Livre blanc juridique Olfeo

Co-écrit avec le cabinet d'avocats Alain Bensoussan

Olfeo

Filtrage et Internet au bureau : Enjeux et cadre juridique !

SOMMAIRE

Préface

« Face aux solutions de filtrage d'url, deux questions se posent aujourd'hui à l'employeur : est-il légitime de mettre en place de telles solutions ? Comment les mettre en œuvre conformément au droit, le cas échéant ?

A la première question, on peut répondre en premier lieu qu'il est désormais établi que la responsabilité de l'employeur, public ou privé, peut être engagée du fait de l'utilisation par ses collaborateurs notamment de ses accès internet.
Il existe en effet plusieurs dispositions légales qui imposent à l'employeur de prendre des mesures pour empêcher les accès illicites au sein de son établissement. Il paraît donc essentiel pour lui de vérifier les conditions d'utilisation de ses outils.

La jurisprudence la plus récente conforte d'ailleurs cette possibilité, en légitimant la mise en œuvre d'un contrôle des connexions internet.

Dès lors, la problématique qui se pose à l'employeur est celle annoncée à la seconde question : il s'agit d'une problématique de déploiement, en conformité avec le droit. La mise en œuvre de la solution de filtrage d'url doit respecter trois axes : le droit du travail, le droit Informatique et libertés et assurer une gestion adéquate de la preuve.

L'objet de ce livre blanc est de présenter notamment ces modalités de mise en œuvre sous un aspect à la fois juridique et pédagogique ».

Eric BARBRY, *Avocat au Barreau de Paris*
Directeur du Pôle « Droit du numérique » du cabinet Alain Bensoussan

A Les aspects juridiques du filtrage

Le droit des filtres est une réalité juridique qui comporte plusieurs facettes. Il est ainsi constitué :

- De textes législatifs ou réglementaires, voire d'ordre communautaire relatifs à l'usage des filtres ;
- De recommandations ou rapports élaborés par des autorités compétentes ou par des instances représentatives (Cnil, Forum des droits sur Internet…);
- D'un ensemble de jurisprudences, qui imposent des techniques de contrôle d'accès à Internet.

A.1 Le droit de filtrer

Le terme de « filtre » ou de « filtrage », particulièrement le filtrage d'url n'est pas inconnu des textes et jurisprudences actuels.

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

- **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 » ;

- **Un certain nombre de documents** réalisés par la Commission Nationale Informatique et Libertés, 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, ou plus récemment, en 2008, le Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008 dont la Fiche n°6 porte sur le « Contrôle de l'utilisation d'Internet et de la messagerie ».

Au-delà des mots « filtre » et « filtrage », il existe d'autres textes qui visent à travers des terminologies différentes un même objet : celui qui consiste à restreindre ou contrôler les accès à des sites web sur Internet.

- **Ainsi l'article 6 I.– 1° de la loi n°2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique (« LCEN ») ne retient pas le terme de filtre mais, évoquant cette même réalité technique, utilise celui de *« moyens techniques permettant de restreindre l'accès à certains services de communication au public en ligne ou d'opérer une sélection de ces services »*[1] ;

- **De même que l'article L. 335-12 du Code de la propriété intellectuelle** utilise les termes *« moyens de sécurisation »*, à défaut de faire référence aux « filtres » ou au « filtrage »[2] ;

[1] 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 ».

[2] 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'oeuvres 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 projet de loi favorisant la diffusion et la protection de la création sur internet également appelée « loi Hadopi ».**

Le droit communautaire reconnaît également 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'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux. Le considérant n°5[1] met en avant le fait que les outils de filtrage constituent des éléments essentiels pour assurer un environnent plus sûr sur Internet.

A.2 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.

Il apparaît que ce droit existe bien au travers des terminologies différentes du mot log ou loguer comme :

- La « donnée relative au trafic »[2] ;
- Les « données de connexion à des services de communications électroniques »[3] ou « données de connexion »[4] ;
- Les « fichiers logs ou de journalisation »[5].

Il semblerait également que la jurisprudence reconnaisse le droit de loguer :

Dans un arrêt du 9 juillet 2008, la Cour de Cassation[6] 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 décision présente une avancée jurisprudentielle essentielle, et s'inscrit 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

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

[2] 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.

[3] CPCE art. L. 34-1-1, encadrant en particulier la communication des données de connexion afin de prévenir les actes de terrorisme.
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.

[4] Fiches de synthèse « Cybersurveillance sur les lieux de travail » du 11-2-2002 de la Cnil.

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

[6] 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 ».

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).

A.3 La position de la Cnil et du forum des droits sur Internet

A.3.a CNIL et filtrage

La Cnil est sensible à la mise en place de solutions de filtrage au sein des entreprises[1].

La Cnil considère en effet que s'il n'est pas possible d'interdire « de manière générale et absolue » l'utilisation d'Internet à des fins non professionnels, en se référant notamment au contexte de développement des moyens de communication ainsi qu'au contexte jurisprudentiel actuel, rien n'empêche l'employeur de limiter notamment l'accès de ses employés à Internet.

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

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

Selon la Commission, l'employeur peut imposer certaines mesures dans l'utilisation des systèmes d'information, justifiées par 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.

La Cnil rappelle que les modalités de base de contrôle de l'usage d'Internet, et donc de mise en œuvre d'une solution de filtrage supposent également d'un point de vue pratique :

- **La consultation du comité d'entreprise**[2] ou dans la fonction publique du comité technique paritaire notamment ;

- **La mise en place d'une déclaration auprès de la Cnil**, dès lors que le dispositif de filtrage permet un contrôle individuel, en précisant :

    - La durée de conservation des données établies, étant précisé que la Cnil considère qu'une durée de conservation de six mois paraîtrait suffisante dans la plupart des cas ;

    - Ainsi que l'indication de la date à laquelle les instances représentatives du personnel ont été consultées sur la mise en place des outils de filtrage.

Les exigences pratiques ainsi exposées correspondent à la mise en œuvre de cinq principes « généraux » posés par la Cnil, pour la mise en place d'un traitement de données à caractère personnel :

- **Le principe de finalité**, exigeant que le traitement de données à caractère personnel soit réalisé pour un usage déterminé et légitime ;

[1] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008 p. 18.
Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition mars 2004, p. 12.
[2] C. trav. art. L. 2323-32.

- **Le principe de proportionnalité**, faisant référence au principe selon lequel « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché » [1] ;

- **Le principe de transparence, lié au respect des droits des personnes, afin d'assurer la plus grande transparence à l'égard des intéressés ;** ce principe exige une information préalable de l'employé et fait écho au droit du travail rappelant que « aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance»[2] ;

- **Le principe d'une durée limitée** de conservation des données, qui doit être définie par rapport à la finalité du fichier ;

- **Le principe de sécurité** et de confidentialité des données qui prévoit une obligation de sécurité des données à caractère personnel. Seules les personnes habilitées doivent pouvoir consulter ces données, dans le but d'en garantir la confidentialité. Ainsi, les administrateurs réseaux sont en mesure de consulter les données de connexion à Internet ;

Ces principes s'inscrivent dans le cadre :

- D'un souci de transparence qui inspirait la loi Informatique et libertés et qui correspond à une exigence de loyauté dans la collecte des données ;
- D'une démarche de discussion collective, dans la ligne droite de l'exigence de transparence.

A.3.b Forum des Droits sur Internet et filtrage

De son côté, le Forum des Droits sur Internet recommande la mise en place de dispositifs de filtrage par les fournisseurs d'accès à Internet visant les sites pédopornographiques[3]. Il envisage de mettre en place une liste des sites contenant des images ou des représentations d'abus sexuels sur les mineurs, qui serait transmise aux fournisseurs d'accès à Internet.

Ces derniers assureraient alors le blocage des sites listés.

A.4 L'état de la jurisprudence

La 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.

Il est possible de relever la jurisprudence « clé » en matière de filtrage[4], en matière de :

- Données de connexions, qui sont présumées professionnelles permettant le contrôle des salariés[5] ;

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

[1] C. trav. art. L. 1121-1.
[2] C. trav. art. L. 1222-4.
[3] Le Forum des droits sur Internet, Recommandation « Les enfants du Net III, conditions nécessaires à la mise en place du filtrage des sites pédopornographiques par les FAI ».
[4] Pour un exposé plus complet de la jurisprudence en matière de filtrage se reporter à l'annexe « tableau d'analyse de la jurisprudence en matière de filtrage »
[5] Cass. soc. 9-7-2008 retenant que les connexions à Internet sont présumées professionnelles.

