Rapport

Filtrage d'Internet

Equilibrer les réponses à la cybercriminalité dans une société démocratique

Par

Cormac Callanan (Irlande)
Marco Gercke (Allemagne)
Estelle De Marco (France)
Hein Dries-Ziekenheiner (Pays-Bas)

Traduction française :

Estelle De Marco
Avec la contribution de Frédéric Nguyen (fnguyen_at_worldnet_dot_net)

11 mai 2010

Ce rapport a été préparé dans le cadre d'un financement de l'Open Society Institute.

Les opinions exprimées dans ce document ne reflètent pas nécessairement celles de l'Open Society Institute.

Contacts

Pour de plus amples informations, merci de contacter :

M. Cormac Callanan

Tél. : +353 87 257 7791
E-mail : cormac.callanan_at_aconite_dot_ie

M. Marco Gercke

Tél. : +49 221 2707205
E-mail : gercke_at_cybercrime_dot_de

Mme Estelle De Marco

Tél. : +33 4 90 84 16 70
E-mail : estelle.de.marco_at_inthemis_dot_fr

M. Hein Dries-Ziekenheiner
Tél. : +31 71 711 3243
E-mail : hein_at_vigilo_dot_nl

Les opinions exprimées dans ce document ne reflètent pas nécessairement celles de l'Open Society Institute.

Les auteurs

CORMAC CALLANAN **IRLANDE**

Cormac Callanan est directeur d'Aconite Internet Solutions (www.aconite.com), entreprise qui offre une expertise en développement de politiques dans le domaine de la cybercriminalité et de la sécurité sur Internet.

Titulaire d'un master en sciences de l'informatique, il a plus de 25 ans d'expérience professionnelle dans le domaine des réseaux informatiques internationaux et 10 ans d'expérience dans le domaine de la cybercriminalité. Il a assuré des formations auprès d'Interpol, d'Europol et de services en charge de l'application de la loi dans de nombreux pays. Il propose actuellement des services de conseil au niveau mondial et a travaillé sur le développement de politiques avec le Conseil de l'Europe et l'ONUDC.

En 2008, il co-rédigea avec Marco Gercke une étude sur les bonnes pratiques permettant une coopération entre les organes de répression et les fournisseurs de services Internet contre la cybercriminalité (www.coe.int/cybercrime), adoptées sous forme de lignes directices lors de la conférence Octopus de 2008. En 2009, il rédigea avec Nigel Jones un rapport relatif à 2Centre (réseau de centres d'excellence en cybercriminalité pour la formation, la recherche et l'éducation), dégageant les bonnes pratiques internationales en matière de formation, aux investigations liées aux TIC, des services d'enquête et de répression (www.2centre.eu).

Cormac fut président puis secrétaire général d'INHOPE, l'Association internationale de services d'assistance en ligne (www.inhope.org), laquelle facilite et coordonne le travail de services d'assistance en ligne (« *hotlines* ») qui œuvrent contre les usages et contenus Internet illégaux. Il fut co-auteur du premier rapport d'INHOPE, en 2007, sur les tendances de l'Internet au niveau mondial, qui constitua une publication repère pour ce qui concerne la pédopornographie sur Internet.

Cormac fonda en 1997 l'Association irlandaise des prestataires de services Internet (ISPAI - www.ispai.ie), dont il présida le Conseil d'administration durant 5 ans, jusqu'en février 2003. Il fut secrétaire général de l'Association européenne des prestataires de services (www.euroispa.org). En 1998, il fonda et dirigea le service irlandais d'assistance en ligne www.hotline.ie, qui prend en charge les signalements de pédopornographie et de discours de haine sur Internet. Il rédigea le Code de conduite de l'ISPAI.

Cormac fonda en 1991 la première entreprise commerciale irlandaise de prestation d'accès à Internet en B2B - EUnet Irlande – qui fut vendue en 1996. Il est membre du Bureau de l'Association irlandaise pour le droit d'auteur (www.cai.ie). Il fut membre du groupe de travail britannique et irlandais « Rightswatch » (www.rightswatch.com), qui a développé des lignes directrices relatives aux procédures de notification et de retrait en matière de propriété intellectuelle.

MARCO GERCKE **ALLEMAGNE**

Marco Gercke, Docteur en droit, est directeur de l'Institut de droit pénal des médias (Institut fuer Medienstrafrecht) - un institut indépendant de recherche sur les aspects juridiques des actes délictueux et criminels commis en lien avec l'informatique et Internet.

Titulaire d'un doctorat en droit pénal et spécialisé en cybercriminalité, il a enseigné pendant plusieurs années le droit de la cybercriminalité et le droit pénal européen à l'Université de Cologne, et est maître de conférences invité en droit pénal international à l'Université de Macao.

Ses recherches se concentrent sur les aspects internationaux du droit relatif à la cybercriminalité. A cet égard, il est expert auprès de plusieurs organisations internationales, dont le Conseil de l'Europe, l'Union européenne, les Nations Unies et l'Union internationale des télécommunications. Parmi les éléments clefs de ses recherches, figurent les défis que pose la lutte contre la cybercriminalité et les différences que présentent les systèmes juridiques de tradition orale et ceux de tradition écrite lorsqu'ils lui apportent une réponse juridique. Ses derniers projets de recherche ont couvert les activités des organisations terroristes sur Internet, les réponses juridiques à l'usurpation d'identité, le blanchiment d'argent, les activités financées par le terrorisme impliquant des technologies Internet et la responsabilité des prestataires de services Internet.

Marco donne fréquemment des conférences aux niveaux national et international, et est l'auteur de plus de 60 publications relatives à la cybercriminalité. En plus de ses articles et de ses livres, il a publié plusieurs études, incluant des analyses de droit comparé, pour le Conseil de l'Europe. La question de la responsabilité des prestataires de services Internet dans le cadre de la lutte contre la cybercriminalité était le sujet d'une étude qu'il a menée pour le Conseil de l'Europe et qui a été rendue publique en mars 2009. Sa dernière publication de 255 pages sur la cybercriminalité est actuellement en cours de traduction dans l'ensemble des langues des Nations Unies.

Marco a assuré la co-présidence du groupe de travail mis en place par le Conseil de l'Europe ayant soutenu la rédaction des lignes directrices pour la coopération entre les organes de répression et les fournisseurs de services Internet contre la cybercriminalité, adoptées lors de la conférence Octopus de 2008, et est membre du Groupe d'experts de haut niveau de l'UIT. Il est membre du Barreau allemand et secrétaire du département de droit pénal de la Société allemande pour le droit et les questions informatiques.

Une liste complète de ses publications et discours peut être trouvée à l'adresse : www.cybercrime.de.

ESTELLE DE MARCO **FRANCE**

Estelle De Marco, Docteur en droit, est consultante en affaires juridiques et réglementaires liées aux TIC et secrétaire générale du Centre de recherche et d'études sur la sécurité de l'information et la cybercriminalité (CRESIC, Montpellier).

Titulaire d'un Doctorat en droit privé et sciences criminelles, spécialisée en droit civil, droit pénal, droit de l'informatique et droits de l'Homme, elle a plus de 10 ans d'expérience sur les questions juridiques relatives aux TIC et 7 ans d'expérience sur les problématiques juridiques et politiques liées aux contenus illégaux sur Internet (incluant les questions de responsabilité des acteurs Internet, de propriété intellectuelle et de protection des données personnelles). Elle participe au groupe de travail d'Europol sur l'harmonisation des formations en matière de cybercriminalité.

Estelle a été responsable affaires juridiques et réglementaires auprès de l'association française des prestataires d'accès et de services Internet (AFA) durant 6 ans. Elle a une solide compréhension des questions techniques relatives aux TIC. En qualité de responsable du service d'assistance en ligne de l'AFA contre les contenus illégaux, elle était impliquée dans une coopération quotidienne avec les services de police français œuvrant contre la cybercriminalité et participait aux projets d'INHOPE. Elle représentait l'industrie Internet française dans de nombreuses enceintes internationales.

Elle fut membre du groupe de travail du Conseil de l'Europe ayant soutenu la rédaction des lignes directrices pour la coopération entre les organes de répression et les fournisseurs de services Internet contre la cybercriminalité, adoptées lors de la conférence Octopus de 2008. Elle réalisa plusieurs études juridiques relatives à la protection de l'enfance, la cybercriminalité ou la propriété intellectuelle, en soutien des positions de l'industrie vis-à-vis du Ministère de la culture, du Ministère de l'économie ou de la Commission européenne. En coordination avec les membres de l'AFA, elle rédigea la position de l'industrie en matière de lutte contre le spam et la première version du cahier des charges du mécanisme de Signal spam, qui permet aux FAI d'être informés du spam sortant de leur réseau (www.signal-spam.fr). Elle participa à la création de Signal spam et fut membre de son Bureau. Estelle travailla également 4 ans au Tribunal de grande instance de Montpellier.

Estelle est membre de Cyberlex (www.cyberlex.org), une association d'experts juridiques et techniques dans le domaine des TIC, et du comité scientifique de Juriscom.net (www.juriscom.net), une revue juridique en ligne spécialisée en droit des TIC qui publie régulièrement les contributions de juristes, universitaires ou professionnels. Elle a créé et maintenu pendant 10 ans la rubrique « droit et déontologie » du site Internet du Comité Réseaux des Universités, conçue pour les experts techniques (www.cru.fr/documentation/droit-deonto/index).

HEIN DRIES-ZIEKENHEINER **PAYS-BAS**

Hein Dries-Ziekenheiner, LL.M, est le dirigeant de VIGILO consult, une agence de conseil néerlandaise spécialisée dans les domaines de la régulation d'Internet, de la cybercriminalité et du droit lié aux TIC. Hein est titulaire d'un Master en droit civil néerlandais de l'Université de Leiden et a plus de cinq ans d'expérience technique dans les domaines de l'investigation numérique et de l'application de la loi sur Internet.

De par ses rôles de responsable affaires juridiques et réglementaires et de représentant de l'association néerlandaise des prestataires de services Internet (NLIP), Hein a acquis de larges compétences et plus de dix ans d'expérience dans les domaines de la gestion de réseau sur Internet, des politiques relatives à Internet et de l'application de la loi au réseau.

Hein fut délégué au Bureau de l'Association européenne des prestataires de services Internet (EuroISPA). A cette occasion, il contribua activement à des interventions et positions écrites sur une variété de sujets, dont le cadre réglementaire des télécommunications 2002, le régime de responsabilité des prestataires de services Internet et les questions de vie privée. Il représenta l'industrie néerlandaise des prestataires de services Internet dans plusieurs autres enceintes (inter)nationales.

En tant que membre de l'équipe sur la sécurité Internet de l'OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit), l'Autorité néerlandaise de régulation des télécommunications, Hein fut responsable de la première amende importante infligée pour spam dans le contexte du cadre réglementaire de l'Union européenne 2002, et travailla sur le dossier concernant la triste affaire du logiciel malveillant « DollarRevenue ». Il fut en charge de plusieurs autres affaires relatives à des spam ou à des logiciels malveillants dont les dossiers furent constitués par l'OPTA, l'Administration néerlandaise indépendante des postes et des télécommunications.

Hein assure régulièrement des formations auprès de diverses autorités, en matière d'investigation numérique liée au spam et aux logiciels malveillants, et a coopéré en divers endroits du monde sur des affaires de spam avec de nombreux services d'enquête, tels que la FTC et le FBI des Etats-Unis, l'ACMA australienne et le réseau CPC de l'Union européenne, réseau d'autorités publiques chargées de faire respecter les règles de protection des consommateurs dans les Etats membres. Hein est membre de l'Association néerlandaise pour le droit et les questions informatiques. Son entreprise, VIGILO consult, est membre observateur, pour l'industrie, du London action plan (Plan d'action de Londres) sur le spam (LAP).

Hein intervient et publie régulièrement sur des questions relatives à l'application de la loi sur Internet et à la cybercriminalité.

Sommaire

Chapitre 1 SYNTHESE

1.1 Introduction

Le présent rapport explique ce qu'est le filtrage d'Internet. Il fait état des motivations conduisant à la mise en œuvre du filtrage dans une société, des options techniques disponibles à cette fin et des problématiques juridiques qui peuvent avoir une incidence sur les stratégies de filtrage.

