LIVRE BLANC JURIDIQUE

co-écrit par

Olfeo et LEXING ALAIN BENSOUSSAN LE DROIT DES TECHNOLOGIES AVANCÉES

Filtrage et Internet au bureau : Enjeux et cadre juridique

2ème édition

SOMMAIRE

PREFACE

La préface est signée Maître Eric Barbry, avocat au Barreau de Paris et Directeur du Pôle « Droit du numérique » du cabinet Alain Bensoussan.

Ce livre blanc a d'ailleurs été écrit avec Maître Barbry.

« 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 ».

Enfin sur un plan technologique, le filtrage n'est plus limité qu'aux seuls accès au Web. Le filtrage d'url cède ici la place à un filtrage plus étendu : le filtrage protocolaire qui emporte lui aussi son lot de problématiques juridiques **»**.

Maître Eric Barbry,

1. 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 de bonnes pratiques ;
- Et au 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 car il ne saurait être question de filtrer sans informer. Or l'information des personnels passe principalement sinon prioritairement par le déploiement d'une charte d'usage des systèmes d'information.

1.1. 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 » ;

- **L'arrêté du 27 juin 1989**, 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 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 » ;

Le droit communautaire reconnaît depuis plus longtemps encore le droit de filtrer, et ce depuis 1999 à travers :

- **La décision 276/1999 CE du 25 janvier 1999 du Parlement européen et du Conseil** adoptant un plan d'actions 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[1] met en avant le fait que les outils de filtrage constituent des éléments essentiels pour assurer un environnent plus sûr sur Internet ;

[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 ».

- 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).

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 L336-2 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 4 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure** vient modifier l'article 6 I.- 7° : « Lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai. »

- **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. »

- **Le projet de décret d'application de l'article 18 de la LCEN** utilise les termes « **interdire l'accès** de tout ou partie du site aux mineurs », « **faire cesser l'accès** ».
  Le projet de décret a été soumis pour avis au Conseil national du Numérique (CNN), nouvelle instance consultative dans le domaine du numérique créée par le décret n° 2011-476 du 29 avril 2011.

[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 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.

Le 17 juin 2011, le CNN a rendu son avis et recommande notamment :

- de modifier l'article 4 du projet de décret, qui permet, en cas d'urgence, d'enjoindre directement aux FAI de faire cesser l'accès au contenu sans s'adresser préalablement à l'auteur du contenu litigieux. En effet, le CNN rappelle que le rôle premier des FAI n'est pas de contrôler ou d'empêcher la propagation de contenu publié sur internet mais de s'« assurer de sa diffusion conformément au principe constitutionnel de la liberté d'expression et de communication » ;

- de modifier la possibilité pour une autorité administrative de pouvoir ordonner des blocages et des filtrages sur internet sans recourir à un juge. S'appuyant sur la jurisprudence du Conseil constitutionnel, le CNN recommande que cette mesure ne puisse intervenir qu'au terme d'un débat contradictoire, sous l'appréciation et le contrôle préalable d'un juge, et selon une procédure instituée par voie législative ;

- de supprimer la possibilité de sanctionner pénalement les hébergeurs qui méconnaîtraient les injonctions de l'autorité administrative et de clarifier la portée de la sanction complémentaire de « confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou la chose qui en est le produit ».

- **Le projet de loi renforçant les droits, la protection et l'information des consommateurs** prévoit la possibilité pour la DGCCRF de demander à l'autorité judiciaire d'ordonner toutes mesures propres à **prévenir un dommage ou à faire cesser un dommage occasionné par le contenu** d'un service de communication au public en ligne.

 Ce qu'il faut retenir…

Nombreux sont les textes de loi qui imposent ou légitiment le recours au filtrage.

1.2. 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/plate-formes illicites dans beaucoup de domaines :

- Vente d'objets nazis sur le site yahoo.com accessible depuis la France[4] ;
- Vente de parfums Christian Dior en dehors de leur réseau de distribution sélectif[5] ;
- 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]) ;
- Les moteurs de recherche.

[4] TGI Paris, 22-5-2000.
[5] CA Paris, 3-9-2010 n°08/12822.
[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.

Plus récemment **le Président du Tribunal de grande instance de Paris**[11] a ordonné le 6 août 2010, 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**[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 a été ou sera constatée par l'Institut National de l'Audiovisuel (INA).

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

Dans tous ces cas jurisprudentiels, il est question de mettre en place des mesures de filtrage faisant obstacle à l'accès aux sites Internet ou à des pages Internet illicites.

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 utilisent couramment la technique de filtrage pour imposer une restriction d'accès.

1.3. 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 ».

Dans son guide pratique pour les employeurs et les salariés[15], 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

[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] 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.

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 pornographique, pédophile, révisionniste …

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.

 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.

1.4. LE FILTRAGE ET LES USAGES

Le « droit » ne se limite pas aux textes de loi, jurisprudence 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.

On estime que 70% des entreprises utiliseraient une solution de filtrage.

Il faut cependant relativiser ce chiffre car bon nombre d'entre elles ne font pas appel à des solutions dédiées mais utilisent des solutions qui sont intégrées dans des UTM sensés régler toutes les problématiques des accès web d'une entreprise : anti-virus, anti-spam, contrôle d'accès ….

La plupart des grandes entreprises pour leur part, et des entreprises exposées, ont opté pour des solutions dédiées proposées par des entreprises spécialisées.

