernant le BYOD, la CNIL s'est également positionnée sur ce sujet en publiant une fiche pratique sur **« les bonnes pratiques » en matière de BYOD** en février 2015[54].

[51] Cass soc 12 2 2013 n° 11-28649
[52] Cass soc 23 05 2012 n° 10-23521
[53] Cass soc 23 5 2007 n° 05-17.818.
[54] http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/byod-quelles-sont-les-bonnes-pratiques/

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

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

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

LE SAVIEZ-VOUS?

LE BYOD EST UN USAGE INTÉRESSANT D'UN POINT DE VUE ÉCONOMIQUE EN PARTICULIER, MAIS IL EST FORTEMENT RECOMMANDÉ DE BIEN PRÉVOIR LES CONDITIONS ENCADRANT SON UTILISATION.

LA PARTIE PROFESSIONNELLE DU MATÉRIEL UTILISÉE À TITRE PROFESSIONNEL PEUT ÊTRE CONTRÔLÉE. CECI DEVRA ÊTRE PRÉVU DANS LA CHARTE, DE MÊME QUE L'OBLIGATION POUR L'EMPLOYÉ DE METTRE EN EN PLACE DES PRÉREQUIS TECHNIQUES ET SOLUTIONS TECHNIQUES NÉCESSAIRES.

III. NE PAS FILTRER, NE PAS LOGUER : QUELLES CONSÉQUENCES ?

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 posée, il est possible d'apprécier le risque d'une part et la responsabilité d'autre part.

III.1 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.

Or sur ce point le principe de droit international privé est simple :

- **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 tout 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 SAVIEZ-VOUS ?

LE DROIT FRANÇAIS S'APPLIQUE À TOUTES LES ENTREPRISES DONT LE SIÈGE EST SITUÉ EN FRANCE AINSI QU'AUX INFRACTIONS COMMISES EN FRANCE

III.2 QUELS RISQUES ?

Les risques de ne pas filtrer sont de deux niveaux :

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

III.2.a LE NON-RESPECT DE L'OBLIGATION LÉGALE 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**[55], aurait pour certains auteurs, assimilé l'employeur qui donne accès à Internet à ses employés, 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'en informer les utilisateurs

[55] 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[56] 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 SAVIEZ-VOUS ?

LE CODE DE LA PROPRIÉTÉ INTELLECTUELLE RENFORCE L'OBLIGATION DE FILTRAGE DES ENTREPRISES

III.2.b LE RISQUE DE NE PAS FILTRER POUR UNE ENTREPRISE OU ADMINISTRATION

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

- L'article **1384** du Code civil
- L'article **121-2** du Code pénal
- L'article **L 336-3** du Code de la propriété intellectuelle

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

Sans oublier l'impact toujours réel mais difficilement mesurable aujourd'hui de **l'arrêt de la Cour d'appel de Paris du 4 février 2005**[57].

Le risque civil

L'article 1384 alinéa 5 du code civil dispose « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. (…) Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ».

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

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

Le risque pénal

L'article 121-2 du Code pénal dispose « Les personnes morales, à l'exclusion de l'État, 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 pour des accès illicites :

- **À des sites en raison de leurs contenus** portant notamment atteinte :
  - **Aux mineurs**, tels que les contenus pédopornographiques ou encore les contenus incitant à l'anorexie.[58]
  - **À des sites de jeu 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)
  - **À la protection des auteurs**, s'agissant des sites contrefaisants
  - À 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[59].

[57] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005
[58] Article 223-2-1 du Code Pénal

- **<u>À des sites au regard des produits et services qu'ils commercialisent</u>** <u>tels que notamment</u> :

  - Des organes et produits du corps humain
  - Des drogues
  - Des objets à caractère pédophile
  - Des armes à feu et explosifs
  - Des médicaments
  - Du tabac
  - De l'alcool
  - Des logiciels permettant de porter atteinte à un système de traitement automatisé de données
  - Des logiciels de contournement de mesures techniques de protection ou d'information

Plus généralement, des produits interdits ou réglementés.

LE SAVIEZ-VOUS ?

L'ENTREPRISE PEUT VOIR SA RESPONSABILITÉ ENGAGÉE DU FAIT DES AGISSEMENTS DE SES SALARIÉS

III.3 QUI EST RESPONSABLE ?

III.3.a LA RESPONSABILITÉ DE L'EMPLOYEUR

Au civil

Selon l'article 1384 alinéa 5 du code civil, l'employeur est responsable des dommages causés par ses salariés dans l'exercice de leurs fonctions.

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

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

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

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

La jurisprudence précise que la responsabilité du dirigeant peut être limitée si l'employé a agi[60] :

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

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

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

La Cour d'appel d'Aix-en-Provence qui a rendu un arrêt retenant la responsabilité de l'employeur au motif principal que[61] :

- « 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 la 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 1384 alinéa 5 du Code civil**, militent fortement en faveur de la mise en place par l'employeur de tous les outils permettant de maîtriser, voire de contrôler l'utilisation de l'Internet par les employés.

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

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

Au pénal

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

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

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

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

La réponse est loin d'être simple et trouve un de ses fondements dans **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'État, **sont responsables pénalement**, selon les distinctions des articles 121-4 à 121-7, **des infractions commises, pour leur compte, par leurs organes ou représentants**. »

À 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 dans ce cas on peut supposer que **seule la responsabilité de l'employé** sera retenue

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

À la question de savoir si l'employeur peut être responsable du fait que ses employés puissent accéder à des sites illicites (sites à caractère pédophile, 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**[62] », c'est-à-dire si la commission de protection des droits de l'Hadopi, **en application de l'article L. 331-25 du Code de la propriété intellectuelle**, lui a préalablement adressé, par voie d'une lettre remise contre signature ou par tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à Internet.

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**

[62] 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 ».

peine complémentaire de suspension de l'accès à Internet prévu par l'article L. 335-7 en cas d'actes de **contrefaçon sanctionnés** par les articles L. 335-2, L. 335-3 et L. 335-4 du Code de la propriété intellectuelle lorsqu'ils sont commis au moyen d'un service de communication au public en ligne.

Ainsi l'entreprise peut se voir condamner à une:

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

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

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

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

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.

L'article 5 de la loi n°2013-711 du 5 août 2013 ajoute après cette phrase : « 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'infraction prévus dans 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[63]) ?

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 circonstances 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**[64], 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.

À ce titre, la doctrine précise qu'à partir du moment où la faute a un lien avec le service, cette faute personnelle apparaît comme « non dépourvue de tout lien avec le service », du fait qu'elle a été réalisée soit pendant l'exercice des fonctions de l'agent, soit parce que l'exercice de sa mission a 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.[65]

La jurisprudence a estimé que dans ce cas **la faute personnelle n'est « pas dépourvue de tout lien avec le service** ».[66]

LE SAVIEZ-VOUS ?