Note : Les citations figurant dans cette synthèse ne sont pas directement attribuées à leur auteur. Ces citations sont clairement indiquées entre guillemets et peuvent être retrouvées dans le texte principal de la présente étude, accompagnées d'une référence précise à leur auteur et à leur source. La reproduction de ces citations à partir du présent rapport n'est autorisée qu'accompagnée d'une référence à leur auteur originel ET d'une référence à la page précise du chapitre concerné de la présente étude, où le nom de cet auteur est mentionné.

1.2 Qu'est-ce que le filtrage d'Internet ?

Le présent rapport propose une analyse détaillée de l'état actuel de la situation en matière de filtrage d'Internet, une présentation de l'environnement juridique et réglementaire relatif à ce filtrage, ainsi que des observations concernant l'efficacité d'une telle mesure et son impact, tant sur la lutte contre la cybercriminalité, que sur le maintien de la démocratie et de la sécurité des individus.

La question de savoir où se trouve le meilleur équilibre entre la protection de l'enfance et la protection des libertés démocratiques est très complexe, et doit être tranchée in fine à un niveau national, dans chaque pays, au terme d'un large débat entre les acteurs concernés, débat devant tenir compte des instruments internationaux contraignants, tels que la Convention européenne des droits de l'Homme (CEDH).

Selon les membres du Parlement européen, le libre accès à Internet, sans ingérence, est un droit d'une considérable importance. Internet est « *une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information*», dont l'accès est protégé par le droit à la liberté d'expression, même s'il n'est pas actuellement considéré comme un droit fondamental autonome[1].

Ces dernières années, certains Etats démocratiques ont promu l'usage de technologies de filtrage d'Internet visant différents types de contenus. Ils ont invoqué l'intérêt général pour requérir la mise en œuvre de mesures spécifiques de filtrage, en vue d'assurer le respect de divers aspects de leur politique publique, dans un contexte où les caractéristiques d'Internet rendent l'application de la loi difficile (au niveau international). Les contenus visés sont variés et concernent tant la disponibilité d'objets nazis sur des sites de vente en ligne, que l'hébergement de sites de jeux d'argent dans des Etats dont les législations sont libérales sur

[1] Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe, 2007/2153(INI), § 23, accessible à cette adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//FR. Voir infra, sous-section 6.6.2.2.

la question. De manière analogue, certains Etats, au régime moins ouvert sur l'information, utilisent le filtrage comme une ressource technique qui leur permet d'étendre, au monde électronique, leur pratique du contrôle de l'information.

Qu'est-ce que le filtrage d'Internet ?

Le filtrage d'Internet (parfois nommé blocage d'Internet) n'est pas une activité récente. Il en est question depuis plusieurs années. Toutefois, la notion recouvre une si large gamme de pratiques, de matériels informatiques, de logiciels et de services, qu'il serait une erreur de croire que tous les types de filtrage sont les mêmes ou qu'ils sont d'efficacité équivalente, qu'ils entraînent les mêmes conséquences juridiques ou bien qu'un système donné pourrait être aisément utilisé pour cibler plus d'un type de contenus.

Le premier objectif du filtrage d'Internet est d'empêcher un contenu d'atteindre un ordinateur personnel ou un poste informatique, à l'aide d'un produit logiciel ou matériel dont la fonction est de surveiller l'ensemble des communications Internet et de déterminer s'il y a lieu d'empêcher la réception et/ou l'affichage de contenus spécifiquement ciblés.

Par exemple, un message électronique peut être bloqué car il est suspecté d'être un spam, un site web peut être filtré parce qu'il est suspecté de contenir des logiciels malveillants, ou une session de pair à pair (« *peer-to-peer* » ou P2P) peut être interrompue parce qu'elle est suspectée de véhiculer un échange de contenus à caractère pédopornographique.

L'expression « filtrage d'Internet » elle-même paraît quelque peu inappropriée, car elle semble suggérer que le filtrage du réseau est simple à mettre en œuvre et qu'il se résume à la possibilité de choisir de l'activer ou de le désactiver, aussi simplement que s'il s'agissait d'utiliser un interrupteur. Rien ne peut être plus éloigné de la réalité, en ce que les technologies de filtrage d'Internet sont particulièrement complexes et peuvent souvent être contournées avec une grande facilité. Il y a plusieurs raisons à cela, la plus essentielle étant qu'Internet a été conçu pour être décentralisé, et qu'il a été doté d'une capacité intrinsèque à assurer que les données puissent circuler « en contournant » toute barrière qui pourrait être mise sur leur route[2].

Le filtrage d'un contenu Internet mis légalement à disposition hors d'un pays, mais considéré comme étant illégal dans ce dernier, peut parfois être considéré comme une option permettant au dit pays de tenter de maintenir ses propres standards culturels nationaux, dans une situation d'accès global.

Il peut être dit que le filtrage d'Internet commença il y a vingt ans avec le filtrage des messages électroniques non sollicités (spams). Cette initiative vit le jour pour plusieurs raisons, mais était initialement destinée à éviter la saturation des réseaux. Elle a constitué un domaine constant de recherche et de développement, et a été au cœur d'une compétition soutenue entre les initiatives anti-spam et les activités de spamming. Malgré les efforts considérables que la lutte anti-spam a impliqués sur une longue période de temps, tout utilisateur des services de messagerie électronique sait aujourd'hui que le filtrage du spam n'a pas été un franc succès, puisqu'il n'a pas permis d'éradiquer ce type de messages du réseau.

Il est important de noter que tous les systèmes de filtrage d'Internet sont sujets à des problèmes de faux-négatifs[3] et de faux-positifs[4], lesquels sont minimisés, dans les systèmes avancés, lors de la conception des technologies de filtrage.

[2] L'éventail complexe des problématiques techniques est résumé au chapitre 5 de la présente étude.
[3] Un faux négatif est un message électronique qui se trouve autorisé à passer au travers du filtre anti-spam, car lors de son contrôle il est noté comme étant négatif, c'est-à-dire comme ne contenant pas de spam, alors qu'il s'agit effectivement d'un spam. D'où l'expression de faux-négatif.
[4] Un faux-positif est un élément qui ne devrait pas être bloqué mais qui l'est en pratique par le filtre, car ce dernier le note comme étant positif. Puisque ce résultat positif est incorrect, on parle de faux-positif.

Toutefois, ces problèmes peuvent devenir plus prononcés et avoir des conséquences plus importantes lorsque les systèmes de filtrage sont appliqués au réseau Internet public et imposés à l'ensemble des internautes sur un territoire donné. Ils constituent dès lors une problématique significative pour la société, considérée dans son ensemble. Puisque le contrôle ou le débat public entourant la mise en œuvre de ces systèmes est souvent réduit à son minimum, lorsqu'il n'est pas en outre inadapté, et que cette mise en œuvre a lieu sans la permission directe des utilisateurs des services Internet concernés, il est nécessaire que ces systèmes soient conçus, développés, gérés, mis en œuvre et audités d'une manière bien plus transparente et responsable.

Internet peut être filtré de différentes manières. Le filtrage personnel et le filtrage sur réseau sont les deux principales méthodes de filtrage à être pratiquées quotidiennement. Il existe également des hybrides de ces deux méthodes.

Le filtrage mis en œuvre au niveau de l'utilisateur final permet de décider des types de contenus qui seront filtrés, sur la base de critères propres à chaque utilisateur. Il peut être adapté et configuré différemment pour répondre aux besoins de plusieurs catégories d'utilisateurs (parents, enfants, enseignants, étudiants, etc.). Ce type de filtrage est le plus précis, mais il n'empêche pas les utilisateurs d'accéder aux contenus qu'ils choisissent de voir ou de télécharger, même si ces contenus sont potentiellement illégaux.

En cas de filtrage d'Internet placé sur le réseau, le prestataire de service (fournisseur d'accès à Internet, employeur, club, etc.) peut déterminer les types de contenus ou d'activités à filtrer pour TOUS les utilisateurs de ce service, à tout le moins s'agissant des contenus directement accessibles par l'intermédiaire de son équipement réseau, sur lequel est mise en œuvre la mesure de filtrage (parfois, le système peut être configuré pour décider des critères de filtrage en fonction d'utilisateurs identifiés).

Deux problématiques clefs doivent être débattues dans le cadre d'une réflexion sur le filtrage d'Internet :

- Comment spécifions-nous techniquement ce qu'il convient de filtrer ?

  Les processus qui collectent, examinent, évaluent et cataloguent les contenus, afin d'identifier ceux d'entre eux qui devraient être bloqués, sont complexes et consommateurs de ressources. Ces processus doivent être développés, testés et mis en œuvre, et le personnel qu'ils requièrent doit être identifié et entraîné.

  - L'utilisation de listes noires (« *block lists* ») constitue la stratégie de filtrage la plus commune ;
  - L'identification automatique est à l'étude mais offre des résultats limités ;
  - Les systèmes de classification (« *rating* ») sont disponibles depuis de nombreuses années mais n'ont pas eu le succès escompté.

- Qui devrait choisir ce qui devrait être filtré sur Internet ?
  - Dans les pays où l'autorité judiciaire est indépendante du pouvoir législatif et du pouvoir exécutif, ce qui devrait être le cas dans toutes les démocraties libérales, seul un juge devrait avoir la compétence de constater l'illégalité d'un contenu, d'une situation ou d'une action.
  - Cette situation génère l'un des défis majeurs que doivent relever les systèmes de filtrage d'Internet. Les procédures juridiques actuelles, nationales comme internationales, sont rarement adaptées au traitement des défis transfrontaliers que pose Internet ou de la vitesse de communication des services Internet. En conséquence, la participation de l'autorité judiciaire aux décisions de filtrage est rarement suffisante.

Le réseau international de services d'assistance sur Internet (INHOPE) coordonne un réseau de services d'assistance en ligne (« *hotlines* »). Ces derniers, implantés dans plus de 30 pays,

prennent en charge les signalements de ressources à caractère pédopornographique présentes sur Internet. Ces services d'assistance ont reçu plus de 500 000 signalements en 2005, 850 000 signalements en 2006 et plus d'un million de signalements en 2007, sachant que ces chiffres sont plus élevés chaque année. Les chiffres exacts pour 2008 n'ont pas encore été publiés. Sur le nombre de signalements reçus entre septembre 2004 et décembre 2006, moins de 20% ont été considérés comme illégaux OU préjudiciables, et seul 10% du total a été considéré comme illégal par les services d'assistance en ligne.

Une problématique cruciale concernant les listes de contenus à filtrer ou listes noires (« *blocking lists* ») est leur sécurité et leur intégrité. De telles listes sont extrêmement recherchées par les personnes disposées à en expérimenter le contenu. Même sans compter les listes de contenus qui sont publiées sur Internet à la suite d'indiscrétions, des recherches indiquent qu'il pourrait être possible de faire de l'ingénierie inverse sur les listes utilisées par n'importe quel prestataire de services.

Le filtrage de la pédopornographie sur Internet ne conduit pas à faire cesser les abus sur enfants. Il n'entraîne pas la disparition des images ou leur retrait du réseau. La réponse la plus efficace qui puisse être apportée à la pédopornographie/aux images d'abus sur enfants est le retrait de ces dernières du réseau Internet, accompagné d'investigations pénales concernant le producteur des images et d'initiatives aux fins de retirer l'enfant de la situation abusive où il se trouve, pour lui prodiguer des soins et lui permettre de récupérer dans un environnement sécurisé.

Le filtrage d'Internet rend parfois plus difficile l'accès à ce type de contenus (selon le système de filtrage retenu), en sorte que seules les personnes les plus déterminées et les plus techniquement averties pourront le trouver (en fonction du logiciel client utilisé). Lorsque les images comprennent des informations permettant d'identifier les victimes, leur filtrage peut également protéger ces dernières d'un nouveau sentiment d'exploitation[5].

Malheureusement, certains des contenus illégaux ayant trait à la pédopornographie et étant disponibles sur des sites web sont actuellement hébergés dans des pays et auprès de prestataires d'hébergement dont la législation nationale comme le contrôle et l'intervention politiques ne sont pas comparables aux bonnes pratiques actuelles, au regard des standards internationaux. Les procédures de notification et de retrait (« *notice and take-down* ») des contenus que connaissent ces pays et ces hébergeurs sont également trop peu développées, ou ne fonctionnent pas. Les initiatives destinées à répondre à ces problématiques doivent être encouragées.