 Ce qu'il faut retenir…

70% des entreprises filtrent… et vous ?

1.5. 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** »[16] ;
- Les « **données de connexion** à des services de communications électroniques »[17] ;
- Les « **données de connexion** »[18]
- Les « **données d'identification** » 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.

Il en est de même de la jurisprudence :

Dans **un arrêt du 9 juillet 2008**, **la Cour de Cassation**[19] 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 un autre arrêt rendu le 9 février 2010[20].

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).

Ainsi que pour la Cnil :

La Cnil qui utilise les termes de « fichiers logs » ou « fichier de journalisation »[21] a publié un certain nombre de documents relatifs aux logs et notamment :

[16] 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.
[17] CPCE art. L. 34-1-1, encadrant en particulier la communication des données de connexion afin de prévenir les actes de terrorisme introduit par la loi n° 2006-64 du 23-1-2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.
[18] Fiches de synthèse « Cybersurveillance sur les lieux de travail » du 11-2-2002 de la Cnil.
[19] 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 ».
[20] Cass soc 9-2-2010 n°08/45253 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.»
[21] Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition mars 2004.

- **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 »[22] ;

- **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 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. 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. »

1.6. 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 des matériels et 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 »[23].

[22] Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition mars 2004.
[23] Cass soc. 21-12-2006, n°05-41.165.

- 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[24].

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[25].

Dans un certain nombre de documents, la Commission rappelle la nécessité d'informer les IRP 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 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.

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.

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) qui préconisent l'adoption d'une charte.

Selon l'étude 2010 sur les menaces informatiques et les pratiques de sécurité en France réalisée par le CLUSIF (Club de la sécurité de l'information français), 67 % des entreprises interrogées ont une charte d'utilisation des systèmes d'information soit une augmentation de 17% par rapport à 2008. Près de 83% des entreprises de plus de 1000 personnes disposeraient d'une charte.

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.

[24] Cass. soc. 15-12-2010, n° 09-42691.
[25] Cnil « Cybersurveillance sur les lieux de travail » 11-2-2002.

2. LES NOUVEAUX USAGES - LE NOUVEAU FILTRAGE

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

Deux usages nouveaux se sont répandus : l'accès intensif des entreprises aux réseaux sociaux d'une part ; l'accès public à Internet d'autre part.

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

2.1. LES RESEAUX SOCIAUX ET L'ENTREPRISE

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

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

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

- Travail en réseaux (networking) ;
- Travail en communauté (hubworking) ;
- Web TV d'entreprise ;
- Communication 2.0 (facebook, …) ;
- Mise en contact pro via plusieurs plates-formes ;
- Tweet et blog d'entreprise …

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

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

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

En terme 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[26].

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 inédit et important. En effet, si beaucoup de législations leur sont applicables notamment la législation relative aux droits d'auteur, à la loi Informatique et libertés, les incriminations relatives aux STAD[27] ou encore la loi pour la confiance dans l'économie numérique, bien d'autres règles s'appliquent à l'utilisation d'internet telles que la liberté d'expression et les limites qui sont les siennes: diffamation, injure, dénigrement, concurrence déloyale, pour ne citer que les principales.

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

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

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

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 19 novembre 2010, le conseil de prud'hommes** a dit le licenciement pour faute grave des deux salariées fondé considérant que « [l'un des salariés] a choisi dans le paramètre de son compte, de partager sa page Facebook avec « ses amis et leurs amis » permettant ainsi un accès ouvert notamment par les salariés ou anciens salariés de la société. (…) ce mode d'accès à Facebook dépasse la sphère privée (…) la production aux débats de la page mentionnant les propos incriminés constitue un mode de preuve licite du caractère bien fondé du licenciement ». Les deux salariées ont interjeté appel.

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. L'entreprise doit donc trouver un moyen pour se prémunir des risques.

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…). Il faut toutefois que cela soit indiqué de manière spécifique et colle à l'activité de l'entreprise.

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

Malgré tout, devant l'ampleur du phénomène et la présence grandissante des communications d'entreprise sur les réseaux sociaux, il paraît de plus en plus difficile d'interdire strictement l'accès à ce type de réseau.

C'est la raison pour laquelle le filtrage cède de plus en plus le pas vers ce que l'on appelle l'administration des accès web.

Il ne s'agit plus d'autoriser les uns et d'interdire les autres, mais de prévoir, en fonction des besoins de l'entreprise, qui aura accès à quoi et pour y faire quoi.

 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

2.2. LES ACCES PUBLICS AU WEB

L'accès public au web se développe comme une traînée de poudre.
Hier limitée aux cybercafés et à quelques aéroports pionniers dans le domaine des hot spot, aujourd'hui l'accès public au web est partout : salons, hôtels, restaurant, point d'information public,…).

Il faut ici rappeler deux réalités juridiques :

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

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

Les entreprises fournissant un réseau interne ouvert au public au sein de l'entreprise constituent des réseaux internes ouverts au public[28]. Ces réseaux ne sont pas soumis à l'obligation de se déclarer opérateur auprès de l'Arcep, seuls les réseaux ouverts au public sont soumis à l'obligation de déclaration[29].

- **L'article L. 336-3 alinéa 1, 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. »

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

 Le saviez-vous ?

Toute personne qui « offre » un accès public peut voir sa responsabilité engagée du fait des accès illicites des tiers.