LE PREMIER DONT LA RESPONSABILITÉ SERA RECHERCHÉE EST L'EMPLOYEUR

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

III.3.b **RESPONSABILITÉ DE L'UTILISATEUR**

En tant qu'utilisateur des moyens informatiques et de communication électronique 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 1382 et 1383 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 communication électronique 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 au moins quatre 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 pouvait les ouvrir hors la présence du salarié, sauf si celui-ci les identifiait comme étant personnels.[67]

[67] 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 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.[68]

- **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[69].

- **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.

LE SAVIEZ-VOUS ?

L'UTILISATEUR EST RESPONSABLE DE SES ACTES… ENCORE FAUT-IL QUE L'ENTREPRISE SOIT EN MESURE DE L'IDENTIFIER

III.3.C RÔLE ET RESPONSABILITÉ DES ADMINISTRATEURS/DSI

Le rôle des administrateurs

Comme le précise la CNIL dans son **« Guide pratique pour les employeurs et les salariés »**[70], 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.

[68] Cass soc 15 12 2010 n ° 09-42.691
[69] CA Versailles 31-5-2011 Mickael P. c/ Mireille B.P.
[70] Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2010.

Selon la fiche pratique CNIL « Peut-on accéder à l'ordinateur d'un salarié en vacances »[71], 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 « L'administrateur a pour mission d'assurer le fonctionnement normal et la sécurité des réseaux etsystèmes dont il a la charge. En conséquence de cette mission, l'administrateur est tenu par une obligation de confidentialité et ne doit donc pas divulguer des informations dont il a eu connaissance dans le cadre de ses fonctions.»[72]

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

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

- Au **bon fonctionnement technique** des applications
- À **la sécurité**
- À **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[73]. L'employeur ne doit cependant pas accéder aux contenus identifiés comme personnels par l'employé.

Tous les fichiers qui ne sont pas identifiés comme « personnels » sont réputés être professionnels de sorte que l'employeur peut y accéder hors la présence du salarié[74]. 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 a été dûment convoqué, 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**[75].

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 communication électronique, 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

[71] Fiche pratique CNIL « Peut-on accéder à l'ordinateur d'un salarié en vacances », 19 juillet 2010.
[72] Recommandation de l'ANSSI Flux HTTPS n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.
[73] Cass. 18-3-2003.
[74] Cass. 18-10-2006.
[75] 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 ».

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 quelle 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[76] a confirmé le licenciement d'un administrateur qui avait téléchargé pendant ses heures de travail des fichiers piratés et contrefaits en utilisant le système, à des fins personnelles étrangères à l'activité de son employeur.

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

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

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

Les logiciels de prise en main à distance permettent aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique. 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[77] qu'une telle utilisation n'est pas conforme aux principes de proportionnalité et de finalité posés par la loi Informatique et Libertés.
Lors de l'utilisation de tels logiciels, la CNIL recommande aux gestionnaires techniques de prendre deux précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquels ils accèdent :

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

LE SAVIEZ-VOUS ?

LE DÉFAUT DE FILTRAGE POURRAIT ÊTRE CONSIDÉRÉ COMME UNE FAUTE PROFESSIONNELLE PAR DÉFAUT DE MISE EN ŒUVRE DE BONNES PRATIQUES

[76] CA Paris 22e ch. C 4-10-2007 RG 03/12345.
[77] Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2010.

IV. PLAN DE DÉPLOIEMENT

IV.1 ÉTAPE 1 : LE CHOIX DE LA SOLUTION

Une solution de filtrage pertinente doit être capable de proposer :

- Des **catégories pertinentes qui correspondent au droit pénal** du pays et segmentées en fonction **des centres d'intérêt** des utilisateurs
- Un **taux de reconnaissance** élevé (aptitude à reconnaître les sites visités par les utilisateurs)
- La pertinence du **classement** (choix de la bonne catégorie pour un site au regard de la législation et de la culture du pays)

IV.1.a LE BON CHOIX DES CATÉGORIES

La législation et les centres d'intérêt 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.

BONNE PRATIQUE

IL FAUT SAVOIR CHOISIR UN OUTIL ADAPTÉ À SON BESOIN, RÉPONDANT AUX OBLIGATIONS LÉGALES ET QUI COLLECTE DES DONNÉES NON DISCRIMINATOIRES

IV.1.b L'IMPORTANCE DU TAUX DE RECONNAISSANCE

La qualité d'une solution de filtrage se mesure également en grande partie à la qualité de ses bases d'URLs.

Il y a environ 800 millions de sites web dans le monde. On comprend que la taille de la base de données ne peut pas être considérée comme un critère de qualité satisfaisant.

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.

IV.1.c LA QUALITÉ DU CLASSEMENT : LES SITES DANS LES BONNES CATÉGORIES

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 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 évoqué 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 naturellement 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.

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

- **Le droit « Informatique et Libertés »**
- **Le droit du travail**

ÉTAPE 2 : LE RESPECT DU DROIT INFORMATIQUE ET LIBERTÉS

IV.1.a LES PRINCIPES DE LA LOI INFORMATIQUE ET LIBERTÉS

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

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

- **Constitue une donnée à caractère personnel « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

- **Constitue un traitement de données à caractère personnel : « toute opération ou tout ensemble d'opérations portant sur de telles données**, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

L'article 8 I de ladite loi précise également des **interdictions en matière de collecte ou de traitement de certaines données** :

- « **Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement** ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. »

En application **de l'article 6 de la loi Informatique et Libertés**, un traitement de données à caractère personnel ne peut porter que sur des données :

- **Collectées de manière loyale** et licite

- **Adéquates, pertinentes**, **complètes, exactes, mises à jour** si nécessaire et non excessives eu égard à la finalité du traitement

- **Conservées sous une forme permettant l'identification des personnes** concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées

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

Les données issues 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.

IV.1.b LES DÉMARCHES PRÉALABLES À METTRE EN ŒUVRE

Schématiquement, pour qu'un outil de filtrage soit mis en œuvre conformément à la loi Informatique et Libertés, 3 grands principes doivent être respectés :

- Le droit des personnes
- Les formalités à accomplir
- La sécurité des données

Le droit des personnes

Les personnes concernées par un traitement de données à caractère personnel disposent de cinq droits :

- Le droit à l'information
- Le droit d'accès
- Le droit d'interrogation
- Le droit d'opposition
- Le droit de rectification

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[78] :

- De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant
- De la finalité poursuivie par le traitement
- Du caractère obligatoire ou facultatif des réponses aux questions des formulaires
- Des conséquences éventuelles, à son égard, d'un défaut de réponse
- Des destinataires ou catégories de destinataires des données
- Des droits qu'elle détient
- Des transferts de données à destination d'un État non-membre de la Communauté européenne

Cette information peut être réalisée par le biais de la charte.