Il est important de noter la nature intrusive de nombre de stratégies de filtrage. Ceci est particulièrement vrai des mécanismes les plus précis de filtrage de contenus, qui requièrent l'analyse du contenu échangé entre les utilisateurs. Cette situation est problématique tant en termes d'investissements (les investissements requis sont invariablement élevés, dans ce type de scénarios), que dans le cadre d'une approche plus large, sociétale.

La proportionnalité d'une mesure de filtrage est généralement difficile à évaluer, car elle dépend essentiellement du « but légitime »[6] particulier qu'il s'agit de préserver dans le cadre de chaque situation factuelle, de l'utilité de la mesure pour atteindre ce but légitime dans des circonstances particulières, et des caractéristiques du mécanisme de filtrage comme de l'impact de ces dernières sur les autres droits et libertés.

Les conséquences d'une mesure de filtrage d'Internet, en termes d'ingérence dans l'exercice des libertés fondamentales, sont mises en lumière au chapitre 6 de la présente étude. Toutefois, plusieurs mesures de filtrage peuvent autoriser des ingérences additionnelles, en raison de la nature des mécanismes qui sont utilisés pour les mettre en œuvre.

[5] Ce point est discuté plus en détail au chapitre 6 de la présente étude.
[6] Voir infra, section 7.4.

Toute mesure qui constitue une ingérence dans l'exercice de certaines libertés doit voir sa proportionnalité évaluée, en premier lieu, au regard du but légitime qui lui a été assigné, et, en second lieu, au regard de son effet général, lequel ne doit pas aller au delà de ce qui est nécessaire pour atteindre le but poursuivi et, dans tous les cas, lequel doit « *ménager un certain périmètre* » pour l'exercice de la liberté qui se voit ainsi limitée, et non « *provoquer (l') extinction* » de cette dernière.

Chaque fois qu'une mesure de filtrage est autorisée en raison de son utilité à préserver un intérêt légitime, son fonctionnement le plus basique ne doit pas limiter les autres libertés d'une manière disproportionnée, et certaines garanties doivent être prises afin que cette mesure ne soit pas utilisée d'une manière qui pourrait menacer ces libertés encore plus avant.

Dans tous les cas, il doit être noté qu'aucune des stratégies identifiées dans le présent rapport ne semble être en mesure de prévenir complètement le sur-blocage (ou filtrage excessif). Cette problématique est de première importance lorsqu'il s'agit d'équilibrer, d'une part le besoin de filtrer les contenus à caractère pédopornographique, et d'autre part le besoin de respecter les droits de l'Homme et la libre expression. Il semble inévitable que des contenus légaux soient bloqués, là où le filtrage est mis en œuvre.

En outre, les contenus électroniques peuvent être échangés par l'intermédiaire de différentes technologies Internet. En conséquence, la pratique de n'appliquer le filtrage qu'à un nombre limité de ces technologies (telle que celle de ne filtrer que le trafic en direction des serveurs web) pourrait sans aucun doute conduire à l'utilisation d'une méthode alternative de distribution de ces contenus. Ceux qui ont à l'esprit de distribuer des contenus illégaux par l'intermédiaire d'Internet disposent d'une myriade d'options pour le faire, en dépit des mesures de filtrage mises en place. D'un point de vue technique, les initiatives de filtrage ne peuvent, en conséquence, qu'assurer la protection des personnes qui pourraient accéder aux contenus par inadvertance. Il semble improbable que les stratégies de filtrage, ainsi que nous le montrons dans le présent document, soient en mesure de prévenir efficacement ou de manière substantielle les infractions ou la « revictimisation ».

Les initiatives de filtrage des contenus peuvent être considérées comme un acte de reterritorialisation, lorsque l'objectif d'un pays est de s'assurer que ses normes nationales s'appliquent à l'ensemble du contenu disponible sur Internet, pour les personnes qui utilisent Internet sur son territoire.

Tous les types de filtrage sont différents, tous les types de contenus sont différents, et tous les types d'infractions sont différents.

1.3 Le débat sur le filtrage d'Internet et ses motivations

Le débat relatif au « filtrage d'Internet » ne peut pas être limité à une problématique unique. Ce débat est aussi complexe que le sujet lui-même. Les domaines de préoccupations sont extrêmement divers et les défis auxquels doivent faire face les décideurs politiques, dans le cadre des réponses qu'ils apportent aux problèmes posés par les contenus électroniques, sont complexes.

De nombreuses motivations sous-tendent la croyance (ou dans certains cas, l'espoir) de la société selon laquelle des initiatives de filtrage pourraient résoudre certaines problématiques sociétales majeures, là où les autres approches ne se sont pas révélées très efficaces. De nombreuses entités différentes ont déjà mis en œuvre le filtrage. Une large gamme de contenus est la cible de ces tentatives de filtrage. Ces dernières peuvent elles-mêmes être abordées de diverses manières, selon les personnes qu'elles visent. Plusieurs pays ont d'ores et déjà adopté des systèmes de filtrage d'Internet.

Internet est un réseau de réseaux, vaste et complexe, qui comprend une myriade de systèmes informatiques, de protocoles et de services. La première étape de toute initiative de filtrage est de déterminer l'endroit où, sur Internet, le filtrage peut être tenté. Une deuxième

problématique clef est de déterminer, d'une part, qui choisit ce qui devrait être bloqué, et, d'autre part, quels niveaux de connaissances et de compétences doivent posséder les différents utilisateurs et organisations qui entendent organiser le filtrage de contenus électroniques. Un large éventail de contenus peut être la cause de différents problèmes dans différentes sociétés, et chaque mesure de filtrage doit être accompagnée de la description, tant de la variété des contenus qu'elle cible, que du processus ayant conduit le gouvernement à considérer le filtrage d'Internet comme constituant une solution possible à ces problèmes. Il est important de prendre note des motivations premières qui conduisent les décideurs politiques à envisager le filtrage d'Internet et des raisons pour lesquelles, dans certains cas, des approches alternatives semblent avoir échoué. Une mesure de filtrage cible généralement soit les producteurs, soit les consommateurs de contenus illégaux, et connaît différents niveaux d'efficacité selon le choix qui est fait entre ces deux catégories.

Toutes les approches et les motivations qui sous-tendent les tentatives de filtrage d'Internet doivent être clairement différenciées afin de permettre leur comparaison, au sein de l'éventail complexe qu'elles représentent.

Le premier critère pouvant être utilisé pour différencier les différentes approches qui sous-tendent le filtrage est la cible de l'outil de filtrage. Il existe en général quatre différentes cibles de filtrage, qui correspondent aux approches suivantes :

- L'approche basée sur le service, par exemple la messagerie électronique ;
- L'approche basée sur le contenu, par exemple les discours haineux, la pédopornographie, les sites de jeux d'argent ;
- L'approche basée sur l'utilisateur, par exemple les utilisateurs téléchargeant de la musique illégale ou envoyant du spam ;
- L'approche basée sur les moteurs de recherche, par exemple pour empêcher l'affichage des résultats de recherche concernant des sites web illégaux.

Un second critère pouvant être utilisé pour différencier les différentes approches qui sous-tendent le filtrage d'Internet est la qualité du responsable de la prise de décision concernant le sort des contenus illégaux. Le responsable de la prise de décision est la personne ou l'institution qui prend la décision relative à ***ce qui*** devrait être filtré.

- Décision individuelle ;
- Décision institutionnelle ;
- Législateur / Cour ou tribunal.

Le filtrage d'Internet est considéré comme étant la solution technique à apporter à un éventail étendu d'activités illégales. Dans une large mesure – mais ce n'est pas toujours le cas – ces activités font l'objet d'incriminations pénales dans le pays qui entend mettre en œuvre ou qui a déjà mis en œuvre la technologie de filtrage. Elles ne sont toutefois pas toujours appréhendées par la loi de la même manière, dans le pays d'hébergement des contenus litigieux. La pédopornographie relève de ces catégories de contenus qui, concernés par le filtrage, font l'objet de dispositions pénales.

L'application de la loi est difficile sur Internet, en ce que les contenus sont souvent mis légalement à disposition depuis des serveurs qui se trouvent hors du pays concerné. Cette difficulté est une conséquence directe de l'hétérogénéité des différentes normes nationales qui réglementent la publication de contenus électroniques. La tentative de filtrage visant un contenu qui est légalement mis à disposition hors d'un pays, mais qui est considéré comme illégal à l'intérieur de ce même pays, pourrait être vue comme une option permettant à ce dernier d'œuvrer au maintien de ses propres standards culturels, dans une situation d'accès global.

Les autres contenus pouvant être la cible d'une mesure de filtrage incluent :

- Le spam – les organisations de prestataires de messagerie électronique signalent qu'au moins 85 à 90 pour cent de l'ensemble des messages électroniques envoyés sont actuellement des spams. La plupart des mesures de filtrage sont en la matière mises en œuvre avec le consentement de l'utilisateur.

- Les contenus érotiques et pornographiques – souvent pris en considération par les décideurs politiques dans le contexte de la prévention de l'accès des mineurs aux contenus considérés comme préjudiciables. Dans certains pays, *des « systèmes de vérification de l'âge adulte »* (« *adult verification systems* ») ont été développés pour prévenir l'accès des mineurs à des sites réservés aux adultes. D'autres pays font tomber sous le coup de la loi pénale tout échange de pornographie, même entre adultes.

- La pédopornographie – qui est universellement condamnée et qui est largement reconnue comme étant une infraction pénale. Malgré les efforts et les coûts considérables qu'elles ont impliqués, les initiatives visant à contrôler la distribution en réseau de contenus à caractère pédopornographique ont démontré n'avoir eu que peu d'effet dissuasif sur les auteurs d'infractions.

- Les sujets politiques controversés / les discours haineux / la xénophobie – certains pays répriment pénalement la publication de contenus de haine raciale, violents ou xénophobes, tandis que de tels contenus peuvent être légalement publiés dans d'autres pays qui garantissent une forte protection de la liberté d'expression, comme les Etats-Unis.

- Les jeux d'argent illégaux – Internet permet aux personnes de contourner les restrictions liées aux jeux d'argent. Les casinos en ligne y sont largement accessibles, la plupart d'entre eux étant hébergés dans des pays dont la réglementation concernant les jeux d'argent sur Internet est libérale, voire inexistante.

- La diffamation et la publication de fausses informations – les sites web peuvent afficher des informations fausses ou diffamatoires, particulièrement dans les forums et les salles de discussion, lorsque les messages qui y sont postés par les utilisateurs ne sont pas vérifiés par un modérateur.

- Les contenus publiés par des organisations terroristes – la publication de messages de propagande et d'informations relatives à la commission d'infractions est commune.

- La violation de droits d'auteur – elle inclut l'échange de musiques, de fichiers et de logiciels protégés par un droit d'auteur, par l'intermédiaire de systèmes de partage de fichiers, et le contournement des systèmes de gestion des droits numériques (« *Digital Rights Management* »). Les technologies permettant le pair à pair (« *Peer-to-Peer* », P2P) jouent toutefois un rôle essentiel sur Internet.

Pourquoi envisager de filtrer Internet ?

- Le manque d'instruments de contrôle sur Internet

  Internet a originellement été conçu sur la base d'une architecture réseau décentralisée, réagissant aux pannes et aux perturbations. En conséquence, Internet est résistant aux tentatives extérieures de contrôle. Des initiatives de filtrage pourraient être considérées comme un moyen d'implémenter les instruments, qui n'ont pas été prévus dans le cadre du développement du réseau, permettant de tels contrôles.

- La dimension internationale

  La coopération internationale, basée sur les principes de la traditionnelle assistance juridique mutuelle, est souvent très lente et consommatrice de temps. Les exigences de

forme et le temps nécessaires à la collaboration avec les autorités en charge de l'application de la loi à l'étranger entravent souvent les investigations. Le filtrage d'Internet pourrait dès lors être considéré comme une manière d'agir, même dans ce type de cas où les limites de l'actuelle coopération internationale empêchent que des mesures soient prises en un laps de temps approprié.

- L'importance décroissante de l'infrastructure nationale d'hébergement

  La publication d'un contenu peut s'avérer parfaitement conforme à la loi dans un pays, et constituer une infraction pénale dans un autre pays. Les tentatives de filtrage de contenus peuvent dès lors être considérées comme des actes de reterritorialisation, lorsque l'objectif d'un pays est de s'assurer que ses normes nationales s'appliquent à l'ensemble du contenu disponible sur Internet, pour les personnes qui utilisent Internet sur son territoire.