- Vente de parfums Christian Dior en dehors du leur réseau de distribution sélective ;

- Diffusion de pages à contenus racistes ;

- Diffusion de propos négationnistes.

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, toutes les fois que s'est posée la question de mettre en place des mécanismes faisant obstacle à la consultation des sites illicites.

Dans ce contexte, il a généralement été question d'interpréter **l'article 6-I 8° de la loi pour la confiance dans l'économie numérique**, qui autorise l'autorité judiciaire à prescrire, en référé ou sur requêtes, toutes les 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.

Le débat judiciaire s'est souvent cristallisé autour de la question de l'efficacité des mesures de filtrage et à la nature de l'obligation incombant au prestataire technique à savoir : une obligation de résultat ou une obligation de moyens.
Les tribunaux considèrent en général que cette obligation de filtrage incombant au prestataire technique relève d'une obligation de moyens.
Les tribunaux prennent généralement en compte l'état actuel de la technique, c'est-à-dire l'état de l'art pour apprécier l'efficacité des mesures de filtrage mises en œuvre par les prestataires techniques.

A.5 Les usages

Au sens large, la notion de « droit » ne se limite pas aux seules dispositions législatives ou réglementaires et à la seule jurisprudence, mais cette notion tient compte également des « usages » et des réflexions doctrinales.
Les usages s'entendent de la manière dont les acteurs économiques pratiquent le filtrage. Les réflexions doctrinales s'entendent des publications, conférences ou séminaires à caractère juridique qui portent sur la problématique du filtrage.
Force est de constater que s'agissant des usages, un très grand nombre d'entreprises a décidé de se doter d'outils de filtrage. S'agissant des réflexions doctrinales, il existe aujourd'hui un certain nombre de publications ou de manifestations à caractère juridique qui témoignent de l'importance pour les acteurs économiques de mettre en œuvre des solutions de filtrage d'url.[1]

[1] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008.
Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition mars 2004.

B Ne pas filtrer : un risque juridique

Ce risque juridique se distingue lui-même en trois niveaux :

- Un premier niveau de risque entoure les sites présentant un caractère illicite ;
- Un deuxième niveau existe lorsque des entreprises sont légalement tenues de mettre en œuvre des outils de contrôle d'accès à Internet et décident de ne pas satisfaire à cette obligation légale ;
- Un troisième niveau de risque juridique est lié tout particulièrement à la responsabilité du chef d'entreprise face aux agissements de ses préposés.

B.1 Les catégories de sites présentant un caractère illicite en France

Il existe deux types de sites web illicites :

- Les sites illicites en raison de leurs contenus ;
- Les sites illicites du fait des produits et services qu'ils commercialisent.

S'agissant de la première catégorie de sites web, il s'agit de sites dédiés à des 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 [1];
- Aux monopoles, par exemple en matière de jeux de hasard ;
- 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.

Pour ce qui concerne la seconde catégorie de sites web, il s'agit de la mise à disposition, de la vente, de la location de produits 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.

[1] 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.

B.2 Les personnes tenues de filtrer selon la loi

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.

B.2.a Les fournisseurs d'accès

L'obligation légale la plus exemplaire dans ce domaine correspond à celle qui pèse sur les fournisseurs d'accès à Internet à travers **l'article 6 I. – 1° de la LCEN.**

> 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.

La question se pose alors de savoir ce qu'est un fournisseur d'accès à Internet, et donc de déterminer qui est finalement tenu à cette obligation de mise à disposition d'outils de restriction d'accès.

B.2.b Les entreprises sont-elles dans l'obligation de filtrer ?

A priori, la LCEN vise les fournisseurs d'accès au sens premier du terme, puisque l'article 6 dont il est question s'inscrit dans le chapitre 2 de la loi, intitulé «les prestataires techniques ».

Il existe cependant un double doute quant au fait de considérer que seuls les fournisseurs d'accès au sens premier du terme, c'est-à-dire ceux qui sont déclarés auprès de l'ARCEP, se trouvent tenus à cette obligation.

- **Le premier doute est constitué par les dispositions de l'article de L. 34-1 du Code des postes et communications électroniques** :

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

De fait, cet article élargi de manière considérable la notion même d'opérateur de communications électroniques.

Il est donc possible de soutenir que les obligations visant à mettre à disposition des outils de restriction d'accès ne sont pas limitées aux seuls fournisseurs d'accès au sens technique du terme, mais à toute personne qui permettrait au public une connexion à Internet (espace d'accès libre à Internet, point d'information public, accès dans des espaces de manifestions publiques : salons, hôtels, cybercafés).

- **Le second doute provient de l'arrêt de la Cour d'appel de Paris du 4 février 2005**[1] qui 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, qui est de mettre à disposition des outils de filtrage et d'informer les utilisateurs.

A côté des textes législatifs ou réglementaires déjà adoptés, il convient de tenir compte de certains projets ou propositions de loi.

- **A ce jour, est débattu devant le parlement le projet de loi favorisant la diffusion et la protection de la création sur Internet.**

Ce texte dans sa première version prévoyait une modification de l'article L. 336-2 du Code de la propriété intellectuelle.

Cette modification avait pour objet de permettre au juge des référés de prendre notamment « toute mesure de suspension ou de filtrage des contenus » ou « toute mesure de restriction de l'accès à ces contenus », en cas d'atteinte aux droits d'auteurs ou droits voisins.

Le projet de loi, tel qu'adopté par le Sénat en première lecture le 30 octobre 2008 a maintenu cette possibilité pour le juge, utilisant une formulation plus large correspondant à la possibilité pour ce dernier de prendre « toutes mesures propres à prévenir ou à faire cesser » une telle atteinte, incluant donc les mesures de filtrage ; de telles mesures étant prises à l'encontre de « toute personne susceptible de contribuer à (…) remédier » à l'atteinte aux droits d'auteurs et aux droits voisins. Ces dispositions visent ainsi tous les prestataires : éditeur, hébergeur, fournisseur d'accès à Internet.

Le projet de loi tel qu'adopté en première lecture par le Sénat retient également que la Haute Autorité (« Hadopi ») qu'il créé a pour mission « d'évalue(r) les expérimentations conduites par les professionnels concernés dans le domaine des technologies de reconnaissance des contenus et de filtrage » et de « rendre compte des principales évolutions constatées dans ce domaine ».

Lors de sa première lecture devant l'Assemblée nationale, le 2 avril 2009 le texte adopté par le Sénat a été modifié par les députés. En particulier, les modifications de l'article L.336-2 du Code de la propriété intellectuelle n'ont pas été maintenues.

Même si ce projet de loi présente de nombreuses difficultés, s'agissant de son adoption[2], il n'en reste pas moins qu'il témoigne de la volonté législative de protéger les auteurs s'interrogeant sur la possibilité de développer des dispositifs de filtrage.

B.2.c Le titulaire de l'accès

Cette obligation de filtrer pour l'abonné est d'ailleurs consacrée en matière de propriété intellectuelle par l'article L. 335-12 du Code de la propriété intellectuelle. Cet article impose à l'abonné - aussi bien entreprise que particulier - de veiller à ce que son accès ne soit pas utilisé à des fins de reproduction ou de représentation d'œuvres de l'esprit,

[1] « 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. »

[2] Le texte finalement retenu par la Commission mixte paritaire le 7 avril 2009 a été rejeté par l'assemblée nationale le 9 avril 2009.

sans l'autorisation des titulaires des droits d'auteurs. En d'autres termes, l'abonné doit s'assurer que son accès à Internet n'est pas utilisé en particulier à des fins de contrefaçon, tel que le téléchargement illicite.

Pour ce faire, le Code de la propriété intellectuelle prévoit la mise en oeuvre de « moyens de sécurisation » qui lui sont proposés par son fournisseur d'accès à Internet.

B.2.d Les établissements 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 ».

C'est également sur ce même terrain que s'est récemment 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.

B.3 La responsabilité de l'employeur

B.3.a Responsabilité civile

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.

