Filtrage et Internet au bureau

LIVRE BLANC JURIDIQUE VOL. I :

Droit de filtrer, droit de loguer

Olfeo
La sécurité positive

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

VOLUME I

DROIT DE FILTRER, DROIT DE LOGUER

Il n'y a plus de doute aujourd'hui, le filtrage est admis sur tous les plans : légal, jurisprudentiel, normatif et de bonnes pratiques ainsi que sur le plan des usages.

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

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

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

PREFACE

« 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 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 Eric Barbry
& Maître Polyanna Bigle

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

LE DROIT DE FILTRER, ASPECT LEGAL

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

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

- **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 protection des mineurs du 18 février 2004** prévoyant « la mise en œuvre d'outils de **filtrage** dans les établissements ou écoles »
- L'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale qui précise que le filtrage est un des éléments des dispositifs de sécurité des systèmes d'information et des informations traitées par le système lui-même (article 89)
- L'instruction interministérielle n° 901/SGDSN/ANSSI en date du 28 janvier 2015 relative à la protection des systèmes d'information sensibles qui précise que le filtrage, notamment le filtrage applicatif (consistant à inspecter l'en-tête et le contenu des paquets IP), est une des mesures à prendre pour assurer la sécurité des réseaux (objectif 31 et annexe 2)
- Les différents arrêtés, pris en application du code de la défense, fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité[1]. L'annexe I de ces arrêtés fixe les règles de sécurité que les opérateurs d'importance vitale sont tenus de respecter pour protéger leurs systèmes d'information. Parmi ces règles

[1] Ces arrêtés datent du 10 juin 2016 pour les secteurs des produits de santé, de la gestion de l'eau et de l'alimentation, du 11 aout 2016 pour les secteurs de l'énergie et des transports et du 28 novembre 2016 pour les secteurs de l'audiovisuel et information, des communications électroniques et internet, de l'industrie et des finances.

l'une concerne le filtrage, obligeant l'opérateur à mettre en place « des mécanismes de filtrage des flux de données circulant dans ses systèmes d'information d'importance vitale (SIIV) afin de bloquer la circulation des flux inutiles au fonctionnement de ses systèmes et susceptibles de faciliter des attaques informatiques ». L'opérateur doit notamment « définir les règles de filtrage des flux de données (filtrage sur adresse réseau, sur protocole, sur numéro de port, etc.) permettant de limiter autant que possible la circulation des flux aux seuls flux de données nécessaires au fonctionnement et à la sécurité de ses SIIV ».

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

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

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

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

Les États membres ont jusqu'au 9 mai 2018 pour adopter les mesures de transposition. A ce titre, le régime juridique applicable au filtrage pourrait évoluer et ainsi être renforcé.

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 » :

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

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

- **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 »[4]
- 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** »[5]
- **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. »
- **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 bloqué à un accès Internet, si le retrait n'a pas été fait sous vingt-quatre heures
- **Un de ses décrets d'application n°2015-125 du 5 février 2015**[6] relatif à la protection des internautes contre les sites provoquant à des actes de terrorisme ou en faisant l'apologie, et les sites diffusant des images et représentation de mineurs à caractère pornographique, pris pour l'application de l'article 6-1 de la loi n °2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique

[4] 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 ».

[5] 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 oeuvre 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.

[6] 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

S'il concerne expressément les fournisseurs d'accès à Internet, le décret **décrit les modalités de blocage des sites** contrevenant **aux dispositions des articles 227-23 et 421-2-5 du Code pénal** « précise la procédure permettant d'empêcher l'accès des internautes aux sites incitant à la commission d'actes de terrorisme ou en faisant l'apologie et aux sites diffusant des images et représentations de mineurs à caractère pornographique. »

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

Depuis la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, le fait de consulter habituellement un site internet mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes, est sanctionné par l'article 421-2-5-2 du code pénal. Bien que ce texte ne renvoie pas directement au filtrage de sites internet, il peut cependant constituer une base juridique à un dispositif mis en œuvre pour filtrer les sites dont la consultation habituelle est prohibée par la loi (dispositif de blocage institué par un employeur ou alerte mise en œuvre dans les établissements d'enseignement par exemple).