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

2.3. LES FLUX SECURISES : HTTPS, FTPS, …

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

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

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

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

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

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

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

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

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

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

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

Elles doivent pour cela à minima :

- Recueillir, en complément de la charte Internet, l'autorisation individuelle des collaborateurs pour un déchiffrement de ces flux ;

- Modifier leur déclaration Cnil pour spécifier qu'elles pourront accéder à de telles données.

2.4. LE FILTRAGE ETENDU

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 est en train d'évoluer vers un filtrage étendu : le filtrage protocolaire.

Encore peu répandu il sera à n'en pas douter rapidement déployé par les entreprises et remplacera vite le seul filtrage URL au cœur des bonnes pratiques de l'entreprise.

 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.

3. NE PAS FILTRER, NE PAS LOGUER : QUELLES CONSEQUENCES ?

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

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

3.1. 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 français.

Or sur ce point la règle est simple :

- **Au civil, l'article 3 de la loi n° 66-537 du 24 juillet 1966** sur les sociétés commerciales **et à l'article 1837 du Code civil** disposent 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. »

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

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.

3.2. QUELS RISQUES ?

Les risques de ne pas filtrer sont de deux niveaux :

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

3.2.1. LE NON-RESPECT DE L'OBLIGATION LEGALE DE FILTRAGE

3.2.1.1. 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, aurait pour certains auteurs, assimilé l'employeur qui donne accès à ses employés à Internet, à un fournisseur d'accès.

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

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

- De **conserver les données d'identification** énumérées au sein du décret 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.

3.2.1.2. Le risque spécial : Hadopi

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 ?

La loi Hadopi renforce l'obligation de filtrage des entreprises

3.2.2. LE RISQUE POUR UNE ENTREPRISE DE NE PAS FILTRER

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.

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[30].

3.2.2.1. 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.

3.2.2.2. Le risque pénal

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

L'entreprise pourrait donc voir sa responsabilité engagée pour des accès illicites :

- **A 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, faisant actuellement l'objet d'une proposition de loi en cours de discussion[31];

[30] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005 ; cet arrêt aurait pour certains auteurs, assimilé l'employeur qui donne accès à ses employés à Internet, à un fournisseur d'accès.
[31] Proposition de loi de Madame Boyer visant à combattre l'incitation à l'anorexie n° 781, déposée le 3-4-2008 devant l'Assemblée nationale.

- **A des sites de jeux en ligne illégaux** (ceux qui sont accessibles depuis le territoire français alors qu'ils n'ont pas bénéficié de l'agrément délivré par l'Autorité de régulation des jeux en ligne);

- **A la protection des auteurs**, s'agissant des sites contrefaisants.

Il s'agit également de sites dont les contenus dépassent la liberté d'expression, tels que les sites racistes ou révisionnistes[32].

- **A des sites au regard des produits et services qu'ils commercialisent** tels que notamment :

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

Plus généralement, des produits interdits ou réglementés.

 Le saviez-vous ?

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

3.2.3. RISQUES PARTICULIERS : EXEMPLE LES ETABLISSEMENTS SCOLAIRES

Si la lutte contre les atteintes aux droits de propriété intellectuelle sur Internet justifie la mise en œuvre d'outils de filtrage, il en est de même concernant la lutte contre les images et représentations illicites sur le réseau.

En effet, **l'article 227-23 du Code pénal incrimine** notamment **le fait d'offrir, ou de rendre disponible l'image ou la représentation d'un mineur présentant un caractère pornographique**.

Ce texte fait ressortir une nouvelle fois la nécessité d'un filtrage, faisant ainsi obstacle à l'accès aux images et représentations illicites.
Les fournisseurs d'accès, de services d'hébergement et les éditeurs de contenus sont ici encore incités à utiliser des dispositifs de filtrage et notamment le filtrage d'url afin de prévenir toute infraction à l'article 227-23 du Code pénal.

C'est d'ailleurs dans ce contexte de lutte contre l'accès à des contenus illicites que le Ministère de l'Education nationale a décidé de mettre en place des dispositifs de filtrage, notamment au sein des écoles, collèges, lycées, en élaborant un « guide pratique de mise en place du filtrage ».

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

C'est également sur ce même terrain que s'est placé le Forum des droits sur Internet qui a publié le 4 novembre 2008 la recommandation « Les enfants du Net III » encourageant l'utilisation de solutions de filtrage sur Internet.

Enfin, **l'article 4 de la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite LOPPSI 2**, qui vient de modifier l'article 6 I. 7° prévoit désormais que lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux FAI les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai.

3.3. QUI EST RESPONSABLE ?

3.3.1. LA RESPONSABILITE DE L'EMPLOYEUR

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.

Comme il a été indiqué, la responsabilité de l'employeur peut, sur le terrain de l'article 1384 aliéna 5, être engagée du fait des fautes commises par les salariés dans l'exercice de leurs fonctions.

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

La jurisprudence précise que la responsabilité du dirigeant peut être limitée si l'employé a agi[33] :

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

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

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

- **La Cour d'appel d'Aix en Provence** qui a rendu un arrêt retenant la responsabilité de l'employeur au motif principal que[34] :
  - « En ce qui concerne par contre la responsabilité de la société Lucent Technologies en sa qualité de commettant, il n'est pas contestable que Nicolas B. qui occupait les fonctions de technicien test dans une entreprise "dont l'activité est construction d'équipements et de systèmes de télécommunication" selon ses propres écritures, et dans lesquelles l'usage d'un ordinateur, et d'Internet, doit être quotidien, a agi dans le cadre de ses fonctions.