Qui filtrer ?

Le filtrage de contenus Internet illégaux peut être vu non seulement comme un instrument dirigé contre les personnes qui sont responsables de la mise en ligne de ces contenus (les producteurs), mais également comme un outil visant à empêcher les utilisateurs de télécharger des contenus illégaux (les consommateurs).

- Le producteur des contenus illégaux – le fournisseur de contenus illégaux

  Internet est devenu un outil majeur de distribution de contenus à caractère pédopornographique, en ce qu'il offre un certain nombre d'avantages aux auteurs d'infractions, avantages qui rendent les investigations difficiles. De manière analogue, les appareils photo et les caméscopes numériques modernes sont devenus les premiers outils de production de pédopornographie.

  Les raisons présidant à la mise en œuvre des technologies de filtrage sont donc ici les mêmes que celles qui justifient l'incrimination pénale de l'échange de pédopornographie, à savoir la réduction du volume des crimes et délits, et la protection des enfants.

- Le consommateur de contenus illégaux

  En plus de prohiber la production, la publication et la mise à disposition de pédopornographie, un nombre significatif de pays incriminent pénalement la possession de pédopornographie. La demande de tels contenus pourrait favoriser leur production de manière suivie. Par ailleurs, un certain nombre de pays vont au delà de l'incrimination de la possession de pédopornographie, en incriminant également l'action ***d'accéder*** à des contenus à caractère pédopornographique.

Alors même que le filtrage d'Internet ne permet *pas* de retirer les contenus à leur source et que cette circonstance fait obstacle à la possibilité, pour la mesure, de prévenir les infractions de mise en ligne de tels contenus, cette même mesure, lorsqu'elle est techniquement efficace, a le **potentiel de prévenir les infractions commises par certains utilisateurs, qui tentent d'accéder à un site web, soit pour visualiser, soit pour télécharger, un contenu à caractère pédopornographique**. Le succès de cette prévention dépend de l'efficacité des technologies de filtrage mises en place et du niveau de motivation et de connaissances de l'utilisateur.

Les problèmes principaux que pose le filtrage sont l'absence de retrait du contenu à sa source et les nombreuses possibilités de contourner la mesure. Ces aspects ont différentes conséquences :

- Le contenu est toujours accessible par l'intermédiaire d'une connexion qui n'est pas soumise à la mesure de filtrage ;

- Dès lors que les technologies de filtrage sont développées et mises en œuvre, elles peuvent être utilisées dans d'autres objectifs. La raison principale de cette inquiétude est l'absence de transparence qui entoure la mise en œuvre de ce type de technologies ;
- Le fait que le contenu ne soit pas supprimé permet aux utilisateurs de rechercher la manière d'y accéder en contournant les solutions techniques de protection ;
- Il existe plusieurs manières de contourner les mesures de filtrage qui sont actuellement en discussion ;
- Le fait que les contenus ne soient pas supprimés suggère à l'utilisateur qu'il s'agit de sites web auxquels il peut accéder en toute confiance, puisque les autorités ont clairement échoué dans leurs tentatives de les faire supprimer et de diligenter des investigations à leur sujet ;
- Les échanges de pédopornographie par l'intermédiaire de systèmes de partage de fichiers ou de messages électroniques chiffrés ne sont pas couverts par les approches actuelles concernant le filtrage du web ;
- Le fait de rendre invisibles de tels contenus pourrait dévoyer le débat politique, puisqu'il pourrait créer l'impression selon laquelle le problème de la pédopornographie en ligne a reçu une réponse adaptée, et par là même réduire les inquiétudes de la société civile en la matière.

Outre les limites systémiques que rencontrent les approches relatives au filtrage, des problématiques techniques et juridiques doivent être prises en considération.

Autres approches non basées sur le filtrage :

- Améliorer les moyens alloués à la coopération internationale, afin de réduire le laps de temps qui sépare l'identification d'un contenu illégal hébergé à l'étranger et le retrait de celui-ci ;
- Travailler au retrait de ce type de contenus pour empêcher les délinquants chevronnés d'y avoir accès ;
- Enquêter sur les images à caractère pédopornographique pour assurer l'identification des victimes qui y figurent et leur retrait de la situation abusive où elles se trouvent.

Plusieurs pays européens tels que la Finlande, la Norvège, la Suède, la Suisse, le Royaume-Uni et l'Italie, de même que des pays non européens tels que l'Australie, la Chine, l'Iran et la Thaïlande, pratiquent le filtrage d'Internet. Les approches techniques, l'objectif du filtrage, de même que le degré de participation de l'industrie, y sont variables.

En Australie, par exemple, une liste noire (« *block-list* ») générée par l'Autorité australienne des communications et des médias (ACMA), devra vraisemblablement être utilisée obligatoirement par tous les fournisseurs d'accès à Internet (FAI). Au royaume-Uni, la liste noire est générée par l'IWF (Internet Watch Foundation). La technologie utilisée est BT Cleanfeed, autrement dit une technologie basée sur le filtrage d'URL. Au Danemark, la liste noire est générée par le Centre national de lutte contre la criminalité liée aux nouvelles technologies (« *National High Tech Crime Centre* ») de la police nationale danoise, et par le service d'assistance en ligne « Save the Children Denmark ». En Finlande, le filtrage était initialement basé sur une liste de domaines fournie par la police finlandaise. La plupart des FAI de ce pays participent aujourd'hui à l'opération, sur la base d'un blocage DNS.

1.4 Aspects techniques du filtrage d'Internet

Le développement et la mise en œuvre de différentes technologies de filtrage, sur Internet, sont loin d'être une nouveauté. Le spam, les virus et logiciels malveillants provenant d'Internet, à l'instar de nombreux autres contenus qui ne sont ni souhaités, ni sollicités par

les utilisateurs finaux, ont été pendant longtemps la cible des efforts de filtrage entrepris par l'industrie, pour des raisons de sécurité et d'utilisabilité, ou par l'Etat, dans le cadre de son rôle d'élaboration et de mise en application des lois et politiques.

Un panorama des principaux systèmes de filtrage d'Internet utilisés aujourd'hui est essentiel, de même qu'une analyse de la manière dont ces derniers sont appliqués à différents services Internet. Ces systèmes ont par ailleurs des impacts techniques et suscitent de vraies questions. Il existe également de nombreuses manières de les contourner, ce qui nous conduira à une analyse de leur efficacité, laquelle génère plusieurs inquiétudes.

Les Etats démocratiques ont promu l'usage de technologies de filtrage d'Internet dans différents domaines. Ils ont invoqué l'intérêt général pour requérir la mise en œuvre de certaines mesures de filtrage, en vue d'assurer le respect de divers aspects de leur politique publique, dans un contexte où les caractéristiques d'Internet rendaient l'application de la loi difficile (au niveau international). De manière analogue, certains Etats, au régime moins ouvert sur l'information, utilisent le filtrage comme une ressource technique qui leur permet d'étendre leur pratique du contrôle de l'information aux médias électroniques.

Tous ces développements s'articulent autour de la disponibilité de technologies de filtrage d'Internet. En fonction de leurs caractéristiques techniques, ces technologies peuvent s'avérer plus ou moins efficaces ou contournables. Les techniques de filtrage des contenus à caractère pédopornographique sont l'objet principal de la présente étude, mais il est important de noter qu'un grand nombre de ces technologies peuvent être utilisées pour filtrer d'autres types de contenus ou d'activités, sans investissements supplémentaires significatifs.

L'identification du contenu

La mise en œuvre d'une décision de filtrage requiert la présence d'identificateurs de contenus. Les contenus sur lesquels se concentre le présent rapport sont généralement de nature visuelle, ce qui signifie qu'ils contiennent soit des images, soit des séquences vidéo, d'abus sexuels sur enfants.

- Les adresses IP
- Les noms de domaine et les DNS
- Les URL
- Le nom et le contenu des fichiers
- Les mots-clefs
- Les signatures de contenu (valeurs de hachage)

La mesure de l'efficacité

1. Il n'est pas possible d'évaluer cette efficacité **en comparant la quantité de ressources qui se trouvent correctement filtrées à la quantité totale de ressources disponibles**, puisque le volume total des contenus illégaux disponibles n'est pas connu.
2. Puisque l'origine des requêtes (« *hits* ») adressées à un site web est souvent incertaine, **les statistiques de volumétrie des requêtes dirigées vers les contenus que filtre une liste donnée constituent un indicateur très rudimentaire**, au mieux.
3. L'analyse du **potentiel** que présente la mesure en termes **de sur-blocage (ou filtrage excessif) et de sous-blocage (ou filtrage insuffisant)** peut être utilisée comme indicateur de l'efficacité des technologies de filtrage d'Internet.
4. Un autre indicateur d'efficacité est la **facilité de contourner le filtrage**. S'il est facile de contourner ou de désactiver une mesure de filtrage, cette dernière n'a a priori pas d'effet sur la disponibilité de la ressource bloquée.

5. **La disponibilité de méthodes alternatives d'accès au même contenu**, quelles que soient ces méthodes, peut être considérée comme un élément de mesure de l'efficacité du filtrage, en l'absence de données plus précises.

6. **La disponibilité d'autres méthodes de régulation**, qui seraient plus efficaces pour prévenir l'accès aux ressources concernées, est également à évaluer – spécialement si ces méthodes sont moins coûteuses, moins intrusives ou plus efficaces quant à la diminution de la disponibilité de la ressource.

Les caractéristiques des stratégies de filtrage

- **Liste blanche (« *allow-list* ») versus liste noire (« *block-list* »)** - Les filtres qui sont configurés par défaut pour « autoriser » tous les contenus à l'exception de ceux qui sont définis dans une liste spécifique sont communément considérés comme ayant recours à une « liste noire » (« *block-list* »). Les filtres qui sont configurés par défaut pour bloquer l'ensemble des contenus à l'exception de ceux qui sont spécifiquement définis dans une liste sont considérés comme ayant recours à une « liste blanche » (« *allow-list* »).
- **Intervention humaine (filtrage dynamique ou manuel)** - Typiquement, les filtrages mis en place pour lutter contre la pédopornographie se basent sur les signalements des utilisateurs et sur les investigations menées par les services en charge de l'application de la loi. Les contenus du filtre sont généralement sélectionnés manuellement, chacun d'entre eux étant vérifié et confronté aux critères de la liste noire (« *block-list* ») par l'administrateur de cette liste. D'un autre côté, beaucoup de filtres, comme ceux des anti-spam et de certains antivirus, utilisent souvent des critères prédéfinis pour bloquer le contenu sans aucune intervention humaine. Ces critères peuvent être complexes et avoir des facettes multiples.
- **Point de filtrage** - Les stratégies de filtrage peuvent être différenciées en fonction de l'endroit où elles sont mises en œuvre sur le réseau. Les filtres pour postes clients, qui se trouvent placés au niveau de l'utilisateur, permettent aux parents et aux administrateurs de l'ordinateur de sélectionner et de bloquer certains types de contenus. D'autres techniques de filtrage sont utilisées à l'échelle d'une entreprise, d'un FAI, voire d'un pays. Elles requièrent typiquement que les flux soient envoyés en amont vers des machines centrales, chargées d'analyser le trafic.

Niveau de détail ou de spécificité

- **Adresses IP** – Le filtrage d'une *adresse IP* implique que tous les autres services et utilisateurs qui partagent cette adresse IP seront également bloqués.
- **Noms de domaine** - Le filtrage d'un nom de domaine bloquera ***la totalité*** du contenu résidant derrière ce nom de domaine.
- **Les URL (« *Uniform Resource Locators* »)** – De meilleurs résultats en termes de précision seront obtenus en utilisant un filtrage basé sur l'URL. En raison de la facilité qu'il y a à contourner ce type de filtrage, le mettre en place peut conduire à un risque significatif de sous-blocage (ou filtrage insuffisant).
- **Les signatures de contenus** - Les ressources Internet peuvent être classifiées et filtrées en utilisant les signatures de contenus qui ont été préalablement catégorisés comme étant illégaux. De nouveaux contenus peuvent être facilement ignorés par le filtre. Le chiffrement des contenus rendra cette méthode de filtrage totalement inopérante.
- **Les mots-clefs** - Il s'agit d'un filtrage basé sur les mots-clefs trouvés dans le nom de fichier, dans l'URL ou dans le texte de la ressource à laquelle un utilisateur souhaite accéder. Il est dans ce cas nécessaire de procéder à une analyse complexe des mots-clefs qui se trouvent ainsi reconnus, par rapport au contexte de leur utilisation.