Concernant les sites terroristes qui pourraient être consultés, des mesures de filtrage peuvent être prises afin de prévenir des comportements de radicalisation. Une alerte automatique pourrait être mise en œuvre afin de transmettre à un service compétent des informations relatives à la consultation de sites internet identifiés comme « radicaux ». Dans l'hypothèse où une telle alerte conduit à collecter et traiter des données à caractère personnel (nom et prénom, horaires et lieux de connexion, etc.) des mesures particulières doivent être prises afin d'assurer la sécurité de ces données et de protéger les droits des personnes. Plus largement, certains services de l'Etat, tels que les préfectures ou encore les référents radicalisation pour l'Education nationale (voir notamment le guide interministériel de prévention de la radicalisation), peuvent intervenir dans la mise en place de certains dispositifs de lutte contre la radicalisation.

CE QU'IL FAUT RETENIR…

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

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[7]
- Vente de parfums Christian Dior en dehors de leur réseau de distribution sélectif[8]
- Diffusion de pages à contenus racistes[9]
- Diffusion de propos négationnistes[10]
- Jeux en ligne et paris hippiques[11]
- Site d'hébergement de vidéos (YouTube[12], Dailymotion[13])

Déjà en 2010, **le Président du Tribunal de grande instance de Paris**[14] a ordonné, en application de la loi du 12 mai 2010 relative à la concurrence et à la **régulation du secteur des jeux d'argent et de hasard en ligne**, aux fournisseurs d'accès à Internet, de prendre **« toute mesure de filtrage**, pouvant être obtenue par blocage du nom de domaine, de l'adresse IP connue, de l'URL, ou par analyse du contenu des messages, mises en œuvre alternativement ou éventuellement concomitamment, de manière à ce qu'elles soient suivies de l'effet escompté sur le territoire français ».

La cour d'appel de Paris a reproché à une société de courtage **de ne pas avoir mis en œuvre un filtrage efficace**[15], et le même jour de ne pas avoir détaillé le fonctionnement effectif d'un tel filtrage ni détaillé ses résultats[16].

Dans une décision du 14 décembre 2010, **le Tribunal de Grande Instance de Créteil**[17] a fait injonction à un hébergeur **d'installer sur son site un système de filtrage efficace et immédiat** des vidéos dont la diffusion a été ou sera constatée par l'Institut National de l'Audiovisuel (INA).

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

Cette jurisprudence en matière de filtrage s'est développée depuis le début des années 2000, en particulier en parallèle du développement de la vente sur Internet, ce qui a posé un certain nombre de problématiques liées à l'accès à des sites illicites.

De 2011 à 2014, la position de la jurisprudence en matière de filtrage à l'égard des fournisseurs d'accès à Internet et hébergeur s'est assouplie, avec notamment deux arrêts du même jour de la Cour de cassation. **Il en ressort que les fournisseurs d'accès à Internet ne sont pas astreints à effectuer contrôle permanent et a priori d'Internet.** [18].

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

CE QU'IL FAUT RETENIR…

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

[18] Cass civ-1 7 2012 n° 11-15.165 et 11-15.188

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 »,** 11 février 2002
- **Le rapport de la CNIL** « **La cyber surveillance 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 cyber surveillance particulièrement intrusifs, 20 mars 2013
- **L'article de la CNIL sur « l'analyse des flux https : bonnes pratiques et questions »,** 31 mars 2015

Dans son guide pratique pour les employeurs et les salariés[19], 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 ».

[19] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2010 p. 18.
Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition mars 2004, p. 12.