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

- 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.

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

Cette responsabilité pénale peut elle-même être appréhendée sous deux angles :

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

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

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

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

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

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

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

- **Soit l'infraction est commise et l'entreprise en est bénéficiaire** et alors la responsabilité de l'entreprise et de ses **dirigeants sera sans doute engagée**.

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

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

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

Ainsi si l'employeur a commis une « négligence caractérisée[35] », 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 de 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, et qu'il ne l'a pas fait, il 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 prend l'exemple **des 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.

  - 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 » ;

- De même, on peut faire référence à **l'article 227-24 du Code pénal** qui lui, **vise à empêcher que des mineurs puissent accéder à des messages à caractère violent ou pornographique ou de nature à porter gravement atteinte à leur dignité humaine** : une entreprise qui compterait parmi ses stagiaires des mineurs, s'exposerait aux risques d'infractions prévus à cet article, confirmant plus encore la nécessité de mise en œuvre de solutions de filtrage.

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

En résumé, que l'employeur soit tenu de manière exprès ou qu'il y soit vivement invité, selon le fameux principe de précaution, il est dans son intérêt aujourd'hui de mettre en œuvre et

[35] 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. ».

de déployer des mesures de contrôle d'accès à Internet et de loguer les actes de ses salariés sur Internet.

 Le saviez-vous ?

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

3.3.2. RESPONSABILITE DE L'UTILISATEUR

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

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

La Cour de Cassation[36] **dans deux arrêts distincts**, a qualifié de licenciement pour faute grave le licenciement de deux 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. En effet, le salarié avait envoyé des courriers à caractère pornographique depuis sa messagerie professionnelle. Or, la Cour de Cassation a rappelé que les courriers adressés par le salarié depuis sa messagerie professionnelle étant présumés avoir un caractère professionnel, l'employeur peut les ouvrir hors la présence du salarié, sauf si celui-ci les identifie comme étant personnels.

Par ailleurs, la Cour de Cassation a qualifié le licenciement d'un salarié ayant violé une interdiction posée par la charte informatique mise en place par l'entreprise et intégrée au règlement intérieur de licenciement pour faute grave justifiant le licenciement immédiat de l'intéressé. En effet, le salarié avait utilisé sa messagerie professionnelle pour la réception et l'envoi de documents à caractère pornographique et la conservation sur son disque dur d'un nombre conséquent de tels fichiers, à savoir 480, alors que la charte prohibe formellement la

[36] Cass. soc. 15-12-2010.

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.

Dernièrement, **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[37].


Le saviez-vous ?

L'utilisateur est responsable de ses actes … si l'entreprise est en mesure de l'identifier.

3.3.3. ROLE ET RESPONSABILITE DES ADMINISTRATEURS / DSI

3.3.3.1. Le rôle des administrateurs

Comme le précise la Cnil dans son « Guide pratique pour les employeurs et les salariés »[38], les administrateurs ont pour fonction d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Dans le cadre de leurs fonctions, ils peuvent être amenés à accéder à des informations personnelles concernant les utilisateurs (messagerie, historique des sites consultés, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…). D'après la Cnil, un tel accès n'est justifié que lorsque le bon fonctionnement des systèmes informatiques ne pourrait être assuré.

Selon la fiche pratique CNIL « Peut-on accéder à l'ordinateur d'un salarié en vacances »[39], 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.

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

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

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

Cependant, si un employé est absent, 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[40]. L'employeur ne doit cependant pas accéder aux contenus identifiés comme personnels par l'employé.

[37] CA Versailles 31-5-2011 Mickael P. c/ Mireille B.P.
[38] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2010.
[39] Fiche pratique CNIL « Peut-on accéder à l'ordinateur d'un salarié en vacances », 19 juillet 2010.
[40] Cass. 18-3-2003.

Tous les fichiers qui ne sont pas identifiés comme « personnel » sont réputés être professionnels de sorte que l'employeur peut y accéder hors la présence du salarié[41]. 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 appelé, ou en cas de risque ou évènement particulier. Le salarié ne peut s'opposer à un tel accès si ces conditions ont été respectées. »

S'agissant des données de connexions à internet, une jurisprudence a retenu qu'elles ne relevaient pas de la vie privée, mais étaient présumées professionnelles. L'employeur peut donc y avoir accès, en dehors de la présence du salarié[42].

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

3.3.3.2. 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[43] a confirmé le licenciement d'un administrateur qui avait téléchargé pendant ses heures de travail des fichiers piratés et contrefaits en utilisant le système, à des fins personnelles étrangères à l'activité de son employeur.

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

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

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

Les logiciels de prise en main à distance permettent aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique. 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[44], qu'une telle utilisation n'est pas conforme aux principes de proportionnalité et de finalité posés par la loi « Informatique et libertés ».

[41] Cass. 18-10-2006.
[42] 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 ».
[43] CA Paris 22e ch. C 4-10-2007 RG 03/12345.
[44] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2010.

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.

4. PLAN DE DEPLOIEMENT

4.1. ETAPE 1 : LE CHOIX DE LA SOLUTION

Une solution de filtrage pertinente doit être capable de proposer :

- Un **choix des catégories correspondant au droit pénal** du pays et segmentées en fonction **des centres d'intérêts** des utilisateurs ;
- Un **taux de reconnaissance** élevé (aptitude à reconnaître les sites demandés) ;
- Une **qualité du classement** pertinente (choix de la bonne catégorie).