Cette question est posée, indépendamment des problématiques étudiées ci-avant relatives aux champs d'application de l'article 6 de la LCEN, et provient des dispositions juridiques civiles et pénales relatives à la responsabilité de l'employeur.

Le débat porte essentiellement sur le niveau de responsabilité de l'employeur face à un usage illicite de l'Internet par ses employés.

Cette responsabilité est spécifiquement organisée à travers l'article 1384 alinéa 5 du Code civil :

L'article **1384 alinéa 5 du Code civil**, qui 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 »

Cet article pose donc le principe d'une possible responsabilité de l'employeur concernant les agissements de ses employés en général, et donc sur Internet.

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

Cette jurisprudence précise que la responsabilité du dirigeant peut être limitée si l'employé a agi[1] :

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

Récemment la **Cour d'appel d'Aix en Provence** a rendu un arrêt retenant la responsabilité de l'employeur au motif principal que[2] :

> « 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*.
>
> 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 quelle que soit le débat résiduel qui demeure quant à la fiabilité totale des solutions disponibles.

B.3.b Responsabilité pénale

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

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

La réponse est loin d'être simple et trouve un de ses fondements à l'article **121-1 du Code pénal :**

L'article **121-1 du Code pénal** 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** :

L'article **121-2 du Code pénal** dispose que :

« 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.) : la réponse dépend essentiellement des obligations légales posées par le législateur.

- Si l'on se réfère à **l'article L. 335-12 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 de l'obligation de mettre en œuvre les outils de restriction d'accès qui lui sont proposés permettant d'éviter les actes de contrefaçon.

- Si l'on prend l'exemple des dispositions pénales de lutte contre la pédophilie :

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. »

Les termes « *le fait d'offrir ou de rendre disponible* » laisse à penser que la responsabilité de l'employeur pourrait être recherchée du fait que ses employés pourraient accéder à de tels contenus.

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 de déployer des mesures de contrôle d'accès à Internet.

B.4 Responsabilité 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** :

> Les articles **1382 et 1383 du Code civil** disposent que :
>
> « 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 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.

B.5 Responsabilité des administrateurs / DSI

B.5.a Le rôle des administrateurs

Comme le précise la Cnil dans son « Guide pratique pour les employeurs et les salariés »[1], 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.

Les administrateurs sont en outre soumis à une obligation de confidentialité. Ils ne doivent donc pas communiquer les informations dont ils auraient eu connaissance dans le cadre de leurs fonctions.

En particulier, ils ne peuvent révéler les informations entrant dans le champ du secret des correspondances et de la vie privée des utilisateurs, dès lors que de telles informations ne portent atteinte :

- Ni au bon fonctionnement technique des applications ;
- Ni à la sécurité ;
- Ni à l'intérêt de l'entreprise.

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

S'agissant des données de connexions à internet, une jurisprudence récente 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[2].

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.

B.5.b Les responsabilités du personnel informatique

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.

Il en est notamment ainsi dans la décision de la **Cour d'appel de Paris du 4 octobre 2007**[3], qui 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 :

---

[1] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008.

[2] 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 ».

[3] CA Paris 22e ch. C 4-10-2007 RG 03/12345.

- **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.

B.6 Le droit applicable

Tout employé ayant accès aux sites interdits par la loi française, même si l'entreprise est étrangère, engage en plus de sa responsabilité pénale, celle de l'entreprise et de ses dirigeants selon l'article L 113-2 du code pénal.

> **L'article L 113-2 du code pénal** dispose :
>
> 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.

La pratique actuelle d'internet fait ressortir que de plus en plus de contenus sont hébergés à l'étranger.

Cette tendance ne doit pas faire oublier qu'un hébergement à l'étranger ne fait pas obstacle à l'application du droit français, dès lors que les contenus sont accessibles en France. Ce principe est désormais bien établi, depuis les jurisprudences « UEJF c/ Yahoo ! Inc. et a. »[1].

Ce principe se trouve par ailleurs confirmé par la jurisprudence récente du tribunal de grande instance de Paris[2] du 7 janvier 2009, qui a considéré que l'exploitation matérielle du site www.google.fr en Irlande ne faisait pas obstacle à l'engagement de la responsabilité de la société Google France. Le tribunal a en effet considéré que la société française était « la seule société du groupe a intervenir légalement en France et qui est celle qui apparaît et se comporte comme responsable sur ce territoire de l'activité publicitaire du site internet portant le même nom Google France. »

[1] Pour un exposé plus complet de la jurisprudence en matière de filtrage se reporter à l'annexe « tableau d'analyse de la jurisprudence en matière de filtrage »

[2] TGI Paris 3e ch. 3e sect. 7-1-2009.

C Plan de déploiement

C.1 Etape 1 : Le choix de la solution

Une solution de filtrage pertinente doit être capable :

- Le choix des catégories : elles doivent correspondre au droit pénal du pays et être segmentées en fonction des centres d'intérêts des utilisateurs ;
- Le taux de reconnaissance : l'aptitude à reconnaître les sites demandés ;
- La qualité du classement : le choix de la bonne catégorie.

C.1.a Le bon choix des catégories

Les 3 principaux moteurs d'acquisition d'une solution de filtrage sont :

- Le risque pénal ;
- La chute de productivité ;
- La bande passante.

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. Il faut pour cela que la solution de filtrage d'url propose des catégories qui permettent d'exclure précisément les sites illicites. De même il est indispensable que celles-ci les centres d'intérêts extraprofessionnels des internautes.

C.1.b L'importance du taux reconnaissance

La taille de la base de données d'url 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'entreprise, cette base ne sera pas pertinente quelque soit sa taille.

Plutôt que la taille, il faut donc préférer le taux de reconnaissance. Le taux de reconnaissance se définit comme la proportion des sites demandés par l'utilisateur qui seront effectivement reconnus par le filtre. 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.

Ainsi, 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.

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.

C.1.c La qualité du classement : les sites dans les bonnes catégories

Le troisième critère d'évaluation est la qualité de classement. 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).

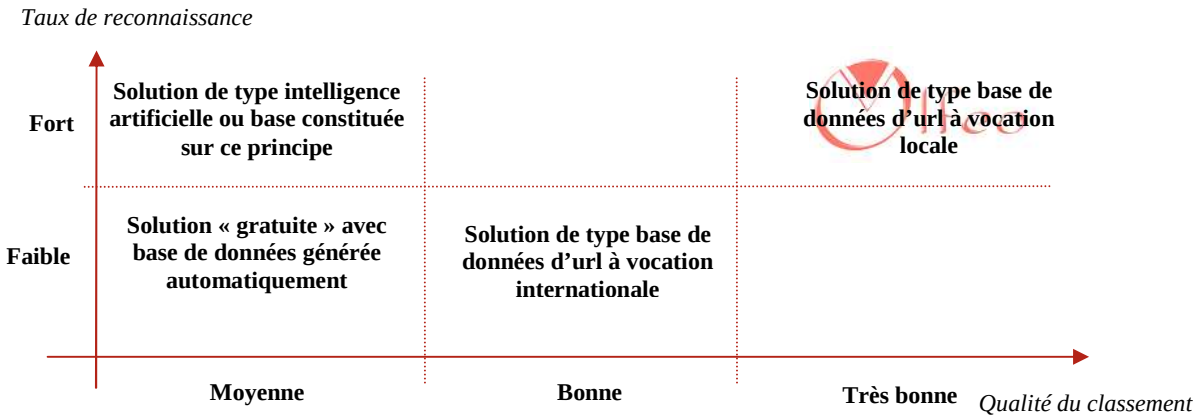
L'appréciation de l'appartenance d'un site à une catégorie plutôt qu'à une autre nécessite :

- **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.
Les solutions fonctionnant sur le principe de l'intelligence artificielle offrent quant à elles un très bon taux de reconnaissance puisqu'elles n'ont pas de base de données et qualifient les sites 'à la volée' mais leur qualité de classement est très lointaine des solutions ayant choisi une qualification manuelle ou semi manuelle. Par ailleurs, elles ne reconnaissent que les sites en langues européennes qui sont loin de représenter les principales menaces.

C.1.d Le panorama des solutions de filtrage

Le graphique, ci-dessous, permet de classer les solutions par type selon les deux principaux critères d'analyse de la qualité :



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.