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, racisme…

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

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

Chaque employé doit être notamment informé :

- Des finalités poursuivies
- 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 keys loggers, qui tracent tous les caractères saisis sur un clavier par un utilisateur sur son ordinateur. Ils permettent ainsi à un employeur de connaitre 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, certains dispositifs de captation de données informatiques à l'insu des personnes concernées.[20]

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

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

  Ce document vise à procurer les éléments organisationnels qui permettent de structurer la base de règles sur lesquelles s'appuie la politique de filtrage réseau appliquée sur un pare-feu d'interconnexion.

  Il est destiné à toutes les personnes ayant pour mission d'élaborer et d'appliquer ou d'administrer des architectures d'interconnexion sécurisées, qui désirent s'assurer que leurs des 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.

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

- Les référentiels d'exigences publiés par l'ANSSI et applicables aux prestataires d'audit de la sécurité des systèmes d'information (PASSI), aux prestataires qualifiés en matière de détection des incidents de sécurité (PDIS) et aux prestataires de réponse aux incidents de sécurité (PRIS) prévoient des obligations particulières de filtrage:
    - dans le référentiel applicable aux PASSI, les exigences de l'ANSSI relatives au déroulement d'une prestation d'audit incluent un audit d'architecture consistant en la revue des règles de filtrage et un audit de configuration afin de vérifier la sécurité des configurations des équipements de sécurité « type pare-feu ou relais inverse (filtrant ou non) et leurs règles de filtrage, chiffreurs, etc. » (articles VI.4.1 et VI.4.2 et annexe 3) ;
    - le filtrage est au cœur du référentiel applicable aux PDIS dans la mesure où le système d'information du service de détection des incidents de sécurité (service assurant la gestion des incidents, événements et notification au sens de l'article II.1) est organisé en zones de confiance, cloisonnées entre elles par des mécanismes de filtrage, d'authentification et de contrôle d'accès (article II.2). Le filtrage constitue donc un dispositif essentiel afin d'assurer le respect des exigences relatives à la protection de l'information (articles II.3, IV.2.2, IV.3.10 et suivants), la politique de filtrage devant être maintenue à jour en permanence (articles IV.3.7) ;
    - le référentiel applicable aux PRIS prévoit de nombreuses exigences relatives au déroulement d'une prestation de réponse aux incidents de sécurité. A ce titre un plan de remédiation (visant à limiter la compromission, enrayer l'activité de l'attaquant et durcir la sécurité du système d'information de la victime) doit être élaboré et devant prévoir un « durcissement de la politique de filtrage » (article VI.6.6). La politique de filtrage est d'ailleurs un prérequis que le commanditaire de l'audit doit fournir au prestataire avant la réalisation de la prestation (annexe 4).

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 SI ET DE LA SÉCURITÉ

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 ?

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** »[21]
- 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[22]
- 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[23]
- Les « **données de nature à permettre l'identification** » prévus à l'article 6 II de la LCEN et énumérées au sein du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication de données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne [24]

Il en est de même de la jurisprudence :

[21] 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.
[22] Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
[23] 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.
[24] 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.

Dans **un arrêt du 9 juillet 2008**, **la Cour de Cassation**[25] 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 rendu par la **Cour de cassation** le 9 **février 2010**[26] et par la **Cour d'Appel d'Aix en Provence** dans un arrêt du **22 février 2013**[27], ainsi qu'implicitement dans un **arrêt du 10 mai 2012** de **la Cour de Cassation** en confirmant l'arrêt d'appel.[28]

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 de son salarié. Ainsi dans **l'arrêt du 10 mai 2012** précité, elle précise que « si l'employeur peut toujours consulter les fichiers qui n'ont pas été identifiés comme personnels par le salarié, il ne peut toutefois les produire dans une procédure judiciaire, si leur contenu relève de la vie privée sans l'accord de ce dernier. »[29]

Ainsi que pour la CNIL :

La CNIL qui utilise les termes de « fichiers logs » ou « fichier de journalisation »[30] a publié un certain nombre de documents relatifs aux logs et notamment :

- **Les Fiches de synthèse « Cyber surveillance sur les lieux de travail » du 11 février 2002** où elle utilise les termes de « fichiers logs ou de journalisation »[31]

- **Le rapport de la CNIL « La cyber surveillance 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 a posteriori un accès frauduleux à des données personnelles, une utilisation abusive de telles données, ou de déterminer l'origine d'un incident, il convient d'enregistrer les actions effectuées sur le système informatique.