4.1.1. LE BON CHOIX DES CATEGORIES

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 et répondant aux obligations légales et qui collecte des données non discriminatoires

4.1.2. L'IMPORTANCE DU TAUX DE RECONNAISSANCE

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

Il y a environ 200 millions de sites web dans le monde. Très vite 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 urls 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.

4.1.3. LA QUALITE DU CLASSEMENT : LES SITES DANS LES BONNES CATEGORIES

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

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

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

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

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

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

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

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

- Le droit « informatique et libertés » ;
- Le droit du travail.

4.2. ETAPE 2 : LE RESPECT DU DROIT INFORMATIQUE ET LIBERTES

4.2.1. LES PRINCIPES DE LA LOI INFORMATIQUE ET LIBERTES

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

En vertu **de l'article 2 alinéa 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 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 d'identifier les comportements de personnes physiques, les informations qu'ils comportent constituent bien des données à caractère personnel au sens de la loi.

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

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

4.2.2. LES DEMARCHES PREALABLES A METTRE EN OEUVRE

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 ;

4.2.2.1. 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[45] :

- 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 ;
- 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 Etat 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 :

- « 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 Etat 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 »[46].

Ces droits ont pour but « d'encourager la transparence dans l'exploitation des données à caractère personnel »[47].

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[48].

4.2.2.2. La déclaration Cnil

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

[45] Loi 78-17 du 6-1-1978, art.32.
[46] Loi 78-17 du 6-1-1978, art. 40.
[47] Alain Bensoussan, « Informatique, télécoms, internet » éd. 2008, n°1639.
[48] Loi 78-17 du 6-1-1978, art. 38.

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.** Lorsque ceux-ci ne relèvent pas des dispositions prévues aux articles 25, 26 et 27 de la loi relatifs aux demandes d'autorisation.

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.

Cette déclaration doit notamment préciser :

- La finalité du traitement ;
- Les données à caractère personnel traitées ;
- La ou les catégories de personnes concernées ;
- La durée de conservation des données établie, 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.

L'enregistrement de la déclaration auprès de la Cnil ne sera effectif qu'après réception du récépissé portant le numéro de déclaration. Dès réception de ce récépissé, le traitement peut être mis en œuvre.

Le saviez-vous ?

La déclaration normale à la CNIL ne fait que 4 pages.

En revanche, si l'entreprise dispose d'un correspondant informatique et libertés[49], elle se trouvera dispensée de la déclaration normale[50].

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

[49] Tel que le prévoit l'art. 22-III de la loi Informatique et libertés.
[50] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008 p. 18.

Si les données relatives aux employés sont anonymisées, il convient de préciser les modalités de cette anonymisation afin de déterminer si l'anonymisation des données est absolue, c'est à dire si les données ne sont plus nominatives directement (nom, prénom…) et indirectement (adresse mél, 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.

4.2.2.3. 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[51], le responsable d'un traitement de données à caractère personnel est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès. Des mesures de sécurité et de confidentialité adéquates devront donc être prises (mot de passe, sécurisation des accès physique et logique ainsi que des liaisons, …).

Les pouvoirs de la Cnil et les sanctions
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.

4.2.2.4. Le cas particulier du déchiffrement SSL

Au cas particulier où l'entreprise souhaite déchiffrer les flux encapsulés (https, ftps, …) dans un objectif de contrôle de contenu, il est nécessaire de recueillir l'accord individuel des collaborateurs. Une simple mention inscrite dans la charte internet serait insuffisante.

L'entreprise doit alors veiller à ce que seuls les flux des collaborateurs ayant donné leur accord seront déchiffrés. Pour les autres, elle pourra soit interdire l'accès soit l'autoriser mais sans déchiffrement.

4.2.3. 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 ses pouvoirs :

- La Cnil informe de leurs et obligations les personnes concernées par un traitement et les responsables de traitements en proposant notamment des guides, 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 ;

[51] Loi 78-17 du 6-1-1978, art.34.

- Elle dispose d'un pouvoir réglementaire pour encadrer ces traitements et peut élaborer des normes relatives à certains 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 envisage 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 conforme à la loi Informatique et libertés ;

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

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

4.2.4. 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 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 des infractions et peut conduire les tribunaux à prononcer des sanctions pénales.
La sanction encourue varie en fonction de l'obligation non respectée et peut être une contravention ou un délit. La peine maximale encourue est de 5 ans d'emprisonnement et 300 000 euros d'amende.

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

4.3. ETAPE 3 : LE RESPECT DU DROIT DU TRAVAIL

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

- Un outil de contrôle de l'activité des employés, et doit à ce titre être porté à leur connaissance[52] ;

- Une nouvelle technologie introduite au sein de l'entreprise, et doit en conséquence faire l'objet d'une consultation des institutions représentatives du personnel[53].

4.3.1. L'INFORMATION INDIVIDUELLE DES EMPLOYES

4.3.1.1. Simple « document » d'information et/ou charte Internet ?

Dès lors que l'outil de filtrage engendre la collecte des 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 moyens informatiques et de communications électroniques » ou « charte utilisateur ».

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

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.

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**[54] ou, à défaut, des délégués du personnel et à l'avis du comité d'hygiène, de sécurité et des conditions de travail[55].