C.2 Etape 2 : Le respect obligatoire du droit informatique et liberté

C.2.a La loi informatique et liberté et filtrage

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

On entend par traitement de données à caractère personnel[1] : « 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 ».

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.

La loi informatique et liberté impose à toute personne qui souhaite déployer un tel traitement diverses obligations dont les principales sont :

- Les démarches préalables ;
- Le droit des personnes ;
- La sécurité du système et des données qu'il comporte.

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

C.2.b Les démarches préalables à mettre en œuvre : déclaration CNIL

On peut s'interroger sur le type de démarches préalables à mettre en œuvre étant précisé qu'il existe, s'agissant de la gestion du personnel, une norme simplifiée n°46 qui permet de procéder à une déclaration simplifiée auprès de la Cnil, des outils informatiques liés à la gestion des personnels.

Cependant, cette norme exclue expressément des outils permettant le contrôle individuel d'activité des employés et d'une manière générale la mise en œuvre de mesures de cybersurveillance.
Par conséquent la norme simplifiée n° 46 peut suffire, à la condition que le filtrage mis en place n'entraîne pas un contrôle individuel des salariés. Dans ce cas la conservation des logs ne peut se faire par l'outil de filtrage mis en place.

Autrement, il convient, en l'état actuel du droit, de privilégier la réalisation d'une déclaration normale auprès de la Cnil, l'exercice n'étant d'ailleurs pas bien plus compliqué qu'une déclaration simplifiée.

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. En revanche, si l'entreprise dispose d'un correspondant informatique et libertés[2], elle se trouvera dispensée de la déclaration normale[1].

[1] Art. 2 de la loi Informatique et libertés
[2] Tel que le prévoit l'art. 22-III de la loi Informatique et libertés.

C.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[2] ;

- Une nouvelle technologie introduite au sein de l'entreprise, et doit en conséquence faire l'objet d'une consultation des institutions représentatives du personnel[3].

C.3.a L'information individuelle des employés

C.3.a.i 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 a 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 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;

- 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[4] ou, à défaut, des délégués du personnel et à l'avis du comité d'hygiène, de sécurité et des conditions de travail[5] .

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 d'url.

---

[1] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008 p. 18.
[2] C. trav. art. L. 1222-4.
[3] C. trav. art. L. 2323-13 al. 1.
[4] C. trav. art. L. 2323-13 al. 1.
[5] C. trav. art. L. 4612-8.

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

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[1], 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 :

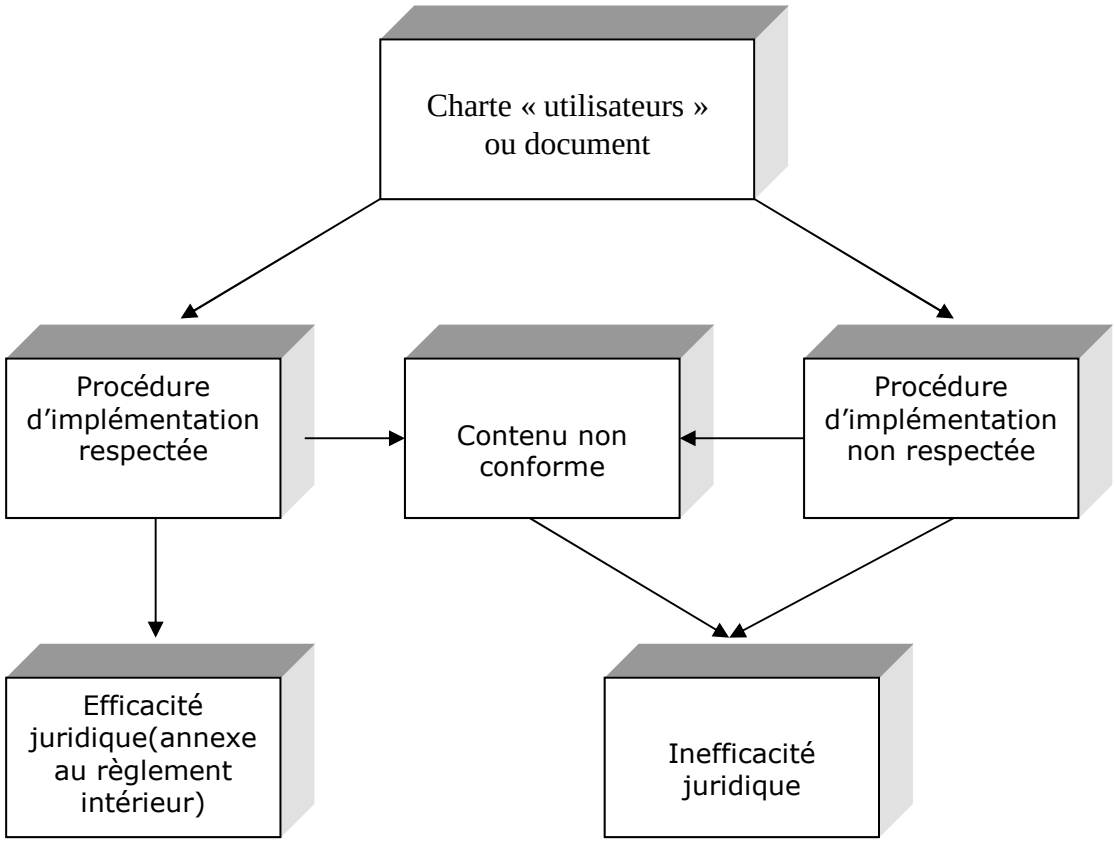
- La soumettre à l'avis du comité d'entreprise ou, à défaut, des délégués du personnel ainsi que, pour les matières relevant de sa compétence, ainsi qu'à l'avis du comité d'hygiène, de sécurité et des conditions de travail[2] et au comité technique paritaire pour les établissements publics, étant précisé qu'un avis négatif ne fait pas obstacle à l'implémentation de la charte ;

- 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[3] ;

- La déposer au greffe du conseil de prud'hommes du ressort du siège social de l'entreprise[4] ;

- La transmettre à l'inspecteur du travail en deux exemplaires[5].

[1] C. trav. art. L. 1321-5.
[2] C. trav. art. L. 1321-4.
[3] C. trav. art. R. 1321-1.
[4] C. trav. art. R. 1321-2.
[5] C. trav. art. R. 1321-4.



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.

C.3.a.ii La particularité du personnel informatique

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

Cette charte a vocation à définir les droits et obligations des administrateurs et comporte nécessairement une disposition spécifique s'agissant des outils de filtrage.

C.3.b L'implémentation « collective »

Dans un second temps, les institutions représentatives du personnel doivent être consultées préalablement à l'introduction d'une nouvelle technologie, que constitue un logiciel de filtrage[1].

Les membres du comité d'entreprise 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[2].

Il convient de préciser qu'un avis négatif du comité d'entreprise ne lie pas l'employeur, et ne l'empêche pas de mettre en place une nouvelle technologie au sein de son entreprise.

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

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.

C.4 Etape 4 : L'administration et paramétrage de la solution

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

Plusieurs autres zones de risque juridique sont ici à traiter :

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

C.4.a Le niveau de paramétrage et la qualité 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 pire encore homophobes.

C.4.b Le traitement égalitaire des utilisateurs

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

C.4.c 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.

C.5 Etape 5 : La Gestion des logs

La question des modalités de gestion des logs est une délicate question, à laquelle le droit apporte peu de réponses.

Ces difficultés résultent en particulier de la combinaison des dispositions :

- Du Code des postes et des télécommunications ;
- Et de l'article 6 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 - dont le décret d'application n'a à ce jour pas été pris-,

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

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 posées 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 l'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[2].

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 minimal de six mois, et un durée maximale de deux ans ;
- Le projet de décret 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 2 une durée d'un an à compter du jour de la création des contenus ;

[1] Renvoyant à la LCEN, art. 6 I. – 1°.
[2] CA Paris 14ème ch. BNP Paribas c/ Société World Press Online 4-2-2005.

- 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 faite par ses employés de l'utilisation d'internet[1].

C.6 Etape 6 : Le maintien en conditions opérationnelles

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

[1] Guide pratique de la Cnil « pour les employeurs et les salariés », édition 2008 p. 18.

D Dimension internationale du filtrage

D.1 La nécessité de respecter la réglementation 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.