Les entités responsables du traitement devront mettre en place une procédure afin de garantir aux personnes concernées l'exercice de leur droit de rectification, d'interrogation et de leur droit d'accès conformément à l'article 39 de la loi Informatique et Libertés.
Ces dernières ont en effet le droit d'interroger le responsable du traitement en vue d'obtenir :

[78] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 32.

- « **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

- Le cas échéant, **des informations relatives aux transferts de données à caractère personnel** envisagés à destination d'un État non-membre de la Communauté européenne

- La communication, sous une forme accessible, des **données à caractère personnel qui la concernent** ainsi que de toutes **informations disponibles quant à l'origine** de celles-ci

- **Les informations permettant de connaître et de contester** la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à son égard. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. »[79]

Ces droits ont pour but « d'encourager la transparence dans l'exploitation des données à caractère personnel »[80].

Les personnes concernées par le traitement ont en outre le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel les concernant fassent l'objet d'un traitement[81].

La déclaration CNIL

De fait, toute entité qui met en œuvre un outil de filtrage doit procéder aux formalités préalables imposées par la CNIL.

On peut s'interroger sur le type de démarches préalables à mettre en œuvre.

L'article 22 de la loi Informatique et Libertés prévoit que les traitements automatisés de données à caractère personnel **doivent faire l'objet d'une déclaration auprès de la CNIL.**
Dès lors que le dispositif de filtrage permet un contrôle individuel, celui-ci doit faire l'objet d'une **déclaration dite « normale** » auprès de la CNIL.

Selon l'article 30 de la loi Informatique et Libertés du 6 Janvier 1978, cette déclaration doit notamment préciser :

- L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre État membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande
- La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions

[79] Loi 78-17 du 6 1 1978, art. 39.
[80] Alain Bensoussan, « Informatique, télécoms, internet » éd. 2014, n°1639.
[81] Loi n° 78-17 du 6 1 1978, art. 38.

- Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements
- Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement
- Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées
- Les destinataires ou catégories de destinataires habilités à recevoir communication des données
- La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit

  Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant
- Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5
- La durée de conservation des données fixée par le responsable du traitement (étant précisé que la CNIL considère qu'une durée de conservation de six mois paraîtrait suffisante dans la plupart des cas)
- L'indication de la date à laquelle les instances représentatives du personnel ont été consultées sur la mise en place des outils de filtrage

La déclaration normale portera en général sur la mise en œuvre de l'ensemble des outils de surveillance et particulièrement sur les outils de filtrage. Si l'outil de filtrage est le seul traitement de contrôle individuel des employés, alors il fera l'objet d'une déclaration normale en tant que tel.

La déclaration pourra alors être transmise par Internet, par un dépôt direct auprès de la CNIL, ou par un envoi par lettre recommandée avec accusé de réception.

LE SAVIEZ-VOUS ?

LA DÉCLARATION NORMALE À LA CNIL NE FAIT QUE 4 PAGES ET PEUT ÊTRE RÉALISÉE EN LIGNE. L'ENREGISTREMENT DE LA DÉCLARATION AUPRÈS DE LA CNIL SERA EFFECTIF DÈS RÉCEPTION DU RÉCÉPISSÉ PORTANT LE NUMÉRO DE DÉCLARATION. DÈS RÉCEPTION DE CE RÉCÉPISSÉ, LE TRAITEMENT PEUT ÊTRE MIS EN ŒUVRE.

En revanche, si l'entreprise dispose d'un correspondant Informatique et Libertés[82], elle se trouvera dispensée de la déclaration normale[83].

Si le dispositif de filtrage ne permet pas de contrôle individuel, il est possible de procéder à une déclaration simplifiée du traitement. En effet, la norme simplifiée n°46 relative à la gestion du

[82] Tel que le prévoit l'art. 22-III de Loi n° 78-17 du 6 1 1978.
[83] Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2010 p. 19.

personnel permet de procéder à une déclaration simplifiée auprès de la CNIL des outils informatiques liés à la gestion des personnels.

Autrement, comme indiqué précédemment, il convient de privilégier la réalisation d'une déclaration normale auprès de la CNIL, l'exercice n'étant d'ailleurs pas plus compliqué qu'une déclaration simplifiée.

Enfin en l'absence de données directement ou indirectement nominatives, le dispositif de filtrage ne constitue pas un traitement de données à caractère personnel et ne nécessite pas une déclaration à la CNIL.

Si les données relatives aux employés sont anonymisées, il convient de préciser les modalités de cette anonymisation afin de déterminer si celle-ci est absolue, c'est à dire si les données ne sont plus nominatives directement (nom, prénom…) ni indirectement (adresse e-mail, adresse IP…).

L'anonymisation des données doit réellement permettre de faire perdre leur caractère personnel aux données afin de rendre impossible toute identification des personnes pour qu'aucune déclaration à la CNIL ne soit nécessaire. L'anonymisation doit donc être irréversible. Si elle est réversible, le dispositif de filtrage doit être déclaré.

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[84], 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 physiques et logiques 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.

IV.1.c LES POUVOIRS DE LA CNIL

La modification de la loi Informatique et Libertés par la loi n° 2004-801 du 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, a renforcé les pouvoirs de la CNIL.

Depuis cette réforme, la CNIL dispose de nouveaux pouvoirs.

L'article 11 de la loi Informatique et Libertés dresse la liste de ces pouvoirs :

[84] Loi n°78-17 du 6 1 1978, art. 34.

- La CNIL informe de leurs obligations les personnes concernées par un traitement et les responsables de traitements en proposant notamment des guides et des modèles sur son site Internet

- Elle veille à ce que les traitements soient mis en œuvre conformément aux formalités préalables de la loi Informatique et Libertés

- Elle dispose d'un pouvoir réglementaire pour encadrer ces traitements et peut élaborer des normes relatives à certaines catégories de traitements et édicter des recommandations

- Elle est consultée sur tout projet de loi ou décret relatif à la protection des personnes à l'égard des traitements

- Elle conseille les personnes et les organismes privés ou publics qui souhaitent mettre en œuvre ou envisagent de mettre en œuvre des traitements

- Elle anime le réseau des Correspondants Informatique et Libertés (CIL)

- Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, après les avoir reconnus conformes à la loi Informatique et Libertés

- Elle dispose d'un pouvoir d'investigation et de contrôle des traitements mis en œuvre

- Elle peut prononcer des sanctions en cas de non-respect des obligations Informatique et Libertés

IV.1.d **LES SANCTIONS**

Les sanctions administratives et pécuniaires que la CNIL peut prononcer sont :

- Un avertissement
- Une mise en demeure
- Une sanction pécuniaire
- Une injonction de cesser le traitement
- Un retrait de l'autorisation de mise en œuvre du traitement

Les sanctions pécuniaires prononcées par la CNIL font l'objet d'un double plafonnement :

- Lors du premier manquement, le plafond est de 150 000 euros

- En cas de manquement réitéré dans un délai de 5 ans, un second plafond est fixé à 300 000 euros ou, s'agissant d'une entreprise, 5% du chiffre d'affaires hors taxes du dernier exercice clos, dans la limite de 300 000 euros

Le non-respect des obligations de la loi Informatique et Libertés constitue également une infraction 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.