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 simplifiée permet de mettre en place rapidement l'outil de filtrage, le document ainsi implémenté n'est pas opposable à l'employé en ce sens qu'il ne permet pas

[52] 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. »
[53] C. trav. art. L. 2323-13 al. 1.
[54] C. trav. art. L. 2323-13 al. 1.
[55] C. trav. art. L. 4612-8.

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 alors être suivie.

Eu égard à son objet, consistant notamment à poser des obligations générales et permanentes concernant les conditions d'utilisation des équipements de travail et à la sécurité au sein de l'entreprise, elle doit être considérée comme une adjonction au règlement intérieur[56], 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 :

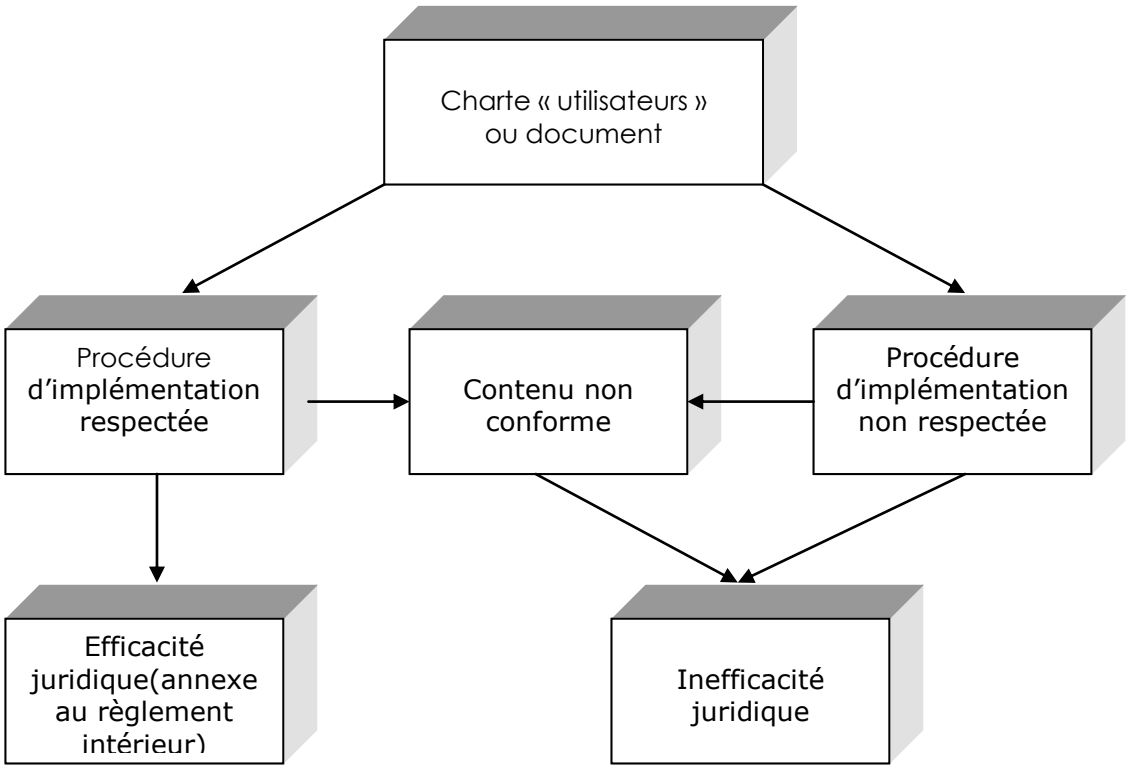
- La soumettre à l'avis du comité d'entreprise ou, à défaut, des délégués du personnel ainsi que, pour les matières relevant de sa compétence, à l'avis du comité d'hygiène, de sécurité et des conditions de travail[57] et au comité technique pour les établissements publics ;

- 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[58] ;

- La déposer au greffe du conseil de prud'hommes du ressort du siège social de l'entreprise, pour les personnes soumises au Code du travail[59] ;

- La transmettre à l'inspecteur du travail en deux exemplaires, pour les personnes soumises au Code du travail[60].

[56] C. trav. art. L. 1321-5.
[57] C. trav. art. L. 1321-4.
[58] C. trav. art. R. 1321-1.
[59] C. trav. art. R. 1321-2.
[60] 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 prestations** (exemple : contrat de sous-traitance sur place);

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

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

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

La procédure d'acceptation individuelle peut être :

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

Idéalement, il est conseillé de rédiger à coté de la « charte informatique » du système d'information applicable aux salariés/agents, une « charte des droits d'accès » pour les tiers de l'entreprise.

La charte des droits d'accès est un document quasi-identique à la charte informatique mais adaptée aux utilisateurs tiers de l'entreprise et qui prévoit notamment des sanctions adaptées pour cette catégorie d'utilisateurs en cas de non respect de la charte.

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

4.3.1.2. La particularité des chartes dans les administrations

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

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

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

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

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

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

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

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

- « Tout fonctionnaire, quel que soit son rang dans la hiérarchie, est responsable de l'exécution des tâches qui lui sont confiées. Il doit se conformer aux instructions de son supérieur hiérarchique, sauf dans le cas où l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public ;

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

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

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

- «Considérant que si, même dans le cas où les ministres ne tiennent d'aucune disposition législative un pouvoir réglementaire, il leur appartient, comme à tout chef de service, de prendre les mesures nécessaires au bon fonctionnement de l'administration placée sous leur autorité [...] dans la mesure où l'exige l'intérêt du service»[61].