D.2 La nécessité de filtrer : une prise de conscience internationale

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

En Espagne, l'article 12bis 3° de la loi n° 34/202 relative aux services de la société de l'information et du commerce électronique[1] 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.

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.
La jurisprudence américaine a, par ailleurs, jugé dans un arrêt de la Cour Suprême[2] 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 filtrages 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 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[3], 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 »[4], 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[5] sont enregistrés par

[1] Ley 34/2002 de servicios de la sociedad de la informacion y de comercio.
[2] Cour Suprême des Etats Unis, « United States v. American Library Association », n° 02-361, 23-6-2003.
[3] Industry Containt Code of Practice.
[4] Internet Industry Association.
[5] Industry Containt Code of Practice.

l'autorité australienne des communications et des médias[1], 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.

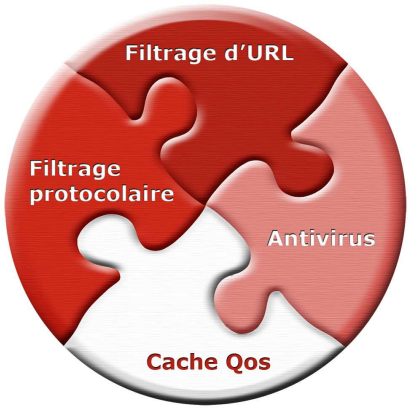
En Grande Bretagne, un guide[2] a été élaboré notamment par le Ministère de l'intérieur en collaboration avec de nombreux fournisseurs de services sur Internet afin d'assurer une plus grande sécurité du réseau pour les mineurs. Ce guide propose notamment comme objectif la mise en place d'un système de 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[3] travaillent d'ailleurs actuellement sur le développement de standards permettant d'évaluer et de tester l'efficacité des solutions de filtrage[4]. Ces travaux déboucheront peut-être sur la même démarche de « labellisation » des logiciels, comme en Australie.

E A propos d'Olfeo

Olfeo est éditeur de la première passerelle française de sécurité Internet.
Olfeo s'adresse aux entreprises et aux administrations françaises de toutes tailles, avec une offre basée sur le comportement des internautes français et les nouveaux modes de consommation d'Internet, le droit pénal applicable et le droit social lié à la régulation de l'utilisation d'Internet.

Olfeo a construit sa passerelle autour de 4 briques complémentaires :

- Le **filtrage d'url** afin de réguler l'utilisation d'Internet,
- Le **filtrage protocolaire** afin d'interdire les flux indésirables qui ne sont pas bloquer par le filtrage d'url : Peer To Peer, Messagerie instantanée, VoIp, etc …
- **L'antivirus de passerelle** afin de stopper en temps réel tous les codes malicieux : virus, spyware …
- **Le Cache et la QoS** afin d'optimiser et mettre des priorités sur les flux et les sites autorisés pendant les heures de bureau.



Disponible en version appliance et logiciel, la passerelle Olfeo offre une solution d'exploitation, de reporting et de supervision unique.
Afin d'offrir une sécurité Internet optimale, les briques s'enrichissent mutuellement mais peuvent s'acquérir indépendamment.

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

- Des **catégories** de filtrage **adaptées au droit pénal français**,
- Une **solution conforme** au **droit du travail** et aux **exigences de la Cnil**,
- Une **base d'url internationale**, incluant de nombreux sites francophones, classée entièrement « à la main » par des équipes françaises,
- Un éditeur et ses **équipes R&D situés à Paris** pour offrir **proximité** et service optimal.

[1] Australian Communication and Media Authority.
[2] Social Networking Guidance.
[3] British Standards Institute.
[4] Pour plus d'information : http://police.homeoffice.gov.uk.

TABLEAU D'ANALYSE DE LA JURISPRUDENCE EN MATIERE DE FILTRAGE

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
<u>Franck L.</u> c/ Entreprise Martin Un salarié responsable de production et de contrôle informatique est licencié pour faute grave, notamment sur le fondement d'une utilisation abusive et personnelle de l'outil informatique mis à sa disposition, l'employeur ayant contrôlé le disque dur du salarié en son absence, pour en extraire les données de connexions à internet. La Cour d'appel de Nancy puis la Cour de cassation ont donné raison à l'employeur.			
CA Nancy, 27 septembre 2006	Le salarié demande en particulier l'infirmation de la décision de première instance sur le montant de la condamnation de son employeur pour licenciement abusif et sans cause réelle et sérieuse ainsi que la réparation de son préjudice moral. L'employeur demande notamment la réformation du jugement pour ce qui concerne le montant des condamnations prononcées par le Conseil des prud'homme pour licenciement sans cause réelle et sérieuse.		Les extraits historiques journaliers de connexion de l'ordinateur du salarié démontrent qu'il se connectait de manière habituelle pour des durées quotidiennes importantes à des sites d'espace de discussion, de rencontres et sportifs et procédait à des téléchargements pour ses besoins personnels et au gravage de disques (films, logiciels, etc.) Compte tenues des responsabilités du salarié au sein de l'entreprise, les faits qui lui sont reprochés sont particulièrement préjudiciables à l'employeur dans la mesure où il mobilisait pour ses besoins personnels une grande partie des capacités de l'installation informatique et qu'il a pris des risques pour sécurité de l'entreprise dans le but d'occulter ses agissements (utilisation d'adresses anonymes). Il y a donc eu détournement de l'outil informatique et usage abusif, caractérisant la faute grave justifiant le licenciement.
Cour de cassation, 9 juillet 2008		Le salarié invoque une violation des articles 8 de la Convention européenne de sauvegarde des droits de l'homme, 9 du Code civil et L.120-2 du Code du travail, se prévalant du principe de respect de la vie privée sur son lieu de travail, et en particulier du secret de ses communication. La méconnaissance de ces dispositions résultant de : - la prise de connaissance par l'employeur, des sites internet consultés par le salarié ; - et ce, en l'absence du salarié et à son insu.	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.

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
<u>Yahoo</u> UEJF c/ Yahoo ! Inc. et a. (fournisseur d'hébergement + éditeur) Sur le site Yahoo.com figure une page « Auctions » proposant à la vente d'objets nazis. Des associations de lutte contre le racisme et l'antisémitisme ont assigné Yahoo, société de droit américain, devant les juridictions françaises pour avoir rendu accessible en France un site internet proposant la vente aux enchères d'objets nazis. Le tribunal de Paris, en référé, a ordonné au fournisseur d'hébergement de prendre des mesures propres à mettre un terme au dommage et au trouble subi. En outre, le juge a enjoint à Yahoo de prévenir tout internaute dont les recherches l'amènerait à pointer sur des pages illicites qu'il doit interrompre la consultation du site concerné sauf à encourir les sanctions prévues par la loi française. Le juge des référés a donc appliqué à une société de droit américain la loi pénale française. Par suite et afin de s'assurer de la mise en œuvre par Yahoo des mesures techniques de filtrage de l'ordonnance de référé, eu égard à l'état de l'art en matière de filtrage, un collège d'expert a été désigné par le tribunal. Au terme de l'analyse des experts, il a été reconnu l'impossibilité d'assurer un filtrage fiable à 100%, la combinaison la plus complète, à savoir filtrage par mots clés et par adresse IP ne permettant de garantir un filtrage fiable qu'à 90%. Faisant sienne les conclusions des experts, le tribunal a reconnu l'impossibilité pour Yahoo de mettre en place des mesures fiables à 100% et a considéré que par les mesures mises en place, Yahoo avait satisfait à l'esprit de l'ordonnance du 22 mai 2000 lui ayant fait injonction. L'état de l'art a été pris en compte pour déterminer l'exécution ou non par Yahoo de l'injonction prononcée à son encontre, une seule obligation de moyen pesant sur le fournisseur d'hébergement.			
TGI Paris, 22 mai 2000, ordonnance de référé	- injonction de détruire toutes données informatiques stockées directement ou indirectement sur son serveur et de cesser corrélativement tout hébergement et toute mise à disposition sur le territoire de la république à partir du site Yahoo.com de messages évoquant le nazisme. - suppression dans tout annuaire de navigation accessible sur le territoire de la république française à partir des sites Yahoo.com et Fr.Yahoo.com la rubrique d'indexation intitulée « negationists ».	Il est « techniquement impossible de contrôler l'accès au service des enchères ou à d'autres services », et en conséquence d'interdire à un internaute appelant de France de visualiser ceux-ci sur son écran.	- la société Yahoo est à même d'identifier l'origine géographique du site qui vient la consulter « à partir de l'adresse IP de l'appelant ». - cette circonstance doit lui permettre d'interdire aux internautes appelant de France « par tout moyen approprié » d'accéder aux services et sites qui seraient susceptibles de recevoir en France une qualification pénale. - « les difficultés rencontrées par Yahoo, pour réelles qu'elles soient, ne constituent pas des obstacles insurmontables ». <u>Dispositif :</u> « Ordonnons à la société Yahoo de prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de vente aux enchères d'objets nazis et de tous autres sites ou services qui constituent une apologie du nazisme ou une contestation des crimes nazis ». Yahoo dispose d'un délai de deux mois pour soumettre au juge les mesures qu'elle compte prendre pour mettre un terme au dommage et au trouble subi et pour prévenir tout nouveau trouble.
TGI Paris, 11 août 2000, ordonnance de référé	Non-respect par Yahoo de l'obligation mise à sa charge par l'ordonnance du 22 mai 2000 de mettre un terme au trouble constaté. => réitérer l'injonction en l'assortissant d'une astreinte de 200 000 francs (environ 30	- conclusions d'un expert privé mandaté par Yahoo : il « n'existe pas, dans l'état actuel de techniques présentées, de mesures pouvant être mises en œuvre sur le site web, permettant de dissuader et rendre impossible toute consultation de certains services internet, sans détruire la qualité de fonctionnement des services internet, proposés ». - les solutions techniques envisagées ne sont pas incontournables et peuvent aboutir ou à bloquer des	- il est important de vérifier les allégations de la société Yahoo relatives à l'impossibilité de proposer des réponses techniques à l'invitation contenue dans l'ordonnance du 22 mai 2000. - le tribunal mandate à cet effet un collège de consultants aux fins de « décrire les procédures de filtrage pouvant être mises en œuvre par la société Yahoo pour interdire l'accès aux internautes opérant à partir du territoire français, à des rubriques qui pourraient être jugées illicites par les autorités judiciaires françaises ».