Pour les personnes morales, l'amende encourue est le quintuple decelle prévue pour les personnes physiques.

BONNE PRATIQUE

L'OUTIL DE FILTRAGE DOIT FAIRE L'OBJET D'UNE DÉCLARATION PRÉALABLE À LA CNIL
L'ACCÈS AUX DONNÉES DE L'OUTIL DOIT ÊTRE SÉCURISÉ

IV.2 ÉTAPE 3 : LE RESPECT DU DROIT DU TRAVAIL

La solution de filtrage constitue à la fois :

- La solution de filtrage constitue **un outil de contrôle** de l'activité des employés, et doit à ce titre **être portée à leur connaissance**[85]

- Une nouvelle technologie introduite au sein de l'entreprise ayant un impact sur les conditions de travail des salariés, et doit en conséquence faire l'objet **d'une consultation des institutions représentatives du personnel**[86]

IV.2.a SIMPLE « DOCUMENT » D'INFORMATION ET/OU CHARTE INFORMATIQUE?

Dès lors que l'outil de filtrage engendre la collecte de données à caractère personnel, un document doit être rédigé pour informer les salariés individuellement et collectivement 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 plusieurs mois.

Ainsi, 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.

[85] 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. »
[86] C. trav. art. L. 2323-13.

L'implémentation de ce document simplifié consiste pour l'employeur à respecter les démarches minimum 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
- **Soumettre** la proposition d'installation de la solution **à l'avis du comité d'entreprise**[87] ou comité technique dans les administrations, à défaut, des délégués du personnel et à l'avis du comité d'hygiène, de sécurité et des conditions de travail[88]

Il convient de préciser qu'un avis négatif de ces comités ne fait pas obstacle à la mise en place de la solution. En revanche, l'absence d'avis rendu, positif ou négatif, empêche la mise en œuvre du logiciel de filtrage.

Si cette démarche permet de mettre en place rapidement l'outil de filtrage, le document simplifié 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.

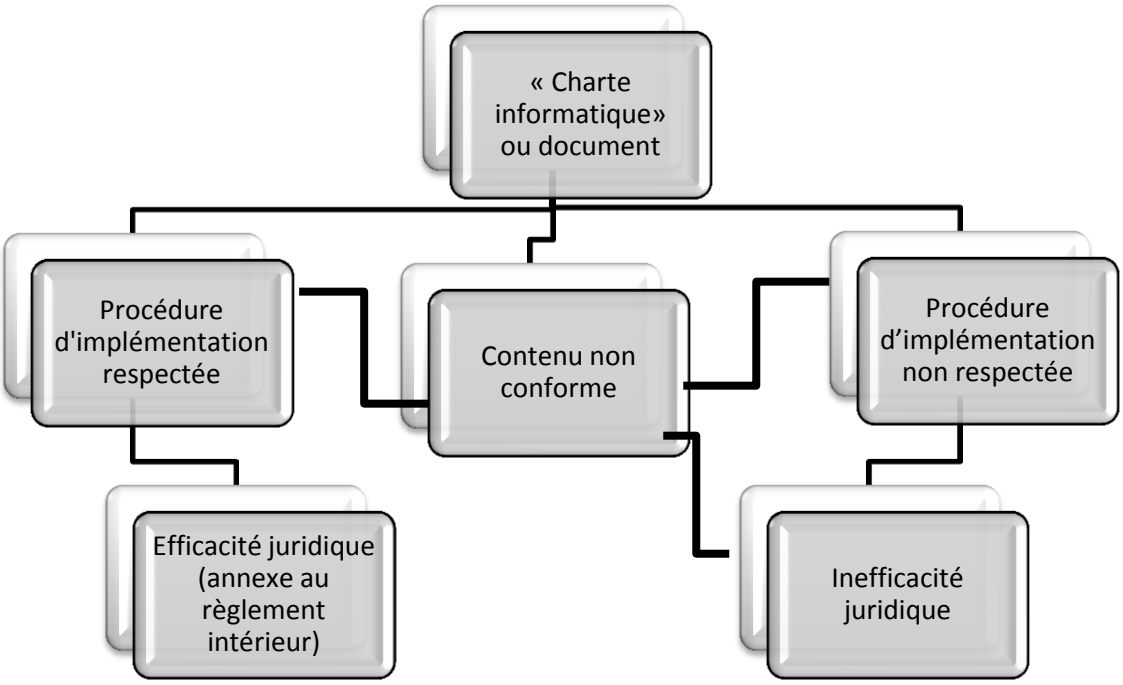
Dans le but de rendre une charte « utilisateurs » opposable aux employés et donc « efficace » juridiquement, une procédure d'implémentation spécifique doit être suivie. Eu égard à son objet, consistant notamment à poser des obligations générales et permanentes concernant les conditions d'utilisation des équipements de travail et à la sécurité au sein de l'entreprise, elle doit être considérée comme une adjonction au règlement intérieur[89], si un tel règlement existe déjà.

La charte constitue alors une annexe au règlement intérieur, dès lors que sa procédure d'implémentation est la même que celle prévue pour la mise en œuvre d'un tel règlement.

Cette procédure d'implémentation de la charte consiste alors à :

- **La soumettre à l'avis du comité d'entreprise ou technique dans les administrations**, à défaut, des délégués du personnel ainsi que, pour les matières relevant de sa compétence, à l'avis du comité d'hygiène, de sécurité et des conditions de travail[90]
- **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[91]
- **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[92]
    - **La transmettre à l'inspecteur du travail en deux exemplaires**[93]

[87] C. trav. art. L. 2323-13.
[88] C. trav. art. L. 4612-8.
[89] C. trav. art. L. 1321-5.
[90] C. trav. art. L. 1321-4.
[91] C. trav. art. R. 1321-1.
[92] C. trav. art. R. 1321-2.
[93] C. trav. art. R. 1321-4.



Par ailleurs, si l'employeur souhaite apporter des **modifications ultérieures** à ce document, il devra de **nouveau respecter la même procédure**.