---

[25] 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 ».

[26] 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.»

[27] 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. »

[28] Cass-soc 10 05 2012 n° 11-11.252

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

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

- 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 logs») des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou 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. »

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

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

La 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 »[32]

- 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[33]

- Dans un arrêt rendu le **19 Janvier 2012**, **la Cour d'appel de Paris** a relevé que le salarié avait procédé à un usage anormal de l'outil informatique qui lui était confié, en installant des logiciels sur le poste de travail alors que cela était formellement **interdit par la charte informatique**[34]

- A la suite **du jugement du Conseil de Prud'hommes de Nice du 30 octobre 2012**, la **Cour d'appel d'Aix-en-Provence** a rendu un **arrêt le 13 janvier 2015** validant le licenciement pour faute grave d'un salarié qui passait plus d'une heure par jour sur Internet pour son usage personnel. La Cour d'appel retient ainsi **une violation délibérée et répétée de la charte informatique, et fait droit aux arguments de son employeur** arguant notamment lui avoir payé de très nombreuses heures de présence sans contrepartie d'un travail effectif

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

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

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[35].

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 « Cyber surveillance 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 une 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 notamment 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**[36], prévoit la mise en place d'une charte d'utilisation des moyens informatiques et de communication électronique pour les employés et également une charte administrateur pour l'accès aux données cryptées.

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), dans sa version 2.0 publiée par arrêté du Premier ministre du **13 juin 2014** et applicable depuis le **1er juillet 2014**, qui préconisent l'adoption d'une charte informatique.

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

Pourtant, les incidents liés aux systèmes d'information se sont multipliés depuis ces dernières années et notamment celles dues à une défaillance au sein même de l'entreprise, les pannes d'origines internes étant passées de 25 % à 35 % entre 2012 et 2014[37]

[35] Cnil « Cybersurveillance sur les lieux de travail » 11 2 2002.
[36] Recommandation de l'ANSSI Flux HTTPS n°DAT-NT-19/ANSSI/SDE/NP, 9 10 2014.

CE QU'IL FAUT RETENIR…

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

POUR EN SAVOIR PLUS

> CONSULTEZ NOTRE "GUIDE DE LA CHARTE INFORMATIQUE" CO-ÉCRIT PAR LE CABINET ALAIN BENSOUSSAN AVOCATS

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

DIMENSION INTERNATIONALE DU FILTRAGE

LA NECESSITE DE RESPECTER LA REGLEMENTATION LOCALE

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

LA NECESSITE 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[38] 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 [39]

En **Belgique**, le filtrage peut être considéré comme légitime s'il est réalisé en respectant, entre autres, les normes relatives au respect de la vie privée et la Convention collective du travail n° 81.[40] Pour plus d'information, consultez notre Livre Blanc Juridique sur le filtrage en partenariat avec le cabinet d'avocats Belge Altius.[41]

Aux **Etats-Unis**, plusieurs Etats 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.

[38] Ley 34/2002 de servicios de la sociedad de la informacion y de comercio.
[39] Ley 121/000081 por la que se modifica el Texto Refundido de la Ley de Propiedad Intelectual
[40] CCT n° 81 sur la cybersurveillance des travailleurs
[41] https://www.olfeo.com/fr-BE/demande-telechargement-du-livre-blanc-juridique-olfeo

Au niveau fédéral, a également été mis en place aux Etats-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.