L'acte réglementaire est un acte :

- Général ;
- Impersonnel ou non nominatif ;
- Visant une fonction, une institution, ou une situation[62]

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

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

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

Cependant, dans le cas où l'acte réglementaire affecterait les droits et obligations statutaires des fonctionnaires ou les prérogatives dont ils bénéficient de par leur appartenance à leur corps, il pourrait faire l'objet d'un recours pour excès de pouvoir « ouvert même sans texte contre tout acte administratif et qui a pour effet d'assurer, conformément aux principes généraux du droit, le respect de la légalité »[63]

La charte doit être adoptée après consultation du comité technique[64] et le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail[65]. 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, le défaut de consultation entacherait la charte d'illégalité.

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

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

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

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

[61] CE sec.7-2-1936 n° 433211 Jamart
[62] Jurisclasseur administratif, fascicule 106-10 Notion d'acte administratif n°10.
[63] CE sec. 17-2-1950 n° 86949 Dame Lamotte.
[64] Article 15 de la loi n°84-16 du 11 janvier 1984
[65] Article 16 de la loi n°84-16 du 11 janvier 1984

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[66].

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.

4.3.1.3. 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 du jeu sur un plan contractuel.

La charte administrateur est un complément indispensable à la charte des utilisateurs car si tout administrateur est un utilisateur, tous les utilisateurs ne sont pas des administrateurs ou dotés de droits d'administration.

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

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 Edition 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 :

- Un administrateur du réseau informatique pour la présence de fichiers en provenance d'Internet approchant les 6 GO d'images, de sons, de vidéos et de progiciels laissant présager un téléchargement 24h/24 et 7 jours/7 depuis le poste administrateur[67];

- 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[68].

[66] Jursiclasseur Administratif Fascicule 193 Agents non titulaires n°65
[67] CA Paris 22ème chambre, 4-10-2007.
[68] TGI Rennes 21-2-2008.

4.3.2. L'IMPLEMENTATION « COLLECTIVE »

Les institutions représentatives du personnel doivent également être consultées préalablement à l'introduction d'une nouvelle technologie que constitue un logiciel de filtrage[69].

Les membres du comité d'entreprise ou du comité technique et le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail dans les administrations 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[70].

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.

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

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

4.4.1. LE NIVEAU DE PARAMETRAGE ET LA QUALITE DES LISTES D'EXCLUSIONS

Sur la première problématique, il faut rappeler que la constitution de listes d'exclusions n'est pas un acte aussi anodin qu'il n'y paraît.
S'il est normal, voire obligatoire d'interdire l'accès à un certain nombre de contenus (pédopornographie, racisme, révisionnisme, contrefaçon …) certaines restrictions portent en elle l'essence même d'une discrimination.

Ainsi, créer des listes d'exclusion autour de thématiques telles que l'homosexualité pourrait être considéré comme attentatoire aux libertés les plus fondamentales des individus voire discriminatoires ou encore homophobes.

[69] C. trav. art. L. 2323-13 al. 1.
[70] C. trav. art. L. 2323-13 al. 2.

4.4.2. LE TRAITEMENT EGALITAIRE DES UTILISATEURS

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

4.4.3. LA CONSERVATION DES PREUVES

Sur la troisième problématique, il faut préciser que le droit de la preuve en matière pré-contentieuse 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 s'agissant des informations et données traitées à travers les outils de filtrage.

4.5. ETAPE 5 : LA GESTION DES LOGS

Il est difficile aujourd'hui de répondre précisément à la question de savoir si l'employeur doit conserver les données relatives à l'utilisation d'Internet par ses salariés.

Cette difficulté résulte en particulier de la combinaison des dispositions :

- **Du Code des postes et des communications électroniques, modifié par la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme** et portant disposition diverses relatives à la sécurité et aux contrôles frontaliers;

- **De l'article 6 de la loi pour la confiance dans l'économie numérique du 21 juin 2004** et son décret d'application du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

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-II[71] de la LCEN fait référence notamment aux « personnes dont l'activité est d'offrir un accès aux services de communication ».

[71] Renvoyant à la LCEN, art. 6 I. – 1°.

De son coté, **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, dans son alinéa 2.

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

Ces difficultés d'interprétation sont d'ailleurs accentuées par l'incertitude persistante quant au champ d'application desdits textes, et leur applicabilité aux employeurs.

Comme il a déjà été précisé, la question n'est en effet toujours pas tranchée s'agissant de la qualification possible de fournisseur d'accès d'un employeur donnant accès à internet à ses employés, comme le rappelle la jurisprudence[72].

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 service de communication électronique accessible au public ou de réseau public de communication 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** ;

- **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[73].

Aux termes du **décret n° 2011-219 relatif à la conservation et à la communication des données**, les FAI 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 FAI 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 FAI 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 :

[72] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005.
[73] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008 p. 18.

- 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 FAI et les fournisseurs d'hébergement doivent **conserver pendant un an** à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement, les informations suivantes:

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

4.6. ETAPE 6 : LE MAINTIEN EN CONDITIONS OPERATIONNELLES

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

5. DIMENSION INTERNATIONALE DU FILTRAGE

5.1. 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.

5.2. 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[74] 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. Les Espagnols souhaitent aussi adopter une loi pour lutter contre la contrefaçon sur internet telle que la loi Hadopi.

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'opération.