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 prestation** (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.

La procédure d'acceptation individuelle peut être :

- Écrite
- Implémentée 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 adapté 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 système peuvent ou non déployer les outils, les paramétrer, ou encore accorder à telle ou telle personne une dérogation temporaire ou définitive[94] .

La particularité des chartes dans les administrations

Le dépôt de la charte informatique au greffe du conseil des prud'hommes et sa transmission à l'inspecteur du travail ne concernent 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'État, fonction publique territoriale, fonction publique hospitalière).

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

S'agissant des agents titulaires de l'État, 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** disposent 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'État

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. »

[94] C. trav. art. R. 1321-1.
98 : Il convindra de le traiter dans une charte des administrateurs et du droit étendu

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»[95].

L'acte réglementaire est un acte :

- Général
- Impersonnel ou non nominatif
- Visant une fonction, une institution, ou une situation[96]

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
- À toute personne placée dans la situation d'utilisateur des systèmes d'information

La charte informatique ne doit pas comporter de dispositions manifestement illégales, ou compromettant gravement un intérêt public. 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[97].

La charte doit être adoptée après consultation du comité technique[98] et le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail[99]. Ces comités n'ont qu'un pouvoir consultatif et la décision revient en dernier ressort à l'autorité hiérarchiquement compétente. Néanmoins, leur consultation étant obligatoire dans le cadre d'une charte informatique.
S'agissant des agents contractuels de l'État, 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.

[95] CE sec.7-2-1936 n° 433211 Jamart.
[96] Jurisclasseur administratif, fascicule 106-10 Notion d'acte administratif n°10.
[97] CE sec. 17-2-1950 n° 86949 Dame Lamotte.
[98] Article 15 de la loi n°84-16 du 11 janvier 1984.
[99] Article 16 de la loi n°84-16 du 11 janvier 1984.

S'il s'agit d'un agent public, le droit applicable 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 et 44** du titre, relatifs à la suspension et la discipline.

Selon les dispositions desdits articles, l'agent non titulaire est soumis, de la même manière que le fonctionnaire civil, 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[100].

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

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 d'utilisation 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'atteinte à la vie privée** mais également pouvoir être sanctionnés en cas d'abus des moyens dont ils disposent.

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 recours à la contractualisation de l'obligation de confidentialité pesant sur l'administrateur, notamment dans une charte administrateur, est également consacré par la Commission Nationale de l'Informatique et Libertés dans le cadre du guide pour les employeurs et les salariés édition 2008, et particulièrement de la fiche pratique n° 7.

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 :

[100] Jurisclasseur Administratif Fascicule 193 Agents non titulaires n°65.

- 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 j/7 depuis le poste administrateur[101]
- 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[102]

IV.2.b L'IMPLÉMENTATION « COLLECTIVE »

Les institutions représentatives du personnel doivent également être consultées préalablement à l'introduction de la nouvelle technologie que constitue un logiciel de filtrage[103].

Les membres du comité d'entreprise ou du comité technique dans les administrations et le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail doivent ainsi être informés et recevoir, un mois avant la réunion dudit comité, les éléments d'information sur le projet envisagé et ses conséquences notamment sur les conditions de travail au sein de l'entreprise[104].
Il convient de préciser qu'un avis négatif du comité d'entreprise ou du comité technique ne lie pas l'employeur, et ne l'empêche pas de mettre en place une nouvelle technologie au sein de son entreprise ou de son administration.

En revanche, le défaut de consultation du comité d'entreprise correspond à un délit d'entrave sanctionné à ce titre par le Code du travail.

Le défaut de consultation du comité technique pour les administrations entacherait également la charte d'illégalité.

BONNE PRATIQUE

ADOPTER UNE CHARTE QUI INTÈGRE LE FILTRAGE. LA CHARTE NE SE DÉCLARE PAS À LA CNIL

IV.3 ÉTAPE 4 : ADMINISTRATION ET PARAMÉTRAGE DE LA SOLUTION

Une fois l'implémentation juridique de la mise en œuvre des outils de filtrage traitée (droit du travail et droit Informatique et Libertés 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'exclusion
- **Le traitement égalitaire des utilisateurs**
- **L'utilisation précontentieuse ou contentieuse** des éléments issus des outils de filtrage utilisés.

[101] CA Paris 22ème chambre, 4 10 2007.
[102] TGI Rennes 21 2 2008 n°03-52216.
[103] C. trav. art. L. 2323-13 al. 1.
[104] C. trav. art. L. 2323-13 al. 2.

IV.3.a LE NIVEAU DE PARAMÉTRAGE ET LA QUALITÉ DES LISTES D'EXCLUSION

Sur la première problématique, il faut rappeler que la constitution de listes d'exclusion 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 elles 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.

IV.3.b LE TRAITEMENT ÉGALITAIRE 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.

IV.3.c 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 document 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 concernant des informations et données traitées à travers les outils de filtrage.

IV.4 ÉTAPE 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 (LCEN) 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[105]

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 ».[106]

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 concernant la qualification possible de fournisseur d'accès d'un employeur donnant accès à Internet à ses employés, comme le rappelle la jurisprudence[107].

En pratique, afin de préserver sa responsabilité et donc son pouvoir de contrôle et de direction, l'employeur doit être capable de retrouver à postériori 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.

[105] Décret modifié par le décret n ° 2014-1576 du 24 12 2014
[106] Renvoyant à la LCEN, art 6 I.1°
[107] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005.

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

- **La directive européenne n°2006/24/CE du 15 mars 2006** sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE, prévoit dans son article 6 une **durée de conservation minimale de six mois**, et une durée **maximale de deux ans**[108]

- **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)[109]

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

[108] Voir toutefois la décision de la Cour de justice de l'Union européenne du 8 avril 2014, dans les affaires jointes C-293/12 et C-594/12.
[109] Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2010, p. 18.

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
- La date et l’heure de la transaction

IV.5 ÉTAPE 6 : LE MAINTIEN EN CONDITIONS OPÉRATIONNELLES

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 (notamment à titre de preuve) des éléments issus des outils de filtrage mis en œuvre.

V. DIMENSION INTERNATIONALE DU FILTRAGE

V.1 LA NÉCESSITÉ DE RESPECTER LA RÉGLEMENTATION LOCALE

La mise en place d'une solution de filtrage à l'international exige également que la mise en œuvre d'un tel outil soit faite en conformité avec la réglementation locale.

V.2 LA NÉCESSITÉ DE FILTRER : UNE PRISE DE CONSCIENCE INTERNATIONALE

De nombreux pays ont compris l'intérêt de filtrer les accès à Internet, mettant en place des mesures allant de l'obligation de filtrage imposée par la loi dans certains établissements, au développement de solutions de filtrage que l'on pourrait considérer comme « labellisées ».