La jurisprudence américaine a, par ailleurs, jugé dans un arrêt de la Cour Suprême[42] que le « Federal Children's Internet Protection Act » n'était pas contraire au premier amendement de la constitution des Etats-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 contrefaçon sur Internet (« Combating Online Infringement and Counterfeits Act » ou COICA) a été adoptée 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. A 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 infiltrée 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

[42] Cour Suprêmedes Etats Unis, « United States v. American Library Association », n° 02-361, 23 6 2003.

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[43].

La **Chine** a adopté le «Computer Information Network and Internet Security, Protection and Management Regulations » qui impose des obligations particulières aux fournisseurs d'accès, les contraignant par exemple à ne pas permettre que les services internet qu'ils fournissent soient utilisés pour, entre autres, porter atteinte à la sûreté de l'Etat ou participer à des activités criminelles[44].

Il en est de même à **Singapour** où le « Broadcasting act » prévoit des obligations particulières de filtrage applicables aux fournisseurs d'accès à internet, obligeant ces derniers à être en mesure de fournir des solutions de filtrage à leurs abonnés[45].

En **Inde**, l' « Information Technology Act » autorise le gouvernement à bloquer l'accès à certains sites internet lorsque la « souveraineté et l'intégrité, la défense et la sécurité de l'Etat » le justifie. De surcroît, les règles spéciales applicables aux cybercafés[46] disposent que ces derniers doivent disposer de dispositifs de filtrage empêchant l'accès aux sites pornographiques ou terroristes[47].

Au **Canada**, des règles particulières ont été adoptées par la Corporation des bibliothécaires professionnels du Québec, au sein de son code de déontologie et notamment un article qui dispose que « 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[48], 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 »[49], 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[50] sont enregistrés par l'autorité australienne des communications et des médias[51], 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. 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.

[43] Site quadrature du net, article « La censure d'internet en Chine vue de l'intérieur », 1 9 2014, Michel de Pracontal
[44] Computer Information Network and Internet Security, Protection and Management Regulations, 30 12 1997.
[45] Broadcasting Act, 15 10 1994.
[46] Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
[47] Plus d'informations sur le filtrage disponible sur: https://freedomhouse.org/report/freedom-net/2015/india.
[48] Industry Containt Code of Practice.
[49] Internet Industry Association.
[50] Industry Containt Code of Practice.
[51] Australian Communication and Media Authority.

En **Russie**, la loi fédérale n°436-Φ3 du 21 décembre 2010 tel que modifié par la loi fédéral n°139- Φ3 du 28 juillet 2012 et n°50- Φ3 du 5 avril 2013 et n°135- Φ3 du 29 juin 2013, relative à la protection des enfants contre les informations portant préjudice à leur santé et à leur développement prévoit le développement et la mise en œuvre d'une politique unifiée de l'Etat Fédéral de Russie pour protéger les enfants contre les informations qui sont préjudiciables à leur santé et à leur développement[52]. Dans ce cadre, cette loi prévoit notamment d'établir des procédures pour examiner les informations[53] ainsi que les modalités du contrôle du respect de l'application de cette loi Fédérale par l'Etat[54].

Les informations contrôlées sont celles destinées à circuler sur le territoire de la Fédération de Russie diffusées par les médias audiovisuel ou télévisuel, dans les publications, quel qu'en soit le support qu'il s'agisse de logiciel (programme informatique), de bases de données, ainsi que toutes informations diffusées par le biais d'un événement ou d'un spectacles, par tous moyens y compris tous système de télécommunication, en ce compris le réseau internet ou les réseaux de communications de téléphonie mobile[55].

Cette loi vise notamment les contenus pornographique[56], violent[57], à langage grossier[58], ou ayant pour objet d'encourager la cruauté[59], de nier les valeurs familiale[60], d'induire les enfants à se droguer, à prendre des psychotropes, du tabac ou d'alcool[61] ou donnant des conseils pour procéder à son propre suicide[62][63].