Les méthodes de distribution de ressources à caractère pédopornographique sur Internet

Les ressources à caractère pédopornographique peuvent être distribuées sur Internet par diverses méthodes, grâce aux connexions Internet à haut-débit. En plus de permettre la diffusion de contenus statiques (autrement dit de photos ou de vidéos), les connexions haut-débit servent également de tremplin pour des comportements tels que *la sollicitation d'enfants à des fins sexuelles* (« *grooming* ») ou *le cyber harcèlement ou cyber intimidation* (« *cyber bullying* »). L'usage croissant des réseaux sociaux a contribué de manière importante au développement de ces activités.

- Les sites web

  Les sites web sont l'un des moyens les plus utilisés pour distribuer des contenus sur Internet. Habituellement, le contenu web est stocké sur le disque dur d'un serveur. Mais il est également possible que ce contenu soit récupéré ou créé dynamiquement, souvent au moyen d'une base de données qui contient les informations nécessaires à cette opération. Il est fréquent que divers serveurs web, gérés par des propriétaires différents, soient associés à une seule et même adresse IP.

- La messagerie électronique et le spam (messages non sollicités)

  La messagerie électronique reste le service le plus utilisé sur Internet, bien plus encore que le web ou les réseaux sociaux.

- Les groupes de news (« *newsgroups* ») du réseau Usenet

  La différence majeure qui existe entre les groupes de news et la messagerie électronique est que les flux de messages qui circulent entre les serveurs Usenet (souvent appelés « *newsfeeds* », pour « distribution de nouvelles » ou « distribution d'articles Usenet »), sont organisés sous forme de groupes, dont le nom suggère le contenu des messages qui y sont échangés.

- Les réseaux de pair à pair (« *Peer-to-Peer* » ou P2P)

  Le partage de fichiers de pair à pair est basé sur des échanges directs de fichiers entre les ordinateurs des utilisateurs finaux, sans passer par un serveur intermédiaire. Bien que cette technologie connaisse des usages légitimes, elle se prête très bien au partage sans droits de fichiers musicaux ou de films, générant ainsi des problématiques majeures pour les titulaires de droits d'auteur.

- Les moteurs de recherche

  En indexant le contenu des sites web, ces services sont capables d'identifier les contenus pertinents grâce à des recherches par mots-clefs et à des algorithmes de recherche complexes.

- La messagerie instantanée (« *IM* ») et autres outils

  Un autre outil important à être utilisé dans le cadre d'échanges de ressources à caractère pédopornographique est la messagerie instantanée. Le canal de messagerie instantanée sert plus à la mise en relation et à la sécurisation de l'échange de ressources, tandis que ce dernier échange a lieu directement par l'intermédiaire d'autres technologies.

Les stratégies de filtrage et leur efficacité

- Le filtrage de sites web

  Il est généralement procédé au filtrage des sites web en utilisant l'un des deux identificateurs suivants :

- Le serveur qui contient le contenu du site web pourrait être bloqué au niveau de son adresse IP, empêchant dès lors toute personne qui se verrait appliquer le filtre d'accéder à cette même adresse. La liste noire ne contiendrait, dans cette situation, que les adresses IP de contenus identifiés comme étant illégaux ;
- Une mesure de filtrage peut être basée sur le nom de domaine, voire sur l'URL spécifique d'une page ou d'un fichier qui se trouve hébergé sur un site web.

Si ce type de filtrage est mis en place au niveau du réseau d'accès et non pas sur l'équipement de l'utilisateur, ce dernier aura alors, toutes proportions gardées, plus de mal à le contourner, car il lui sera nécessaire d'avoir un minimum de connaissances sur le fonctionnement d'Internet.

- Le filtrage de la messagerie électronique (« *Email Blocking* »)

  La plupart des filtres de messagerie électronique sont situés sur les serveurs de messagerie **entrante**, qui reçoivent les messages électroniques à destination de leurs utilisateurs, ou sur des serveurs positionnés juste devant eux sur le réseau. Il existe deux manières de procéder à un filtrage de la messagerie électronique :

  - Des filtres basés sur les connexions peuvent comparer l'adresse IP du serveur expéditeur des messages aux adresses qui sont listées dans un certain nombre de listes noires ;
  - Des filtres peuvent s'attacher au contenu des messages, afin de filtrer ceux dont la nature n'est pas souhaitée.

  Une possibilité de sur-blocage (ou filtrage excessif) existe, lorsque sont bloqués des adresses IP, voire des serveurs entiers de messagerie expéditeurs, en raison d'incidents liés à des contenus à caractère pédopornographique.

- Le filtrage des contenus sur le réseau Usenet

  Les tentatives de filtrage de contenus sur Usenet sont traditionnellement opérées en bloquant l'accès à des sous-parties d'un groupe ou en refusant d'héberger un groupe de news en particulier. Les fournisseurs d'accès à Internet ont pu observer que, lorsqu'ils sont privés d'accès à des arborescences suspectes, les utilisateurs ont tendance à déplacer leurs contenus illégaux vers des groupes dont le nom est moins explicite, ce qui conduit à un plus grand nombre d'incidents, en termes d'accès involontaire à des ressources illégales.

- Le filtrage des résultats des moteurs de recherche

  Il est possible de prévenir l'accès à des résultats de moteurs de recherche, au niveau des prestataires de ces moteurs. Une question importante est celle de la visibilité qui est donnée à de telles initiatives de filtrage. Certains prestataires informent clairement de leur politique en matière de filtrage des résultats, tandis que d'autres ne le font pas. Le contournement de ce type de filtrage est facile : il suffit d'accéder directement au contenu.

- Le filtrage du pair à pair (« *peer-to-peer* » ou P2P) et de la messagerie instantanée (« *IM* »)

  Tenter de filtrer le trafic pair à pair est une tâche difficile. Beaucoup de protocoles P2P sont distribués – ce qui signifie que les fichiers y sont téléchargés par fragments provenant de plusieurs sources et qu'aucun des flux de données ne contient l'intégralité du fichier.

  - La première option permettant le filtrage des contenus sur un réseau P2P consiste à analyser ces contenus en se comportant comme un utilisateur du service. En émettant une requête pour certains fichiers, ou en surveillant les requêtes et les réponses qui leur sont apportées par d'autres utilisateurs, il est possible de trouver des utilisateurs ayant une partie d'un fichier donné sur leur disque dur. Bloquer

l'accès à leur adresse IP ou déconnecter ces utilisateurs, pour le cas où une telle initiative serait juridiquement et techniquement possible, est toutefois le seul remède disponible, extrême ;

- La deuxième option permettant de filtrer les contenus sur ces réseaux, avec un maximum d'efficacité, consiste à utiliser une technologie apparentée à celles qui permettent l'analyse approfondie des paquets (« *Deep Packet Inspection* » ou DPI), autrement dit du trafic réseau, pour reconnaître les fichiers échangés pendant le temps de leur échange.

Vue d'ensemble

Le tableau ci-dessous liste les caractéristiques de chacune des stratégies de filtrage qui ont été abordées jusqu'à présent. Il montre les risques que présentent ces dernières, selon nos estimations, en termes de sur-blocage (ou filtrage excessif) et de sous-blocage (ou filtrage insuffisant). Il fait état des ressources nécessaires à l'exécution de chaque stratégie de filtrage, des différents types de listes noires (« *block-lists* ») et des efforts de maintenance qui sont nécessaires pour chacune de ces listes. Dans sa dernière colonne, il indique pour chaque stratégie si le contenu des communications doit être analysé de manière approfondie (avec une technologie DPI, autrement dit d'inspection approfondie des paquets, ou une technologie équivalente), pour que le filtrage soit efficace.

Média	**Filtrage**	**Efficacité**				**Liste noire (« *Blocklist* »)**		**DPI**
		SUR-blocage (ou filtrage EXCESSIF)	*SOUS-blocage (ou filtrage INSUFFISANT)*	*Ressources requises*	*Contournement*	*Effort de maintenance*	*Identificateur*	
Web	*DNS*	TRÈS PROBABLE	PROBABLE	FAIBLES	FACILE	MOYEN	Nom de domaine	-
	Domaine	TRÈS PROBABLE	PROBABLE	MOYENNES	MOYEN	MOYEN	Adresse IP du nom de domaine	-
	URL	PEU PROBABLE	TRÈS PROBABLE	MOYENNES	MOYEN	ÉLEVÉ	URL	+
	IP	TRÈS PROBABLE	PROBABLE	FAIBLES	MOYEN	MOYEN	Adresse IP	-
	Dynamique	TRÈS PROBABLE	TRÈS PROBABLE	ÉLEVÉES	MOYEN	FAIBLE	Mots-clefs, technologie de reconnaissance d'image et autres	+
	Signatures	PEU PROBABLE	TRÈS PROBABLE	ÉLEVÉES	MOYEN	ÉLEVÉ	Hachage	+
	Hybride (IP+signature /URL)	PEU PROBABLE	TRÈS PROBABLE	MOYENNES	MOYEN	ÉLEVÉ	IP et hachage ou URL	+
E-mail	*Dynamique*	PROBABLE	PROBABLE	MOYENNES	DIFFICILE	FAIBLE	Mots-clefs ou autres	-
	URL	PROBABLE	PROBABLE	MOYENNES	DIFFICILE	ÉLEVÉ	URL	-
	Adresse IP	TRÈS PROBABLE	PROBABLE	MOYENNES	DIFFICILE	ÉLEVÉ	Adresse IP	-
	Signatures	PEU PROBABLE	PROBABLE	ÉLEVÉES	DIFFICILE	ÉLEVÉ	Hachage	+
Usenet	*Par groupe*	PROBABLE	PROBABLE	FAIBLES	FACILE	FAIBLE	Nom du groupe	-
	Par hiérarchie	TRÈS PROBABLE	PEU PROBABLE	FAIBLES	FACILE	FAIBLE	Hiérarchie du groupe	-
Moteur de recherche	*Mot-clef*	TRÈS PROBABLE	TRÈS PROBABLE	ÉLEVÉES	FACILE	MOYEN	Mots-clefs	-
P2P	*Par protocole*	TRÈS PROBABLE	PEU PROBABLE	MOYENNES	DIFFICILE	FAIBLE	Reconnaissance de protocole	+
	Par fichier (signature)	PEU PROBABLE	TRÈS PROBABLE	ÉLEVÉES	DIFFICILE	ÉLEVÉ	Hachage	+
	Par fichier (dynamique)	PROBABLE	TRÈS PROBABLE	TRÈS ÉLEVÉES	DIFFICILE	FAIBLE	Algorithmes évolués	+

Bien que les méthodes de distribution puissent varier, chacune d'entre elles peut se substituer aux autres. Indépendamment de l'efficacité du filtrage d'un contenu sur un média, toute

faiblesse que rencontrerait une mesure de filtrage appliquée au même contenu sur un autre média conduirait probablement à un changement de la méthode de distribution de ce contenu.

La majorité des activités liées à la pédopornographie, sur Internet, fait aujourd'hui intervenir de multiples services et systèmes électroniques. Dans le cadre de plusieurs affaires ayant fait l'objet d'investigations, le contact entre un adulte et un enfant avait été initié dans des salons publics de discussion, puis s'était déplacé vers des salons privés de discussion, pour continuer sa progression par l'intermédiaire de messages électroniques et de textes SMS (« *Short Messaging Service* ») échangés sur les réseaux mobiles. Le rendez-vous physique final y avait été arrangé par la voie d'appels personnels sur téléphone mobile. Mener une enquête sur de telles activités est une réelle gageure et exige de la part des enquêteurs une connaissance très large de tous les aspects des technologies Internet et des télécommunications.

Contourner le filtrage d'Internet

- Les serveurs proxy

  Contourner une mesure de filtrage de l'accès mise en place au niveau de serveurs proxy est très facile. L'utilisateur peut procéder directement à ce contournement en demandant à un serveur proxy externe d'accéder pour lui au contenu filtré. Il pourra ainsi accéder au site concerné en se libérant des contraintes du filtrage local, aussi longtemps que ce serveur proxy externe ne fera pas lui-même l'objet d'une mesure de filtrage.