En **Espagne**, l'article 12bis 3° de la loi n°34/202 relative aux services de la société de l'information et du commerce électronique[110] impose par exemple l'obligation aux fournisseurs d'accès d'informer les utilisateurs sur les outils existant pour le filtrage et la restriction d'accès à des contenus et services sur Internet qui ne sont pas souhaités ou qui peuvent s'avérer nocifs pour la jeunesse et l'enfance, cette disposition étant entrée en vigueur le 29 mars 2008. Enfin, une loi promulguée le 28 octobre 2014 a prévu l'obligation pour les fournisseurs d'accès à Internet de bloquer l'accès à des sites Internet contrefaisants[111].

L'**Italie** ne semble pas disposer de réglementation spécifique propre au filtrage. Le « Garante per la protezione dei dati personali », équivalent de la CNIL, a toutefois édité un guide conseillant aux employeurs de réduire les risques liés à l'utilisation d'Internet notamment en ayant recours à des filtres afin d'empêcher les salariés d'effectuer un certain nombre d'opérations.

En **Belgique**, la jurisprudence et la doctrine n'abordent encore que de façon très limitée la légitimité des solutions de filtrage. Ainsi, il n'existe pas d'obligation légale pour un employeur de filtrer les accès à Internet de ses travailleurs, mais un tel filtrage peut être considéré comme légitime s'il est réalisé en respectant les normes relatives au respect de la vie privée et la Convention collective du travail n°81.[112]

Aux **États-Unis**, vingt et un états fédéraux ont mis en place des lois imposant le filtrage dans les écoles ou les bibliothèques publiques. Ces lois consistent à imposer la mise en place de politiques visant à assurer la prévention en matière d'accès des mineurs à des contenus notamment obscènes ou pornographiques.

Dans le cadre de ces politiques, l'installation de logiciels de filtrage sur les terminaux d'accès aux bibliothèques publiques ou aux ordinateurs des écoles a été imposée.

Au niveau fédéral, a également été mis en place aux États-Unis le « Federal Children's Internet Protection Act » qui est une loi exigeant de certaines bibliothèques publiques d'attester qu'elles utilisent effectivement des logiciels de filtrage sur leurs ordinateurs, dans un but de protection des mineurs, si elles souhaitent recevoir des fonds fédéraux.

[110] Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.
[111] Ley 121/000081 por la que se modifica el Texto Refundido de la Ley de Propiedad Intelectual.
[112] CCT n° 81 sur la cybersurveillance des travailleurs.

La jurisprudence américaine a, par ailleurs, jugé dans un arrêt de la Cour Suprême[113] que le « Federal Children's Internet Protection Act » n'était pas contraire au premier amendement de la constitution des États-Unis protégeant la liberté d'expression, et ce même si les solutions de filtrage peuvent bloquer des sites « licites ».

Cette compatibilité des logiciels de filtrage avec la constitution américaine tient au fait que les bibliothèques se trouvent en mesure de désactiver les solutions de filtrage pour les adultes employés, à leur demande.

En novembre 2010, une proposition de loi de lutte contre les infractions et la contrefaçon sur Internet (« Combating Online Infringement and Counterfeits Act » ou COICA) a été acceptée par le comité judiciaire du Sénat. Cette proposition de loi permettrait au juge américain, à la demande du procureur général, de rendre une ordonnance ou une injonction contre les noms de domaines des sites Internet suspectés de contribuer à la diffusion de contenus illicites. Cette proposition doit cependant encore être approuvée par le Congrès américain.

La jurisprudence américaine relève qu'à certains égards, la protection des salariés nécessite un filtrage. L'employeur peut ainsi parfois être tenu responsable lorsqu'il ne met pas en œuvre les mesures nécessaires à faire cesser une atteinte.

L'employeur pourrait être ainsi tenu responsable de l'existence d'un environnement de travail hostile, tel que défini par la jurisprudence Harris v. Forklift Systems, Inc. La réception de courriers électroniques non sollicités n'est pas en soi problématique. En revanche, si l'employé a notifié à son employeur le problème rencontré, celui-ci doit mettre en œuvre les mesures correctives propres à faire cesser le trouble, sous peine de voir sa responsabilité engagée. Cette responsabilité peut être indirecte si elle résulte de la tolérance de ce genre de courrier électronique sur le lieu de travail, c'est-à-dire du fait de ne pas avoir pris les mesures nécessaires pour éviter la réception de ce type de courriers électroniques par l'employé. La mise en place de ce type de mesures peut prendre notamment la forme d'un filtrage.

En revanche, la jurisprudence américaine s'attache également à la liberté d'expression des salariés, et notamment dans le cadre syndical. Ainsi, une entreprise peut être contrainte de ne pas filtrer l'accès aux réseaux sociaux, dès lors que les employés les utilisent pour discuter de leurs conditions de travail au sein de l'entreprise. À priori, aucune décision n'est encore intervenue en ce sens. Toutefois, une affaire récente a fait l'objet d'une transaction, avec une couverture médiatique importante, affaire dans laquelle une employée avait été licenciée suite à des propos tenus sur un réseau social. Son employeur, une société d'ambulances, a accepté de modifier sa charte informatique afin de laisser à ses employés la possibilité de discuter de leurs conditions de travail en ligne. Selon le National Labor Relations Board (NLRB), les échanges électroniques des employés font partie de l'exercice de leur droit de discuter de leurs conditions de travail.

En **Chine**, selon une étude menée par l'université Harvard, qui aurait infiltré le web chinois, la censure est réalisée par des outils de filtrage automatique par mots-clés, présents sur un grand nombre de sites, mais ils se révèlent assez inefficaces. Les mots-clés peuvent être contournés par des jeux de mots, des métaphores, ou l'utilisation de caractères phonétiquement semblables à ceux d'un mot-clé, mais dont le sens est complètement différent. En pratique, le contrôle est principalement exercé « à la main », par des dizaines de milliers de censeurs, salariés de sociétés privées ou employés de l'État. Les correcteurs appointés lisent les messages publiés et ceux qui sont retenus par les outils de filtrage, et décident lesquels publier et lesquels supprimer.[114]

[113] Cour Suprême des États-Unis, « United States v. American Library Association », n° 02-361, 23 6 2003.
[114] Site quadrature du net, article « La censure d'internet en Chine vue de l'intérieur », 1 9 2014, Michel de Pracontal.

Au **Canada**, il ne semble pas exister de règles particulières relatives au filtrage au niveau législatif. Néanmoins, la Corporation des bibliothécaires professionnels du Québec a adopté au sein de son code de déontologie un article qui dispose « Si les télé-ressources sont filtrées dans le milieu où il œuvre, le bibliothécaire doit prendre des dispositions pour que la clientèle soit informée de la nature et des motifs du filtrage pratiqué ».