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
	000 euros) par jour de retard.	internautes non français, ou à permettre l'accès in fine des sites litigieux à des internautes français, ou encore à bloquer l'accès à des sites non litigieux. - c'est au niveau du point d'accès, c'est-à-dire au point d'initiation de la connexion, que la solution de filtrage serait la plus fiable, c'est-à-dire au niveau de l'outil de consultation (sur le poste de l'internaute) ou au niveau du fournisseur d'accès internet.	- collège de spécialistes = un spécialiste français et deux spécialistes étrangers. Techniciens.
TGI Paris, 20 novembre 2000, ordonnance de référé	<u>Rapport des consultants :</u> <u>Réponse des consultants Laurie & Wallon :</u> - estimation à 70% des adresses IP des français ou résidents sur le territoire français susceptibles d'être correctement identifiées par les prestataires spécialisés - Yahoo procédant à un affichage de bandeaux publicitaires pour les internautes français, elle dispose donc de moyens techniques permettant de les repérer - près de 30% des adresses IP allouées à des français ne peuvent être identifiées correctement - possible d'envisager la sollicitation d'une déclaration de nationalité - idée de destruction des cookies - problématique liée à la description des objets nazis : sont décrits comme tels par les vendeurs par la mention « nazis ». Les consultants considèrent donc qu'il faudrait joindre les deux systèmes : identification géographique + déclaration de la nationalité pour les internautes dont l'adresse IP est ambiguë. Cette solution permettrait d'atteindre un taux de filtrage proche de 90%. <u>Réponse du consultant Vinton Cerf :</u> - relève que les utilisateurs peuvent mentir à propos de leur localisation géographique - problème d'atteinte à la vie privée des internautes (en outre, pourquoi, les internautes étrangers devraient se plier à une décision d'un tribunal français) - utilisation des cookies pour connaître la localisation à chaque nouvelle visite peut être également constitutive d'une atteinte à la vie privée et beaucoup d'internautes les refusent. Ce consultant considère qu'« il n'apparaît pas très opérationnel de se fier à la recherche de la localisation géographique pour imposer le filtrage tel qu'il est décrit dans la décision du tribunal ».		l résulte desdites conclusions que la localisation physique d'un internaute est possible à partir de l'adresse IP. <u>Dispositif :</u> « Constatons que Yahoo a satisfait en grande partie à l'esprit et à la lettre de la décision du 22 mai 2000 contenant injonction à son encontre ». - le tribunal reconnaît que la société Yahoo ne pouvait garantir un résultat fiable à 100% et qu'il lui appartenait donc de mettre uniquement en œuvre les moyens techniques dont elle dispose ; ce qu'elle a fait en l'espèce.
	Constater l'inexécution de l'ordonnance du 22 mai 2000 : injonction de prendre toute mesure pour empêcher l'accès au site illicite.	Impossibilité de mettre en œuvre des moyens techniques de nature à satisfaire les termes de l'ordonnance du 22 mai 2000.	
TGI Paris, 11 février 2003	Demande la condamnation de la société Yahoo en qualité de civilement responsable « en	La société Yahoo précise avoir mis en place une technologie permettant d'empêcher la présentation, sur son service, de ventes d'objets prohibés, au nombre desquels les articles	- par « des modifications de son système de filtrage des offres de vente annoncées le 2 janvier 2001 et entrées en vigueur le 10 janvier suivant, la société Yahoo a « satisfait à l'injonction qui lui avait été donnée et fait

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
	raison du maintien délibéré sur le site internet Yahoo.com d'un service de vente aux enchères d'objets nazis réceptionnés à Paris ».	« nazis ».	cesser les faits objet de la poursuite, quelque qualification qu'elle soit susceptible de revêtir ». - « la promptitude (…) doit s'apprécier au regard des difficultés encourues et du résultat obtenu ». - la solution mise au point est plus satisfaisante que celle initialement envisagée par le juge des référés puisqu'il a été mis en place un barrage ab initio fonctionnant donc dans le monde entier. ⇨ La responsabilité civile de Yahoo ne peut être recherchée.
CA Paris, 6 avril 2005			La cour considère, comme le tribunal, que Yahoo, confrontée à des difficultés techniques, avait agi avec la promptitude requise.
United States District Court, California, 7 novembre 2001		Impossibilité d'exécuter les ordonnances de 2000 rendues par les juridictions françaises du fait de leur incompatibilité avec la constitution et les lois des Etats-Unis, en particulier du 1er amendement qui garantit la liberté d'expression.	- les tribunaux reconnaissent les jugements et décrets étrangers, sauf si leur application était préjudiciable ou contraire aux intérêts de la nation. - reconnaît le droit souverain de la France de s'exprimer en France, mais refus du tribunal de faire appliquer un jugement étranger qui viole la protection de la constitution des Etats-Unis en gelant la liberté d'expression. - 1er amendement plus important que le principe de courtoisie entre pays.
United States Court of Appeals, California, 12 janvier 2006		- la restriction de l'accès en France au site risque d'avoir des répercussions sur le public américain et donc de violer le 1er amendement.	- Yahoo a respecté les mesures ordonnées par le tribunal français en restreignant l'accès du site aux français uniquement. - pas d'entrave au 1er amendement puisque le public américain n'a pas été touché par les mesures techniques. Les mesures s'appliquent au public français sans incidence sur le public américain. L'application du 1er amendement ne peut être étendu en France. - seul une interdiction générale d'accès au site aurait eu des répercussion sur le public américain et aurait constitué une atteinte à la liberté d'expression. Ce n'est pas le cas en l'espèce. - l'accès aux contenus racistes et antisémites sont interdit par la loi française et la violation par le public français de la loi française ne doit pas être facilitée.