- La tunnellisation (« *tunnelling* »)

  Les logiciels de tunnelisation permettent aux utilisateurs de créer un « tunnel » chiffré vers une autre machine située sur Internet, laquelle empêche le système de filtrage de voir passer les requêtes web. Une fois que le tunnel est créé vers l'autre machine, toutes les requêtes Internet passent dans ce tunnel, puis à travers la machine qui est à l'autre bout du tunnel, laquelle sert de relais vers Internet.

- Le changement d'hébergement ou d'URL

  Pour une personne qui publie un contenu, modifier la configuration de son site web pour que ce dernier soit hébergé à une autre adresse (sous un autre nom de domaine, une autre URL ou même une autre adresse IP) est également très facile, et permet effectivement de contourner une mesure de filtrage qui aurait pour cible les adresses IP, les URL ou les noms de domaine.

- Les réseaux de zombies (« *botnets* »)

  La technologie botnet est souvent utilisée à des fins de changements fréquents de nom de domaine (« *domain name rotation* ») ou de dissimulation d'adresse IP. Les machines compromises d'utilisateurs innocents y sont utilisées comme des portails sur le contenu d'un serveur web. En quelque sorte, l'ordinateur de ces utilisateurs est transformé en un serveur proxy simple, c'est-à-dire sans cache.

- Le contournement du filtrage DNS

  Le filtrage effectué au niveau des requêtes DNS est encore plus facile à contourner. Il suffit simplement de changer la configuration de son ordinateur pour utiliser un autre serveur DNS que celui de son FAI (autrement dit un serveur n'incorporant pas le système de filtrage), pour contourner totalement cette méthode de filtrage.

Lorsque le filtrage est réalisé sur tout autre élément qu'une URL complète (laquelle correspond au chemin d'accès complet) ou qu'une signature de contenu, il existe un risque significatif de sur-blocage (ou filtrage excessif). Inversement, le filtrage d'URL ou de signatures de contenus présente un risque significatif de sous-blocage (ou filtrage insuffisant).

Un filtrage efficace du trafic web (autrement dit un filtrage de l'accès de l'utilisateur au contenu lui-même, et pas simplement une mesure utilisant un filtre DNS) requiert des

investissements significatifs dans une infrastructure de proxy à inspection approfondie des paquets et l'interception à grande échelle de l'ensemble des communications Internet.

Les filtres peuvent également procurer des informations utiles aux personnes qui opèrent des sites web à caractère pédopornographique. Si le site qu'elles opèrent a été intégré à une liste noire (« *blocking list* »), elles savent dès lors que leur site web a été identifié par les autorités et qu'il est donc hautement probable qu'elles fassent l'objet d'une enquête et d'une surveillance par les services en charge de l'application de la loi.

- Ces personnes peuvent prendre des mesures pour détruire toutes preuves ET pour relocaliser leurs services n'importe où ailleurs dans le monde ;
- Elles peuvent également tester leurs technologies de dissimulation face au système de détection, pour identifier les techniques qui leur procurent la protection la plus longue contre la détection et le filtrage ;
- Les activités de filtrage peuvent encore perturber l'activité des personnes qui accèdent à de tels sites web, en forçant les opérateurs de ces sites à relocaliser fréquemment leurs contenus. Ces mouvements peuvent également être suivis et dès lors fournir des renseignements utiles aux enquêteurs, ainsi que des informations utiles à la recherche.

L'évasion constante des mesures de filtrage et le maintien parallèle d'un anonymat implique des ressources et des efforts qui ne devraient pas être sous-estimés. Il est probable que cette situation conduise rapidement à la commission d'erreurs. Toutefois, il est important de noter que les ressources et les efforts nécessaires à la création et à la maintenance d'un système de filtrage d'Internet sont tout aussi significatifs, spécialement lorsqu'il s'agit de répondre en permanence à des activités d'évasion.

Implications dans une société démocratique

- Les problématiques de sécurité

  L'infrastructure qui est requise pour exécuter une stratégie de filtrage peut interférer avec de nombreux éléments critiques de la connexion Internet des utilisateurs finaux. En outre, le contenu des listes noires (« *block-lists* ») présente un intérêt particulier pour les pédophiles. Ces derniers sont particulièrement motivés pour utiliser ces listes dans un dessin opposé à celui qui a présidé à leur conception.

- Sur-blocage (« *over-blocking* ») et sous-blocage (« *under-blocking* »)

  Aucune des stratégies identifiées dans le présent rapport ne semble capable de prévenir le sur-blocage (ou filtrage excessif). Cette situation constitue une préoccupation majeure, lorsqu'il s'agit de mettre en équilibre le besoin de protéger les enfants, d'une part, et le besoin de préserver les droits de l'Homme et les libertés, d'autre part. Il semble inévitable que des contenus conformes à la loi soient bloqués, là où le filtrage est mis en œuvre. Le sous-blocage (ou filtrage insuffisant) est également un phénomène universel, particulièrement présent dans les stratégies de filtrage les plus précises et les plus proportionnées.

- Les risques de dérives et la reterritorialisation

  Un grand nombre de stratégies de filtrage sont très intrusives dans les communications électroniques. Les mécanismes de filtrage de contenus les plus précis requièrent une analyse du contenu de la ressource qui est échangée entre les utilisateurs.

Il est important qu'un débat public prenne place et que celui-ci tienne compte des différences fondamentales, d'ordre technique et juridique, qui existent entre chaque type de contenu, ainsi que de la question de la proportionnalité du filtrage, par rapport à d'autres méthodes permettant de réduire les dommages, de prévenir les infractions, ou de procéder à des investigations en matière de cybercriminalité.

1.5 Le filtrage d'Internet et la loi

Le filtrage de contenus illégaux ne consiste pas en un retrait définitif des images, vidéos ou pages web concernées. En raison des inévitables possibilités de contournement de la mesure, des réalités du sous-blocage (ou filtrage insuffisant) et du sur-blocage (ou filtrage excessif), des risques de dérives et de conflits de lois, et du problème selon lequel le filtrage ne conduit pas à la suppression des contenus, la question qui se pose n'est pas simplement celle de savoir s'il faut « filtrer ou ne pas filtrer », mais plutôt celle de savoir quelles mesures de filtrage, proportionnées et acceptables dans une société démocratique, peuvent être introduites. En conséquence, il est crucial de passer en revue les enjeux juridiques et démocratiques que soulève la question du filtrage.

Dresser un panorama détaillé de la question du filtrage d'Internet face à la loi implique de passer en revue les instruments juridiques qui auront une incidence sur un système de filtrage. Les démocraties libérales modernes jouent un rôle crucial de par leur respect actif des libertés fondamentales et des libertés publiques. Il sera nécessaire de prendre en considération les instruments tant nationaux qu'internationaux, aux fins d'identifier les droits fondamentaux qui se trouvent en opposition avec le filtrage d'Internet, et les droits fondamentaux qui pourraient inversement justifier une telle mesure. Le rôle des prestataires de services Internet est fondamental, dans le cadre d'une mesure de filtrage d'Internet, alors que ces derniers opèrent parfois dans des circonstances déroutantes en raison d'exigences légales concurrentes, voire contradictoires.

D'un point de vue juridique, le filtrage d'Internet est une mesure qui donnerait, à une personne ou à une entité, dans l'objectif de protéger un intérêt spécifique, le droit de filtrer, le droit de choisir les moyens technologiques destinés à réaliser cet objectif et le droit de choisir les contenus à bloquer, sachant que cette initiative aurait pour résultat de priver certaines autres personnes de leur droit d'accéder à certains contenus, ou de leur droit de rendre disponibles certains contenus.

Le filtrage d'Internet est en conséquence une mesure qui, pour protéger certains droits ou libertés spécifiques, a un impact négatif, direct et immédiat, sur certains autres droits et libertés. Puisque les droits et libertés sont régis par la loi, l'analyse de la légitimité du filtrage requiert une analyse approfondie des éléments de droit qui autorisent ou peuvent entrer en conflit avec une telle mesure.

Le filtrage d'Internet est également une mesure qui est internationalement débattue. Pour cette raison, la présente étude se concentrera essentiellement sur les droits européen et international, pour ne donner que quelques exemples de leur application par certains systèmes juridiques nationaux.

Au sein de ces systèmes juridiques, le filtrage d'Internet peut entrer en conflit avec des dispositions relevant de deux domaines du droit, que sont les droits de l'Homme et les libertés fondamentales, d'une part, et les dispositions relatives aux communications électroniques, d'autre part. Le filtrage peut inversement se révéler compatible avec certaines dispositions de l'un et l'autre de ces domaines, en fonction notamment de la proportionnalité de la mesure adoptée.

L'enjeu est donc de déterminer la mesure dans laquelle une liberté peut être limitée dans l'objectif d'en préserver une autre. Chacune de ces libertés devra être passée en revue de manière détaillée, afin d'autoriser une conclusion sur les conditions dans lesquelles une mesure de filtrage pourrait être considérée comme juridiquement acceptable.

De nombreux systèmes juridiques nationaux, de même que les systèmes juridiques européen et international, aménagent une place très importante aux droits de l'Homme et aux libertés fondamentales, lesquels peuvent tour à tour être invoqués pour justifier une mesure de filtrage, ou affectés de manière inappropriée par une telle mesure.

La préservation des droits de l'Homme, en particulier de ceux qui pourraient entrer en conflit avec une mesure de filtrage d'Internet, à savoir le droit à la vie privée et le droit à la liberté d'expression[7], est souvent considérée comme intrinsèque à toute démocratie. Trois aspects de l'organisation politique permettent de déceler les relations entre démocratie et libertés :

- Les élections – le principe de la participation de tous à la vie politique ;
- La séparation des pouvoirs - l'organisation institutionnelle permettant la séparation des pouvoirs ;
- Les droits fondamentaux – le souhait et l'engagement pris par l'Etat de respecter les libertés.

La différence entre les droits de l'Homme, les libertés fondamentales et les libertés publiques réside principalement en la personne du *titulaire* de droits, lequel dépend lui-même du contenu du droit attribué, de la valeur juridique du texte qui consacre ce droit et de l'importance accordée à la protection de ce dernier. Un droit particulier peut recevoir chacune des trois qualifications. Il en est ainsi, dans de nombreux pays, du droit à la protection de la vie privée et du droit à la liberté d'expression. Les libertés publiques constituent des limitations aux pouvoirs de l'autorité publique à l'égard des citoyens.

Aux notions de droits de l'Homme et de libertés publiques, a été ajoutée la notion de « droits fondamentaux » ou de « libertés fondamentales ». Les droits et libertés fondamentaux sont :

- protégés « *contre le pouvoir exécutif (et) contre le pouvoir législatif* » ;
- garantis « *en vertu non seulement de la loi mais surtout de la Constitution ou des textes internationaux ou supranationaux* » ;
- protégés « *contre les pouvoirs exécutifs et législatifs, en application des textes constitutionnels (ou internationaux)* », non seulement par « *les juges ordinaires* », mais également par « *les juges constitutionnels et même les juges internationaux* ».

Les premiers textes à avoir consacré les droits de l'Homme et les libertés fondamentales furent nationaux. Les textes internationaux furent adoptés après la seconde guerre mondiale et contribuèrent à modifier les systèmes juridiques locaux. Leur contenu fut également reconnu par les institutions de l'Union européenne.

Les initiatives de filtrage d'Internet doivent être analysées à la lumière des principales libertés fondamentales qui semblent entrer en conflit avec elles – dont la liberté d'expression et le droit au respect de la vie privée et familiale – ou qui semblent inversement les soutenir, comme le droit des enfants à être protégés contre la violence et l'exploitation.

Les instruments internationaux relatifs aux droits de l'Homme ont été adoptés dans le cadre des Nations Unies et du Conseil de l'Europe. Ils incluent :

- La Charte des Nations Unies ;
- La Déclaration universelle des droits de l'Homme des Nations Unies (DUDH) ;
- Le Pacte international relatif aux droits civils et politiques des Nations Unies (PIDCP) ;
- La Convention des Nations Unies relative aux droits de l'enfant ;
- La Convention des Nations Unies relative aux droits des personnes handicapées ;
- La Convention des Nations Unies sur l'élimination de toutes les formes de discrimination raciale ;
- La Convention européenne des droits de l'Homme du Conseil de l'Europe (CEDH) ;
- La Convention sur la cybercriminalité du Conseil de l'Europe.