Un système de classification des informations est mis en place[64] dont les catégories sont déterminées en fonction de l'âge des enfants allant des informations accessibles aux enfants de moins de six ans jusqu'aux informations interdites aux enfants. Ce classement prend notamment en compte le thème du contenu, la manière dont l'information peut être perçue par l'enfant, le taux de risque qu'elle a de porter atteinte à la santé ou au développement de l'enfant[65].

La création, la formation et la gestion de cette classification sont réalisées par des experts et/ou des organisations d'expert accrédité(e)s par le gouvernement de la Fédération de Russie. Cette classification est menée notamment à la demande des organes exécutifs fédéraux, des collectivités locales, ou des personnes morales[66].

Les informations interdites ne doivent notamment pas être accessibles dans les établissements scolaires, les centres de santé, les centres de sport, les institutions culturelles[67].

En **Grande-Bretagne,** l'adoption d'une loi[68] proche de la loi Hadopi, nécessite que soit mis 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.

---

[52] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 4 1° 1), traduite dans le cadre du présent livre blanc.
[53] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 4 1° 3) traduite dans le cadre du présent livre blanc.
[54] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 4 1° 4) traduite dans le cadre du présent livre blanc.
[55] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 2 5) traduite dans le cadre du présent livre blanc.
[56] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 5 2° 7) traduite dans le cadre du présent livre blanc.
[57] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 5 2° 3) traduite dans le cadre du présent livre blanc.
[58] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 5 2° 6) traduite dans le cadre du présent livre blanc.
[59] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 5 2° 3) traduite dans le cadre du présent livre blanc.
[60] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 5 2° 4) traduite dans le cadre du présent livre blanc.
[61] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 5 2° 2) traduite dans le cadre du présent livre blanc.
[62] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 5 2° 1) traduite dans le cadre du présent livre blanc.
[63] Article site internet accessible à l'Url : www.tdg.ch/ Le-Kremlin-va-filtrer-l-internet-russe
[64] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, chapitre 2 : Classification des informations.
[65] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 6 2° traduite dans le cadre du présent livre blanc.
[66] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 17 1° traduite dans le cadre du présent livre blanc.
[67] Loi n°436-Φ3 du 21 décembre 2010 tel que modifié, art. 16 traduite dans le cadre du présent livre blanc.
[68] Digital Economy Act.

Par ailleurs, un guide[69] 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 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[70] travaillent d'ailleurs actuellement sur le développement de standards permettant d'évaluer et de tester l'efficacité des solutions de filtrage[71]. Ces travaux déboucheront peut-être sur la même démarche de « labellisation » des logiciels qu'en Australie.

Le filtrage des sites à contenu pornographique devrait se trouver faciliter depuis la récente création de l'organisme chargé de réglementer les noms de domaine d'Internet, l'Icann, d'adresses avec le suffixe.

[69] Social Networking Guidance.
[70] British Standards Institute.
[71] Pour plus d'information : http://police.homeoffice.gov.uk.

POUR ALLER PLUS LOIN…

Découvrez les 3 volumes suivants sur les enjeux juridiques du filtrage Internet :

Volume II :
Nouveaux usages et filtrage

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

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

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

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

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

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

A PROPOS D'OLFEO

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

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

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

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

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

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

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

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

www.linkedin.com/company/olfeo

https://twitter.com/olfeo

www.youtube.com/user/OlfeoTV

www.facebook.com/societeolfeo

A PROPOS DU CABINET D'AVOCATS LEXING ALAIN BENSOUSSAN

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

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

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

Maître Eric Barbry

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

Maître Polyanna Bigle

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

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

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

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

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

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

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

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

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

www.alain-bensoussan.com

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

www.youtube.com/channel/UC7xrTpr0LGPWVNbYxxDcFVQ