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
<u>Vivastreet</u> SA Parfums Christian Dior et a. c/ SARL Database Management and Information Services et a. (fournisseur d'hébergement) Les sociétés Parfums Christian Dior et autres ont constaté la vente, sur le site www.vivastreet.fr et hors de leur réseau de distribution sélective, de leurs parfums. Il ont alors assigné les fournisseurs d'hébergement du site www.vivastreet.fr et exigé la mise en place, pendant six mois, d'un système de filtrage a priori permettant de détecter et de bloquer l'hébergement d'offres illicites. Sur le fondement de l'article 6-I 7° de la LCEN qui permet de demander aux fournisseurs d'accès et d'hébergement une surveillance ciblée et temporaire et sur le fondement de l'article 6-I 8° qui autorise le tribunal à prescrire en référé toute mesure pour faire cesser un dommage généré par les contenus en ligne, le juge a fait droit à la demande des sociétés Parfums Christian Dior et autres par ordonnance du 26 juillet 2007. Toutefois, quelques annonces ont été diffusées postérieurement. Estimant que l'ordonnance du 26 juillet 2007 avait été mal exécutée quant au flitrage, les sociétés Parfums Christian Dior et autres sont retournées devant le même tribunal qui a maintenu l'obligation d'établir une surveillance, refusant d'attendre la mise en place, deux mois plus tard, d'un « logiciel efficace ». Dans cette affaire, le Tribunal de commerce de Paris a refusé de prendre en compte les difficultés techniques engendrées par la mise en place d'un filtrage qui serait fiable à 100% et a considéré que le fait que quelques annonces illicites aient pu être diffusées postérieurement à l'ordonnance de juillet démontrait la mauvaise exécution par les sociétés Database de l'injonction.			
TC Paris, 26 juillet 2007, ordonnance de référé	<u>Visa : Art.6.I 7°, 6.I 8° et 6-II LCEN :</u> - mise en place d'un système de surveillance dans la rubrique « Beauté / Santé » du site www.visastreet.fr. - mise en place d'un système de contrôle permettant de retirer toute annonce proposant la vente de parfums et produits cosmétiques dont le texte utilise les dénominations des demanderesses. - prise en compte un tableau de concordance ou d'équivalence avec les dénominations pour permettre le contrôle et la surveillance. - mise en place d'un système de contrôle des contrefaçons, à savoir les parfums présentés comme « génériques » ou imitant « les fragrances des demanderesses ».	- prise en compte de la mise en place d'un système de filtrage par mots clefs permettant un contrôle des annonces litigieuses et leur surpression. - engagement à étendre ces systèmes de filtrage en insérant à titre de mots clefs bloquant les mots communiqués par les parties adverses.	- injonction de mettre en place un système de surveillance pour une durée de six mois. <u>Dispositif :</u> « Faisant injonction aux sociétés Database (…) de cesser d'héberger les annonces portant atteinte aux droits des sociétés Parfums Christian Dior (…) en supprimant l'hébergement des annonces litigieuses identifiées par les demanderesses et ce, sous astreinte provisoire de 500 euros par jour de retard et par infraction constatée, passé un délai de huit jours suivant la signification de l'ordonnance, pendant trente jours, passé lequel délai, il sera à nouveau fait droit ». « Faisant injonction aux sociétés Database (…) de mettre en place sur la rubrique beauté santé du site vivastreet.fr (…) dans un délai de huit jours suivant la signification de l'ordonnance (…) : - un système de surveillance ciblé et temporaire pour une durée de six mois des annonces de ladite rubrique, afin de prévenir l'hébergement de toute annonce proposant la vente hors du réseau de distribution sélective des demanderesses de parfums et produits cosmétiques » utilisant les dénominations des demanderesses et/ou comportant un tableau de concordance et/ou offrant la vente des parfums présentés comme « génériques ». En outre, il est fait injonction aux sociétés Database de mettre en place « un système de contrôle ciblé et temporaire » pour une durée de six mois permettant de retirer toutes annonces proposant la vente hors du réseau de distribution sélective du même type de produits.

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
TC Paris, 31 octobre 2007, ordonnance de référé	- exécution de l'ordonnance du 26 juillet 2007 imparfaite : en dépit des mesures de surveillance imposées par le juge, 8 annonces portant atteinte à la dénomination ou au réseau de distribution sélective des demandeurs ont été diffusée sur le site www.vivastreet.fr pendant une durée total de 28 jours. ⇨ liquidation des astreintes. - maintenir en vigueur sur la rubrique « Beauté/Santé » du site www.vivastreet.fr un système renforcé de surveillance ciblé et temporaire des annonces afin de préserver toute annonce, hors réseau de distribution sélective, de parfums et produits cosmétiques utilisant dénomination et/ou comportant un tableau de concordance ou d'équivalence et/ou offrant à la vente des parfums de « grande marque » ou présentés comme génériques. + un système renforcé de contrôle ciblé et temporaire sur les mêmes produits.	Proposent de supprimer sur le site la « boutique santé-beauté ».	Sur la liquidation des astreintes : - une annonce ne correspond pas exactement au texte des annonces visées par l'ordonnance du 26 juillet 2007. - pour les autres, maintenues pendant une durée de 10 jours, liquidation de l'astreinte : 5 000 euros. Sur la poursuite des mesures de surveillance sous astreinte : - les fournisseurs d'hébergement ne justifient pas avoir accompli de diligences nouvelles pour prévenir l'hébergement d'annonces litigieuses. - refus d'attendre comme le demandent les hébergeurs que soit mis en place en France un « logiciel efficace » pour permettre la surveillance : « Il n'est pas question de lier à la bonne volonté d'une partie, l'application d'une décision visant à évier de publier des annonces, dont il n'est pas contesté, qu'elles sont totalement interdites ». ⇨ Enjoint de prévenir ou retirer toute annonce proposant à la vente hors du réseau de distribution sélective de parfums et de produits cosmétiques (même formulation que pour l'ordonnance du 26 juillet 2007). + ordonne l'identification des nouveaux annonceurs dont les annonces ont été publiées après l'ordonnance du 26 juillet 2007.

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
<u>Multimania</u> UEJF c/ Multimania (Lycos France) (fournisseur d'hébergement) L'UJF, après avoir découvert l'existence d'un site http://www.multimania.com/nsdap/ qui diffusait des pages à contenu raciste, a sommé la société Multimania de fermer ce site et de lui communiquer les coordonnées de l'abonné. La société Multimania a fermé immédiatement le site, sans pouvoir communiquer les coordonnées en raison de la législation relative à la communication des données personnelles. Quelques heures après, le site litigieux a été réouvert par son éditeur, puis a définitivement été refermé le lendemain. L'UJF a alors assigné la société Multimania sur le fondement de l'article 1383 du Code civil pour avoir manqué à ses obligations de prudence et de diligence. Le tribunal, puis la cour, ont considéré qu'en l'état des techniques, la société Multimania avait déféré à son obligation d'hébergeur, obligation de moyen et non de résultat. Elle ne pouvait donc voir sa responsabilité engagée du fait de la publication des contenus illicites sur des sites qu'elle héberge.			
TGI Nanterre, 24 mai 2000	Sur le fondement de l'article 1383 du Code civil, l'UEJF reproche à Multimania, « en tant que professionnel de l'internet » d'avoir manqué à ses obligations de prudence et de diligence en hébergeant « un site dont l'illicéité était aisément détectable par le moyen d'un moteur de recherche ».	La société Multimania a fait valoir qu'elle satisfait aux obligations de prudence et de diligence qui lui ont été imposées.	- il n'est pas exigé du fournisseur d'hébergement qu'il exerce une surveillance minutieuse et approfondie des sites qu'il abrite ; - « le contrôle, qui ne peut être effectué a priori avant la mise en ligne du site dont l'initiative revient à l'internaute, est nécessairement aléatoire et faillible du fait des manœuvres de contournement entreprises pour le déjouer » ; - « l'obligation qui lui est faite n'est pas une obligation de résultat » ; - « l'hébergeur doit prendre les mesures qu'un professionnel avisé mettrait en œuvre pour évincer de son serveur les sites dont le caractère illicite est apparent » ; - dès lors, « la responsabilité du fournisseur d'hébergement devant s'apprécier selon ses compétences propres et non selon les compétences idéales de tiers rompus au domaine de la lutte contre le racisme et de l'antisémitisme, aucune faute ne peut être retenue à l'encontre de Multimania ». Dans ces conditions, rejet de l'action de l'UJF.
CA Versailles, 16 mai 2002	Maintient que la société Multimania a manqué à ses obligations de prudence et de diligence en hébergeant un site dont le caractère illicite est aisément détectable. L'absence de vérification du contenu du site est fautive. L'article 1383 du Code civil permettait de pallier les insuffisances des dispositions en vigueur avant la loi du 1er août 2000 posant le principe de l'identification obligatoire de l'auteur d'un site auprès de l'hébergeur lorsqu'il s'agit d'un particulier.	Aucune maîtrise en temps réel sur les pages personnelles mises en ligne, sans contrôle préalable et qui peuvent être modifiées en permanence par leur auteur. Existence d'une charte à laquelle il faut adhérer pour ouvrir un compte. Mise en place de procédure permettant de détecter d'éventuels contenus illicites sur les sites les plus consultés ou concernant les transferts de fichiers volumineux, ces mesures étant complétées par des recherches de noms de fichiers connus comme étant suspects. Rappelle que les procédés techniques sont faillibles et contournables, la détection automatique des contenus illicites n'étant pas possible en l'état des techniques ; pour cette raison, le site litigieux a échappé aux contrôles. Obligation de surveillance = obligation de moyens : doit s'apprécier in abstracto en prenant en compte les circonstances réelles et concrètes dans lesquelles s'effectue la surveillance.	- il ne peut être exigé de Multimania qu'elle surveille en temps réel les sites quotidiennement ouverts chez elle. Cette dernière justifie avoir adopté les procédures de contrôle de nature à permettre, en l'état des techniques considérées, la détection des contenus illicites. - a rapidement satisfait aux demandes de renseignements de l'Uejf grâce aux données de connexion dont elle disposait. ⇨ Les premiers juges ont estimé à bon doit que Multimania avait mis en œuvre tous les moyens que l'on pouvait raisonnablement exiger d'un professionnel de l'hébergement de sites. ⇨ A satisfait à l'obligation à laquelle elle était tenue de prévenir ou de supprimer la présence sur ces sites de contenus à caractère illicite.