Aux Etats-Unis, vingt et un Etats 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 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[75] 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

[74] Ley 34/2002 de servicios de la sociedad de la informacion y de comercio.
[75] Cour Suprême des Etats Unis, « United States v. American Library Association », n° 02-361, 23-6-2003.

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.

Au Canada, il ne semble pas exister de règles particulières au niveau législatif relatives au filtrage. Néanmoins, la Corporation des bibliothécaires professionnels du Québec a adopté, au sein de son code de déontologie un article qui dispose « Si les téléressources 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[76], 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 »[77], 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[78] sont enregistrés par l'autorité australienne des communications et des médias[79], 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.

[76] Industry Containt Code of Practice.
[77] Internet Industry Association.
[78] Industry Containt Code of Practice.
[79] Australian Communication and Media Authority.

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.

La Grande Bretagne, ne semble pas avoir adopté de dispositions législatives propres au filtrage. Toutefois, l'adoption d'une loi récente[80], 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.

Par ailleurs, un guide[81] 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[82] travaillent d'ailleurs actuellement sur le développement de standards permettant d'évaluer et de tester l'efficacité des solutions de filtrage[83]. 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.xxx.

[80] Digital Economy Act.
[81] Social Networking Guidance.
[82] British Standards Institute.
[83] Pour plus d'information : http://police.homeoffice.gov.uk.

LES REGLES D'OR DU FILTRAGE

Le choix de la solution :
Elle doit être conforme à la législation du pays
Elle doit permettre un filtrage non discriminatoire dans le traitement des données à caractère personnel
Elle doit collecter les logs nominatifs en cas de réquisition judiciaire

La déclaration CNIL :
A partir du moment où l'outil collecte des données nominatives, il est nécessaire de déclarer cet outil à la Cnil. Il suffit pour cela de remplir la déclaration dite « normale » (4 pages) et la transmettre à la Cnil.

Ce n'est pas une obligation dans trois cas :

- Les employés sont anonymisés dans la solution, il n'y a pas de déclaration à effectuer.
- L'entreprise dispose d'un Correspondant Informatique et libertés (Cil), il n'y a pas de déclaration à effectuer.
- Le dispositif de filtrage ne permet pas un contrôle individuel du salarié, une déclaration dite « simplifiée » à la norme simplifiée n° 46 peut être effectuée

L'outil de filtrage peut être déployé dès la réception du récépissé de la Cnil.
La charte Internet n'est pas à être déclarée à la Cnil

La consultation des institutions représentatives du personnel :
Lors de l'introduction d'une nouvelle technologie les institutions représentatives du personnel doivent être consultées préalablement. L'introduction de cette nouvelle technologie est soumise à l'avis du comité d'entreprise ou comité technique pour les administrations. Un avis positif ou négatif sur la dite technologie n'est en aucun cas un obstacle au déploiement. Ce qui peut constituer un obstacle est l'absence d'avis.

L'information aux salariés :
Dès lors que l'entreprise collecte des données à caractère personnel, les salariés doivent être informés individuellement.
Dans une démarche simplifiée, un simple document d'information peut suffire si il présente la nouvelle technologie, les objectifs, les règles d'utilisations et la durée de conservation des données collectées. Cette démarche simplifiée permet de prendre le temps de rédiger une charte plus précise au vu de l'utilisation réelle d'Internet dans l'entreprise.

L'opposabilité juridique d'une charte :

- Une charte est juridiquement opposable aux salariés si :
- Elle est soumise à l'avis des du comité d'entreprise ou technique
- Elle est soumise à l'avis du comité d'hygiène, de sécurité et des conditions de travail
- Elle est diffusée individuellement et collectivement
- Elle est déposée au greffe du conseil de prud'hommes, pour les personnes soumises au Code du travail
- Elle est transmise à l'inspection du travail en deux exemplaires, pour les personnes soumises au Code du travail

La preuve :
En cas de litige il convient de conserver la preuve en trois exemplaires : une pour l'huissier (copie non manipulée), une pour l'entreprise, une pour l'accusé.

Les logs :
La conservation des données de connexion des salariés par l'entreprise permet à l'entreprise de se préconstituer une preuve en cas de litige avec les salariés.

6. A PROPOS D'OLFEO

La solution Olfeo permet de sécuriser, d'optimiser et d'analyser l'ensemble de la sécurité Internet à travers 5 produits complémentaires :

- Proxy cache Qos
- Filtrage d'url
- Filtrage protocolaire
- Antivirus de flux
- Portail public

Elle dispose d'une architecture technique exclusive lui assurant de très hautes performances et une grande richesse fonctionnelle.

Olfeo renouvelle l'offre proxy et de filtrage de contenus grâce à une approche innovante basée sur la proximité culturelle, le respect fidèle au contexte juridique local et l'association des utilisateurs à la politique de sécurité.

La stratégie d'innovation d'Olfeo a été plébiscitée par plus de 1.000 clients satisfaits et fidèles. Plus de 96% des clients Olfeo reconduisent leur contrat.

Olfeo a construit une solution spécifiquement pour le marché français, elle offre ainsi des avantages uniques :

- Une protection juridique optimale,
- Une très grande facilité de création des politiques de filtrage grâce à la conformité des catégories aux habitudes de surf
- Un taux de reconnaissance des sites visités de plus de 98%
- Une qualité de filtrage inégalé grâce au classement manuel
- L'association des utilisateurs à votre politique de sécurité

Pour en savoir plus : www.olfeo.com