En **Australie** s'est développée la référence à une liste spécifique de solutions de filtrage enregistrées auprès d'une autorité de régulation d'Internet.

Depuis le 1er janvier 2000, la législation du Commonwealth est entrée en vigueur et s'applique notamment aux fournisseurs d'accès. Cette législation exige notamment de ces derniers qu'ils rendent disponible pour leurs clients au moins l'un des produits de filtrage listés par le Code pratique des contenus de l'industrie[115], éventuellement par le biais d'un lien hypertexte par lequel serait téléchargé le logiciel, ou par le téléchargement de ladite solution sur une page spécifique de l'« Association de l'industrie d'Internet »[116], ou par la fourniture d'un CD contenant un filtre à installer. Ces filtres mis à disposition de ces clients listés par le Code pratique des contenus de l'industrie[117] sont enregistrés par l'Autorité australienne des communications et des médias[118], une agence du gouvernement de régulation d'Internet.
Il est ainsi intéressant de voir que l'Australie a, en quelque sorte, « labellisé » des solutions de filtrage proposées aux clients des fournisseurs d'accès.

L'Australie s'est récemment dotée d'une loi relative à la vie privée sur le lieu de travail[119]. Cette loi établit une interdiction générale de blocage des accès Internet et courrier électronique des employés, mais édicte une liste d'exceptions, parmi lesquels la présence d'un cadre de filtrage prédéfini au sein d'une charte informatique. En d'autres termes, le filtrage doit être prévu par la charte informatique. Dans le cas contraire, l'employeur est en infraction s'il en opère un.

En **Russie**, une loi promulguée par le président russe Vladimir Poutine et publiée en juillet 2012 dans le journal officiel russe «Rossiïskaïa gazeta», prévoit « la mise en place d'un registre fédéral qui réglemente l'activité des sites Internet contenant des informations interdites par la loi, obligeant leurs propriétaires ou les fournisseurs d'accès à les fermer. »

La création, la formation et la gestion de ce registre seraient réalisées par un organe du pouvoir exécutif mandaté par le gouvernement russe.
« Cette loi vise en particulier les sites pédopornographiques, faisant l'apologie de la drogue ou donnant des conseils pour procéder à son propre suicide.[120] »

La **Grande-Bretagne** ne semble pas avoir adopté de dispositions législatives propres au filtrage. Toutefois, l'adoption d'une loi [121], proche de la loi Hadopi, nécessite que soient mises en place au niveau des entreprises des mesures techniques destinées à empêcher l'utilisation de réseaux peer-to-peer en provenance ou à destination des entreprises, celles-ci étant responsables de l'utilisation qui est faite de leur accès Internet.

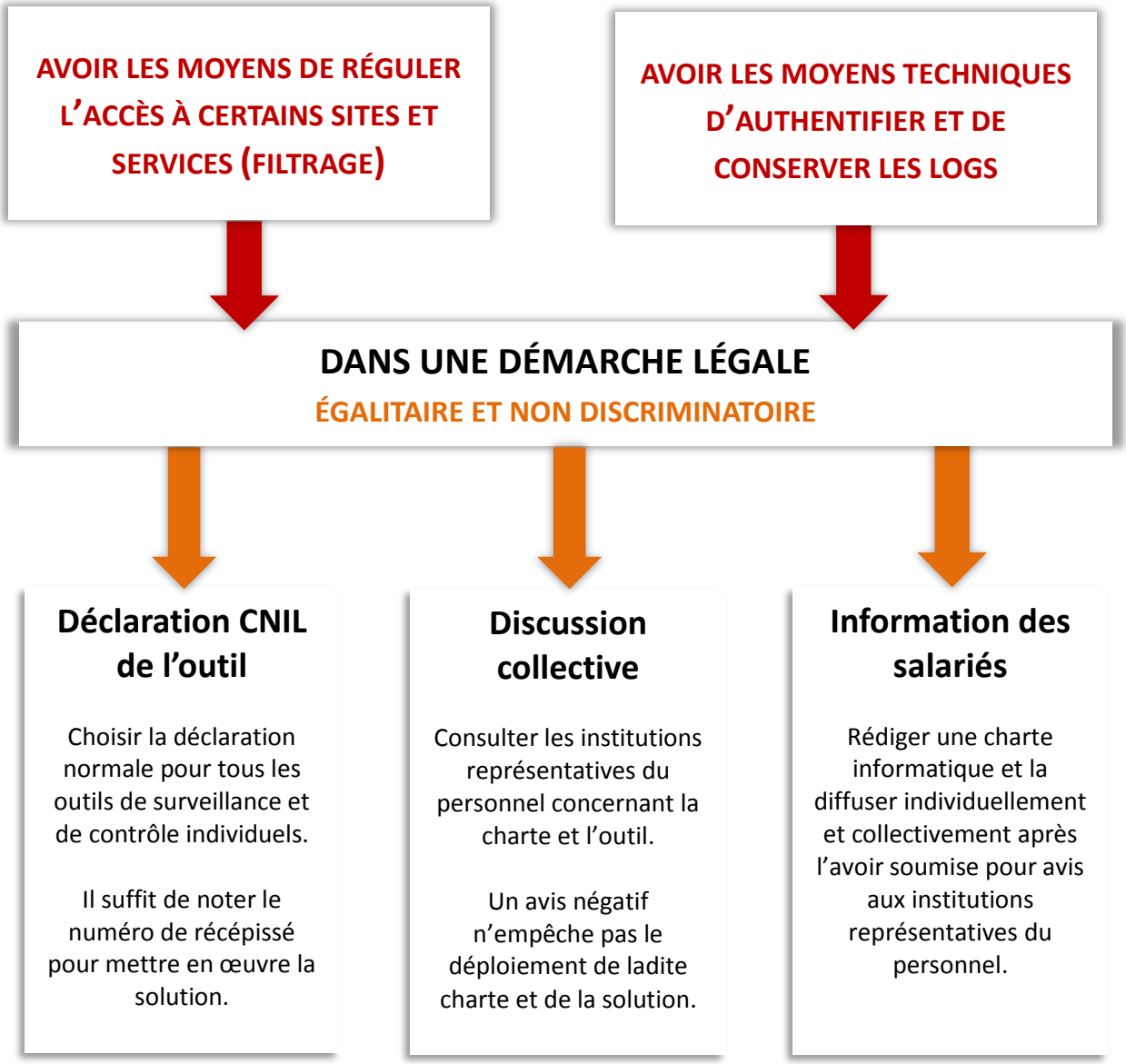
Par ailleurs, un guide[122] a été élaboré notamment par le **Ministère de l'intérieur** en collaboration avec de nombreux fournisseurs de services sur Internet afin d'assurer une plus grande sécurité du réseau pour les mineurs. Ce guide propose notamment comme objectif la mise en place d'un système de