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
<u>Aaargh</u> Uejf et a. c/ OLM,LLC et a. (fournisseurs d'hébergement, sociétés de droit américain) AFA, Free, Tiscali, AOL et a. (fournisseurs d'accès internet) Un site internet hébergé par des fournisseurs d'hébergement américains contient des propos négationnistes rédigés en langue française. Sur la base de la LCEN, plusieurs associations de lutte contre le racisme saisissent en référé le Tribunal de grande instance de Paris pour faire constater que les propos sont illicites. Partant, elles demandent aux fournisseurs d'hébergement de prendre les mesures nécessaires permettant l'arrêt de la publication en ligne du site Aaargh. En application de l'article 6-I 8° de la LCEN, à la suite de l'inaction des hébergeurs, les associations ont demandé aux fournisseurs d'accès internet de prendre les mesures propres à faire cesser le dommage constitué par la mise en ligne des propos négationnistes. Après plus de trois ans de procédure, la Cour de cassation confirme l'interprétation de l'article 6-I 8° de la LCEN et confirme le filtrage imposé aux fournisseurs d'accès internet. Elle considère qu'il peut être prescrit à toute fournisseur d'accès internet de prendre des mesures afin de faire cesser un trouble manifestement illicite, confirmant ainsi l'arrêt de la Cour d'appel de Paris du 24 septembre 2006. La mesure, même imparfaite, permet de réduire, en l'état actuel de la technique, l'accès des internautes à un site illicite. Il appartient donc aux prestataires techniques de mettre en œuvre les moyens dont ils disposent aux vues de l'état de l'art, sans que puisse leur être imposée une obligation de résultat.			
TGI Paris, 20 avril 2005, ordonnance de référé	<u>Au visa de l'article 6-I 8° de la LCEN :</u> - ordonner aux fournisseurs d'hébergement d'empêcher toute mise à disposition du service de communication au public Aaargh à partir de leur serveur et sur le territoire français ; - aucune demande à l'encontre des fournisseurs d'accès internet. + demandent une réouverture des débats pour vérifier l'exécution des obligations prescrites.	Fournisseurs d'hébergement non comparants.	<u>Moyens</u> : « L'affichage du contenu de ce site et son architecture conduisent à retenir que c'est en totalité que celui-ci se présente comme manifestement illicite, toute distinction au niveau de la mesure de retrait entre telle ou telle publication se révélant, au moins sur le plan technique, à la fois impraticable et inefficace ; il ne peut en conséquence qu'être ordonné qu'il soit mis fin à l'accès au site en question afin de faire cesser le dommage ». <u>Dispositif</u> : « Ordonnons à la société de droit américain ThePlanet.com Internet Services Inc. d'empêcher sous peine d'astreinte de 5 000 euros par jour de retard à l'expiration d'un délai de 72 heures faisant suite à la signification de la présente ordonnance, toute mise à disposition à partir de leurs serveurs et sur le territoire français du site internet accessible à l'adresse www.vho.org/aaargh ». + obligation de fournir les éléments d'identification de l'éditeur du site.
TGI Paris, 13 juin 2005, ordonnance de référé	Interdiction de l'accès au site litigieux	La mesure prescrite doit respecter le principe de proportionnalité et être précisée alors qu'il n'existerait qu'un nombre limité de méthodes envisageables pour interdire l'accès au site. Certains fournisseur d'accès internet considèrent que les techniques disponibles ne permettent pas un filtrage efficace et assurant une fiabilité à 100%.	Art. 6-I-8° LCEN <u>Dispositif :</u> « Fait injonction aux sociétés France Telecom Services (…) de mettre en œuvre toutes mesures propres à interrompre l'accès à partir du territoire français au contenu du service de communication en ligne hébergé actuellement à l'adresse « www.vho.org/aaargh ». <u>Délais :</u> 10 jours à compter du prononcé de la décision pour justifier des mesures mises en œuvre.

Juridiction et date de la décision	Demandes	Moyens opposés par les prestataires techniques	Moyens et dispositif de la décision
CA Paris, 24 novembre 2006 (appel des FAI)		L'art. 6-I 8° de la LCEN pose un principe de subsidiarité : ne peuvent être prononcées des mesures contre les fournisseurs accès internet qu'en cas de défaillance des prestataires d'hébergement ⇨ Les demandeurs auraient dû exercer tout recours possible auprès des sociétés de droit américain. La mesure ordonnée par les premiers juges est impropre à faire cesser le dommage. Elle est en outre disproportionnée puisqu'elle entrave l'accès aux sites portant le même nom de domaine. ⇨ Le filtrage opéré par les fournisseurs d'accès internet est inadapté à la lutte contre les contenus illégaux.	- en dépit des difficultés techniques du filtrage, du coût et de la complexité de sa mise en œuvre et de son efficacité contestable, le recours à ce procédé n'est pas exclu. Il permet que soient prises « toutes mesures propres à prévenir ou faire cesser le dommage ». La mesure, même imparfaite, permet de réduire, en l'état actuel de la technique, l'accès des internautes à un site illicite. - les prestataires d'accès ont été laissés libres par le premier juge pour mettre en œuvre tous les moyens dont ils peuvent disposer en l'état de leur structure et de leur technologie. Dans ces conditions, la cour confirme les ordonnances des 20 avril 2005 et 13 juin 2005.
Cass, civ 1, 19 juin 2008		Devant la Cour de cassation, et sur le fondement de l'article 6-I 8° de la LCEN, les fournisseurs d'accès internet demandent que soit constatée l'impossibilité de leur délivrer une injonction dès lors qu'il existe des moyens de contraindre les fournisseurs d'hébergement à mettre fin à leur hébergement du site illicite. En outre, l'injonction faite au fournisseur d'accès internet aurait dû limiter dans le temps la validité et les effets de cette mesure. La mesure prise à l'encontre des fournisseurs d'accès internet est indéterminée dans sa portée, inefficace dans ses effets et a un caractère définitif qui porte ainsi une atteinte manifestement disproportionnée à la liberté de communication publique par voie électronique.	Sur le fondement de l'article 6-I 8° de la LCEN : - l'autorité judiciaire « peut prescrire en référé ou sur requête à toute personne mentionnée au 2 (les prestataires d'hébergement) ou à défaut à toute personne mentionnée au 1 (les fournisseurs d'accès), toutes mesures propres à prévenir ou à faire cesser un dommage occasionné par le contenu d'un service de communication public en ligne ». Rejet du pourvoi.