[7] Voir infra, sous-sections 6.6.1 et 6.6.2.

Bien que l'Union européenne n'ait pas pour l'heure adhéré à la Convention européenne des droits de l'Homme, elle reconnaît la nécessité de préserver les libertés fondamentales et de respecter la CEDH. L'Union européenne met également l'accent sur certaines catégories de droits, à l'instar des textes internationaux analysés, tels que les droits de l'enfant, les droits des personnes handicapées ou le droit de tous à ne pas subir de discrimination.

Les libertés fondamentales susceptibles d'entrer en conflit avec le filtrage

Le filtrage d'Internet peut avoir un impact sur certains droits de l'Homme et libertés fondamentales.

- Les tentatives de filtrage d'Internet peuvent constituer une ingérence dans le **droit à la vie privée**, lorsqu'elles permettent ou requièrent la conservation de données électroniques protégées par la confidentialité, ou lorsqu'elles empêchent les individus de bénéficier de certaines potentialités offertes par le réseau, les privant par là-même de la possibilité de nouer certaines relations ou de faire certains choix de connexion, actes qui relèvent de l'exercice du droit à la liberté de la vie privée. Il en est particulièrement question dans les cas inévitables de sur-blocage (ou filtrage excessif), lequel impacte des sites web totalement innocents.
- Les tentatives de filtrage d'Internet peuvent constituer une ingérence dans le **droit à la liberté d'expression**, lorsqu'elles empêchent des personnes d'accéder à certaines informations en ligne ou de rendre disponibles ces mêmes informations. Le filtrage a de fait un impact négatif sur la diffusion de l'information, sa communication et sa réception.
- Le filtrage d'Internet constitue une ingérence dans les droits spécifiques dont bénéficient certaines catégories de personnes, tels que le **droit des personnes handicapées** d'accéder aux communications électroniques.
- Le filtrage peut être vu comme une alternative au respect de l'obligation, posée aux Etats par la Convention sur les droits de l'enfant, de prendre toutes les mesures internationales appropriées afin de prévenir l'exploitation des enfants à des fins pornographiques.

Le droit au respect de la vie privée et familiale est un droit de l'Homme et une liberté fondamentale, et, de fait, une liberté publique dans de nombreux Etats. Il bénéficie directement aux adultes comme aux enfants, même si la Convention des Nations Unies relative aux droits de l'enfant le complète en consacrant spécifiquement le droit des enfants au respect de leur vie privée en son article 16.

Le respect de la vie privée

Les textes qui garantissent le droit au respect de la vie privée protègent les individus des immixtions arbitraires dans leur vie privée et familiale, leur domicile ou leurs correspondances, et contre les atteintes à leur honneur ou à leur réputation. La DUDH précise que « *toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». Le PIDCP apporte la même précision, et ajoute que **les immixtions doivent être légales**, ce qui permet de s'interroger sur certaines initiatives de filtrage conduites par l'Industrie, qui n'ont aucune base légale. La CEDH permet quant-à-elle certaines immixtions lorsque ces dernières répondent aux conditions décrites dans une dite « clause d'ordre public », qui inclut, elle-aussi, le principe de légalité.

Le principe d'inviolabilité des correspondances, sur le fondement duquel la Cour européenne des droits de l'Homme protège « *le caractère confidentiel des communications privées* », est l'une des libertés fondamentales qui pourraient se trouver directement heurtées par une mesure de filtrage d'Internet.

En fonction de l'objet à filtrer (contenu d'un certain type, protocole de communication), des moyens utilisés pour mettre en place ce filtrage et des règles additionnelles qui sont potentiellement ajoutées pour atteindre l'objectif particulier du mécanisme global, une mesure

de filtrage peut parfois conduire à la conservation du contenu d'un message, ou de certains éléments de ce contenu, en relation avec une personne spécifique, sans le consentement de cette dernière.

Même lorsque les communications reçues ou émises par une personne ne sont pas qualifiées de correspondances, elles restent toutefois protégées par le droit au respect de la vie privée. Sur la base de ce principe, une mesure de filtrage qui conduirait à la surveillance ou à la conservation de données relatives au contenu de ce qu'une personne reçoit, envoie ou consulte, même s'il ne s'agit que de la consultation d'un site web d'une nature particulière, constituerait une ingérence dans le droit de cette personne au respect de sa vie privée. Une telle mesure constituerait également une ingérence dans le droit de cette personne à la protection de ses données personnelles.

Le principe de protection des données personnelles implique la confidentialité de ces données, lorsque celles-ci sont associées à des informations permettant l'identification directe ou indirecte d'une personne physique. Toute information permettant de contrôler l'individu est considérée comme dangereuse, même lorsqu'elle n'est pas utilisée, y compris dans un Etat démocratique.

La liberté de la vie privée peut être comprise comme étant la liberté d'établir et de développer des relations avec autrui, y compris par la voie des communications électroniques, mais aussi « *de faire des choix culturels, ludiques ou de consommation en ligne, ou simplement de s'informer, de naviguer librement sur le réseau* ». La liberté de correspondance, qui est le pouvoir de correspondre avec les personnes de son choix, est elle-même protégée par le droit au secret des correspondances.

Une mesure de filtrage d'Internet qui aurait une incidence négative sur la liberté de correspondance entrerait par conséquent en conflit avec l'article 8 de la CEDH.

Une mesure de filtrage d'Internet peut être considérée comme étant en conflit avec une liberté fondamentale, dès lors qu'elle présente **le risque de constituer une ingérence dans l'exercice de cette liberté, *même si l'usage de la fonctionnalité* qui présente un tel risque *n'entre pas dans les objectifs assignés à la mesure***.

La liberté d'expression

Le droit à la liberté d'expression est un droit de l'Homme et une liberté fondamentale, et, de fait, une liberté publique dans de nombreux Etats. Il bénéficie autant aux adultes qu'aux enfants, et la Convention des Nations Unies sur les droits de l'enfant lui ajoute une déclaration spécifique du droit des enfants à la liberté d'expression.

Ce droit inclut « *la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées* », « *sans considération de frontières* ». Ce droit doit pouvoir être exercé « *sans qu'il puisse y avoir ingérence d'autorités publiques* ». La DUDH et le PIDCP lui ajoutent la liberté de « *chercher* » des informations et des idées « *par quelque moyen d'expression que ce soit* », tandis que le PIDCP explique que ce droit peut être exercé « *sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix* ».

Le PIDCP et la CEDH prévoient que l'exercice du droit à la liberté d'expression comporte des « *devoirs et des responsabilités* » et peut être soumis à certaines restrictions.

La liberté d'expression inclut le droit de recevoir des informations, notamment par l'intermédiaire d'Internet. Toute mesure de filtrage d'Internet qui empêcherait une personne d'accéder à un contenu serait dès lors en conflit avec cette liberté. Ce conflit serait encore plus grand si la mesure préconisait la suspension d'un accès à Internet, prévenant ou empêchant par là-même une personne d'utiliser l'ensemble du réseau Internet ou une partie de celui-ci.

Dans le cadre de la réforme de la législation sur les télécommunications (paquet télécom), le Parlement européen réaffirma, le 6 mai 2009, qu'« *aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux sans décision préalable des autorités judiciaires sauf lorsque la sécurité publique est menacée* ». Plusieurs auteurs et membres du Parlement européen y virent une reconnaissance de l'accès à Internet en tant que droit fondamental.

Que l'accès à Internet soit ou non un droit fondamental *indépendant*, il est à tout le moins protégé en tant que moyen d'exercer le droit à la liberté d'expression. Toute mesure de filtrage d'Internet destinée à empêcher les personnes d'accéder à l'information est par conséquent en conflit avec ce dernier droit. Toute initiative de filtrage limite le droit à la liberté d'expression, dans une mesure plus ou moins grande selon les caractéristiques du filtrage et selon le degré de sur-blocage (ou filtrage excessif) que ce filtrage génère, puisque l'objectif clairement identifié d'une telle mesure est de limiter l'accessibilité de contenus spécifiques.

Les droits de l'enfant

Toute mesure de filtrage d'Internet qui conduirait à empêcher les enfants d'accéder aux informations qui pourraient être utiles à leur développement et à leur éducation à une vie responsable entrerait en conflit avec la Convention internationale relative aux droits de l'enfant, et certainement avec le droit à la liberté d'expression de manière plus générale, particulièrement lorsque cette mesure ne serait pas placée sous le contrôle des parents.

Les droits des personnes handicapées

Les personnes handicapées rencontrent une difficulté que les personnes non-handicapées ne connaissent pas : leur handicap peut parfois être une entrave à l'exercice plein et entier de leurs droits. Ces personnes peuvent être assistées, dans ce cadre, par l'utilisation des communications électroniques – services Internet inclus. En conséquence, une mesure de filtrage d'Internet qui préviendrait l'accès des personnes handicapées aux communications électroniques pourrait empêcher certaines d'entre elles d'exercer des droits fondamentaux que les personnes sans handicap seraient toujours en mesure d'exercer, malgré une interdiction d'utiliser le réseau Internet ou une partie de celui-ci.

Les droits et libertés fondamentaux susceptibles de justifier une mesure de filtrage d'Internet

La protection d'autres droits et libertés pourrait œuvrer au soutien d'une mesure de filtrage d'Internet. Trois de ces droits sont les suivants :

- Le droit des enfants à être protégés contre la violence,
- Le droit des personnes à ne pas subir de discrimination,
- Les droits de propriété intellectuelle.

Les enfants sont fortement protégés contre la violence. Deux aspects de la protection de l'enfance présentent un intérêt particulier :

- Le nombre important de textes qui mettent l'accent sur la prohibition de la violence mentale et physique commise sur la personne d'un enfant, spécialement lorsqu'elle est de nature sexuelle ;
- La prohibition de l'image elle-même d'un crime de nature sexuelle commis sur la personne d'un enfant, à travers l'interdiction de la pédopornographie.

L'importance de la lutte contre la pédopornographie, de même que l'importance de protéger les enfants de la violence et des entraves à leur développement personnel, sont très souvent un argument pour justifier la mise en œuvre de mesures de filtrage d'Internet. Il s'agit même,

souvent, de la seule justification avancée par les gouvernements ou par les acteurs privés qui sollicitent la mise en œuvre d'une mesure de filtrage d'Internet.

Si les arguments mis en avant pour justifier le filtrage devaient être acceptés, il resterait difficile de comprendre, d'un point de vue juridique, en quoi une mesure de filtrage d'Internet devrait être limitée aux seuls contenus à caractère pédopornographique, puisque la loi protège également, spécifiquement, d'autres catégories de personnes contre certaines atteintes, notamment les atteintes générées par la discrimination.

Les droits de l'Homme et les libertés fondamentales bénéficient à tous les individus, sans distinction. Toutefois, puisque les discriminations ont été et peuvent demeurer un problème dans certains pays, plusieurs textes furent signés pour souligner le droit spécifique de tout individu à être protégé contre la discrimination. Sur Internet, les contenus visés par l'interdiction de discrimination peuvent être des textes qui incitent à la discrimination, mais également des images de tortures ou de meurtres, commis pour des motifs de haine raciale. De telles images sont particulièrement choquantes et offriraient une justification tout aussi valide que la pédopornographie au filtrage d'Internet.

Les droits de propriété intellectuelle sont protégés par de nombreux traités au niveau international. Ils comprennent notamment, dans le cadre des textes qui en déclarent le principe, les droits d'auteur et les droits connexes, ces deux derniers protégeant « *les droits des créateurs, artistes interprètes ou exécutants, producteurs et radiodiffuseurs, et contribu(ant) au développement culturel et économique des nations* ». Le droit à la protection des droits de propriété intellectuelle est donc considéré comme un droit de l'Homme et une liberté fondamentale, et peut également être une liberté publique dans certains pays. Ce droit pourrait en conséquence être invoqué en justification d'une mesure de filtrage d'Internet, dès lors qu'une telle mesure serait effectivement en mesure de lui offrir protection.