[115] Industry Containt Code of Practice.
[116] Internet Industry Association.
[117] Industry Containt Code of Practice.
[118] Australian Communication and Media Authority.
[119] Workplace Privacy Act 2011
[120] Article accessible à l'URL : www.tdg.ch/Le-Kremlin-va-filtrer-l-internet-russe.
[121] Digital Economy Act.
[122] Good practice guidance for the providers of social networking and other user-interactive services .

blocage des adresses URL contenant des images pédophiles par tous les fournisseurs d'accès britanniques.
Le Ministère de l'intérieur et l'Institut des standards britanniques[123] travaillent d'ailleurs actuellement sur le développement de standards permettant d'évaluer et de tester l'efficacité des solutions de filtrage[124]. Ces travaux déboucheront peut-être sur la même démarche de « labellisation » des logiciels qu'en Australie.

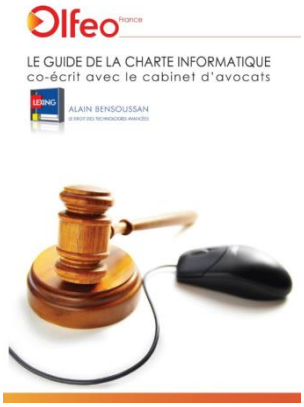
[123] British Standards Institute.
[124] Pour plus d'information : http://police.homeoffice.gov.uk.

VI. LES RÈGLES D'OR DU FILTRAGE : COMMENT PROTÉGER SON ORGANISATION PAR RAPPORT À L'USAGE D'INTERNET CONFORMÉMENT AU DROIT ?



VII. EN SAVOIR PLUS

VII.1 POUR ALLER PLUS LOIN



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

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

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

VII.2 À PROPOS DU CABINET D'AVOCATS ALAIN BENSOUSSAN

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

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

Ces constantes évolutions technologiques ont été source de réflexion et de créativité, l'amenant à rédiger le premier traité de droit de l'informatique en 1985, puis deux ouvrages phares aux Éditions Francis Lefebvre, « Informatique, Télécoms, Internet » (1997, 2001, 2004, 2008, 2012) et « Informatique et Libertés » (2008, 2010) et une collection d'une trentaine d'ouvrages aux éditions Hermès - Lavoisier entre 1991 et 2003. Novateur dans son organisation, sa gestion et son système qualité, son positionnement d'origine, centré sur le droit des nouvelles technologies, l'amène naturellement à intervenir dans tous les autres secteurs des technologies avancées au fur et à mesure de leur apparition et de leur développement.

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

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

Dans sa nouvelle édition 2013, la revue juridique américaine « Best Lawyers » confirme pour la 3ème année consécutive le positionnement d'Alain Bensoussan Avocats qu'il classe parmi les « avocats jugés incontournables » dans les catégories Technologies, Technologies de l'Information, et Contentieux.

De même, pour l'édition 2013 du guide professionnel « Chambers Europe » qui référence cette année encore Alain Bensoussan Avocats parmi les leaders de la catégorie « TMT: Information Technology - France » : « The firm. This team is known across the market for its innovative work in IT law and is one of the largest teams in France to focus solely on IT-related matters. It recently worked with the European Commission on the Intelligent Transport Systems legal framework project ».

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

Enfin, Alain Bensoussan est à nouveau distingué, pour la 4ème année consécutive, par la revue juridique américaine « Best Lawyers » en tant que Best Lawyer en « Droit des Technologies » en 2014-2015.

Site Internet: www.alain-bensoussan.com
Chaîne YouTube: https://www.youtube.com/channel/UC7xrTpr0LGPWVNbYxxDcFVQ
Réseau Lexing : network.lexing.eu/?lang=fr

VII.3 À PROPOS D'OLFEO

Avec plus de 10 ans d'expertise, Olfeo, éditeur français d'une solution de proxy et de filtrage de contenus Internet, apporte une vision exclusive et innovante sur le marché de la sécurité grâce à une approche multi-locale.

La solution Olfeo permet aux entreprises et aux administrations de maîtriser les accès et l'utilisation d'Internet en adéquation avec les exigences culturelles et législatives spécifiques d'un marché. La solution Olfeo est composée de 5 produits complémentaires :

- Proxy cache QoS
- Filtrage d'URL
- Filtrage protocolaire
- Antivirus de flux
- Portail public

Olfeo dispose aujourd'hui d'une version française, suisse, belge, allemande, luxembourgeoise, marocaine, tunisienne et algérienne de sa solution. Cette approche locale garantit une protection juridique optimale, une qualité de filtrage inégalée et une haute sécurité du système d'information.

Olfeo propose également une version internationale de sa solution afin de répondre aux entreprises qui ont des besoins multi-pays.

Cette stratégie d'innovation est plébiscitée par plus de 2000 clients satisfaits, représentant plus de 3 millions d'utilisateurs.

Les avantages exclusifs de la version française de la solution Olfeo :

- Une protection juridique optimale à travers des catégories de filtrage reprenant l'intégralité du périmètre illégal français (Hadopi, Loppsi, ARJEL, lois mémorielles…)
- Une facilité de création de vos politiques de filtrage grâce à des catégories en français conformes à la culture et aux centres d'intérêt des internautes français (débat sur les retraites, logos et sonneries…)

- Un taux de reconnaissance des sites visités par vos utilisateurs supérieur à 98% grâce à la connaissance des habitudes de surf des internautes français
- Une qualité de filtrage inégalée grâce au classement manuel du contenu par des équipes françaises polyglottes
- Le respect du code du travail grâce à la diffusion individuelle de la charte Internet et la conservation des logs des utilisateurs ayant pris connaissance de la charte
- L'association des utilisateurs à votre politique de sécurité grâce à des fonctions exclusives de coaching et d'outrepassement, et la possibilité de personnaliser les messages de blocage
- Une détection instantanée des attaques localisées sur le territoire français grâce à une double protection antivirale
- Un service client dédié et un interlocuteur unique pour accompagner chaque client tout au long de son abonnement

En savoir plus :

www.olfeo.com

Suivre les actualités juridiques, clients et société Olfeo :
http://www.olfeo.com/flux-rss-olfeo

Chaîne YouTube : http://www.youtube.com/user/OlfeoTV

LinkedIn groupe : http://www.linkedin.com/groups/Olfeo-3986777
LinkedIn entreprise : http://www.linkedin.com/company/olfeo