Les dispositions spécifiques aux communications électroniques

Une mesure de filtrage, mise en œuvre au sein de l'Union européenne, doit encore être compatible avec les dispositions européennes relatives aux communications électroniques.

- Ces dispositions incluent les **obligations** des prestataires de services Internet en termes de **qualité de service**, de **service universel** et de **neutralité** ;
- Les dispositions relatives au **régime de responsabilité** des prestataires d'accès à Internet sont encore une base d'arguments permettant à ces prestataires de s'opposer à des mesures de filtrage qui seraient mises en œuvre hors le cadre d'une loi.

Les services inclus dans la notion de **service universel** sont « *des services de communication de base, incluant les communications par la voix et une connexion à Internet* ». Toute mesure de filtrage qui empêcherait un utilisateur d'accéder au réseau téléphonique public serait dès lors en conflit avec l'obligation de service universel. Permettre aux citoyens d'accéder à Internet reste un objectif qui doit être mis en équilibre avec les autres droits et libertés, et l'intérêt général du public.

Si l'accès à Internet haut débit était reconnu dans le futur comme étant une composante du service universel, et si les modifications actuellement apportées à la législation de l'Union européenne relative aux télécommunications étaient finalement adoptées, un Etat pourrait dès lors ne pas être autorisé à mettre en place une mesure de filtrage concernant un utilisateur d'Internet ou un contenu disponible sur ce réseau, sans respecter la Convention européenne des droits de l'Homme, spécialement sa clause d'ordre public et le droit à un procès équitable devant un tribunal ou une cour de justice.

Les opérateurs de communications électroniques doivent également faire en sorte que le **service d'accès** qu'ils fournissent **soit d'une certaine qualité**. Ils sont par ailleurs en charge du transport d'informations de service public. Les exigences y attachées peuvent

s'ajouter aux obligations spécifiques que ces opérateurs peuvent avoir à respecter lorsqu'ils assurent, en outre, le service universel ou une obligation de service public.

Les réseaux électroniques publics sont techniquement très complexes, et la plupart des mesures de filtrage d'Internet sont susceptibles d'accroître, sur ces derniers, le nombre de latences et de pannes. En conséquence, **l'exploitation d'un réseau de communications électroniques et le filtrage sont philosophiquement en opposition**, et demander à un opérateur de mettre en œuvre une mesure de filtrage pourrait placer ce dernier dans une situation où deux obligations aux effets contradictoires doivent être respectées.

Les prestataires de services Internet ont l'obligation de rester neutres vis-à-vis du contenu des communications électroniques échangées sur Internet, à l'instar d'autres catégories de transporteurs (par exemple les opérateurs de téléphone traditionnel ou les services postaux). En conséquence de ce principe, un prestataire de service Internet ne peut choisir de transmettre ou de ne pas transmettre un message en fonction de son contenu, excepté sur la base d'une obligation légale qui justifierait son non-respect du principe de neutralité.

Un prestataire de services Internet n'a pas la permission de surveiller les contenus échangés sur son réseau, excepté sur la base d'une obligation spécifique prévue par la loi. Une mesure de filtrage d'Internet qui requerrait la surveillance de contenus échangés sur les réseaux afin d'identifier des contenus illégaux particuliers ne serait donc pas permise, sauf si elle était spécifiquement prévue par une loi respectant la clause européenne d'ordre public.

En l'absence d'une loi qui les obligerait à filtrer certains contenus spécifiques, les prestataires d'accès à Internet ne peuvent pas surveiller et filtrer des contenus web sans se placer en infraction avec les conditions de leur régime de responsabilité tel que prévu par la Directive de l'Union européenne, et risquer en conséquence de devenir responsables de l'ensemble des contenus qu'ils transmettent.

Un fournisseur d'accès à Internet qui sélectionnerait certains contenus afin de les filtrer, sans y être contraint par la loi, serait en effet susceptible de ne plus répondre aux conditions fixées par son régime de responsabilité actuel. Un tel prestataire prendrait de fait le risque de voir sa responsabilité engagée devant un tribunal pour chaque contenu illégal qui transiterait potentiellement par ses services. Une telle situation serait source de grande insécurité juridique. Elle mettrait en danger le secteur lui-même de la fourniture d'accès, et plus généralement le développement technologique du pays.

1.6 Mettre les libertés fondamentales en équilibre

Du point de vue du Pacte international sur les droits civils et politiques et de la Convention européenne des droits de l'Homme, la question de la mise en équilibre des libertés se révèle toujours dans l'hypothèse d'une limitation apportée à une liberté protégée, dans l'objectif d'en préserver une autre.

Dans le cadre d'une mesure de filtrage d'Internet, les droits de l'enfant, le droit des personnes à la non discrimination, ou les droits de propriété intellectuelle, doivent être mis en équilibre avec le droit à la vie privée et familiale et le droit à la liberté d'expression, qui leur sont opposés.

Certains des droits consacrés par le Pacte international sur les droits civils et politiques et la Convention européenne des droits de l'Homme sont « intangibles », tels que le droit à la vie ou le droit de ne pas être torturé, tandis que d'autres sont « conditionnels », parce qu'ils peuvent être l'objet de dérogations et/ou de limitations, tels que le droit au respect de la vie privée et le droit à la liberté d'expression.

L'équilibre des libertés fondamentales conditionnelles, lorsque différents droits sont en conflit, peut être atteint avec succès en suivant la méthode retenue par la Cour européenne des

droits de l'Homme pour analyser les affaires qui lui sont soumises. Cette méthode peut fournir des lignes directrices sur la manière dont les mesures de filtrage peuvent être mises en œuvre. Elle inclut l'application aux cas d'espèce de **la stricte « clause d'ordre public »**, dont l'un des éléments est **le principe de nécessité** de la mesure **dans une société démocratique**. Ces lignes directrices sont appliquées dans la présente étude à différentes initiatives de filtrage, notamment différenciées selon leurs objectifs, afin d'analyser la manière dont ces mesures pourraient être jugées par la Cour européenne des droits de l'Homme. Nous y voyons qu'un examen de la légitimité du but de ces initiatives de filtrage est également nécessaire, et que la validité de certains systèmes peut être remise en cause. Nous y proposons enfin une série d'étapes à suivre aux fins d'évaluer la légitimité, dans une société démocratique, de toute mesure de filtrage d'Internet.

La « clause d'ordre public »

La possibilité de limiter l'exercice de droits conditionnels peut prendre deux formes différentes :

- Certaines dispositions consacrant des droits conditionnels énumèrent restrictivement les conditions dans lesquelles une limitation de ces droits est acceptable ;
- D'autres dispositions consacrant des droits conditionnels, telles que les articles 8 et 10 de la CEDH relatifs au droit au respect de la vie privée et au droit à la liberté d'expression, prévoient, sous la forme d'un principe général ou d'une « clause générale d'ordre public », que les ingérences doivent être « ***prévues par la loi*** », être inspirées par « ***un ou des but(s) légitime(s)*** » au regard de l'article qui déclare le droit conditionnel en cause et être « ***nécessaires, dans une société démocratique, pour atteindre ce ou ces buts*** ».

Cette clause d'ordre public recouvre en conséquence les trois principes majeurs suivants :

- La **compétence exclusive de la loi pour limiter les libertés ;**
- La **nécessité de poursuivre un ou des but(s) légitime(s), parmi ceux énumérés par la Convention ;**
- La « **nécessité » de l'ingérence « dans une société démocratique »**, principe interprété par la Cour européenne des droits de l'Homme comme impliquant que l'ingérence, « *dans une société qui entend demeurer démocratique* »,
    - Réponde à un « ***besoin social impérieux*** », et
    - Soit « ***proportionnée au but légitime poursuivi*** ».

Le principe de légalité

Toute mesure de filtrage, à tout le moins lorsqu'elle est mise en œuvre dans le cadre de la CEDH, doit être prévue par une loi répondant aux caractéristiques suivantes :

- « *La loi* » doit être « suffisamment accessible »,
- « On ne peut considérer comme une "loi" qu'une norme énoncée avec assez de précision pour permettre au *citoyen de régler sa conduite* »

Le seul type d'accord qui pourrait permettre la mise en place d'une mesure de filtrage serait un contrat entre l'internaute et son prestataire de service Internet. La légalité d'une telle mesure dépendrait essentiellement du type de contenus concernés, de la nature de la violation susceptible de déclencher l'application de la mesure et des preuves recueillies à cet effet. Il est en effet possible d'imaginer qu'un tel contrat, non rédigé de manière raisonnable, puisse être considéré comme étant en infraction avec les dispositions de la Directive de l'Union européenne concernant les clauses abusives dans les contrats conclus avec les consommateurs, particulièrement si elle autorisait le prestataire de services Internet à prendre des sanctions unilatérales à l'encontre de son client.

Le principe de but légitime

La Convention européenne des droits de l'Homme et, s'agissant de la liberté d'expression, le PIDCP, énumèrent restrictivement les buts légitimes pouvant motiver une ingérence dans l'exercice d'une liberté fondamentale.

Un but légitime, poursuivi par la loi autorisant une mesure de filtrage d'Internet, ne suffit toutefois pas à légitimer la limitation d'une liberté dans le contexte de l'application de législation du Conseil de l'Europe. La mesure doit encore être *nécessaire* dans une société démocratique.

S'agissant du droit à la vie privée, la CEDH permet les ingérences lorsqu'elles sont nécessaires (art. 8) :

- *« à la sécurité nationale, à la sûreté publique, au bien-être économique du pays,*
- *à la défense de l'ordre et à la prévention des infractions pénales,*
- *à la protection de la santé ou de la morale,*
- *ou à la protection des droits et libertés d'autrui ».*

S'agissant du droit à la liberté d'expression, la CEDH permet des ingérences lorsqu'elles sont nécessaires (art. 10) :

- *« à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique,*
- *à la défense de l'ordre et à la prévention du crime,*
- *à la protection de la santé ou de la morale,*
- *à la protection de la réputation ou des droits d'autrui,*
- *pour empêcher la divulgation d'informations confidentielles*
- *ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».*

S'agissant du droit à la liberté d'expression, le PIDCP permet des ingérences lorsqu'elles sont nécessaires (art. 19) :

- « *Au respect des droits ou de la réputation d'autrui* »,
- « *A la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques* ».

Pour être légitime, une mesure de filtrage doit en conséquence poursuivre l'un des objectifs énumérés dans le texte qui s'applique à elle, selon la Convention à laquelle le pays concerné est partie, et selon la liberté fondamentale que la mesure limite. La détermination de l'intérêt ou de l'objectif poursuivi par cette mesure peut se révéler être une question cruciale.

- **Le filtrage du spam**

  Les objectifs du filtrage du spam sont, d'une part, la protection des droits du prestataire de services Internet de préserver l'existence de son service de messagerie électronique, et, d'autre part, la protection de la liberté de correspondance de l'utilisateur de ce même service. En conséquence, le but d'une mesure de filtrage du spam, laquelle peut limiter la liberté de correspondance et dès lors le droit au respect de la vie privée, semble être « *la protection des droits et libertés d'autrui* », qui *se trouve être* un but légitime aux termes de l'article 8 de la CEDH.

- **Le but de protection des intérêts de la victime**

  L'un des objectifs poursuivis par une mesure de filtrage visant les contenus illégaux peut être l'intérêt de la victime à ne pas être vue dans le cadre d'une scène de crime. Dans cette situation, la mesure poursuit le but déjà exposé de « *protection des droits d'autrui* », lorsqu'elle limite soit le droit à la vie privée, soit le droit à la liberté

d'expression. Toutefois, l'objectif de protection de la vie privée de la victime pourrait ne pas toujours être de nature à justifier juridiquement le filtrage, notamment car toutes les images à caractère pédopornographique n'incluent pas des éléments d'identification personnelle, tandis que l'inadéquation technologique des mesures de filtrage empêche ces dernières, au mieux dans la plupart des cas, d'atteindre *réellement* leur objectif.

- **Le but de prévention de l'accès à des contenus illégaux : protection de la morale ou de la sensibilité des personnes**

  Une mesure de filtrage visant les contenus illégaux dans le but de protéger les personnes contre la vue de ces derniers, pour des considérations morales ou afin de protéger la sensibilité des personnes les plus faibles de la société, peut être considérée comme poursuivant le but légitime de « *protection de la santé ou de la morale* ». *Si le but de protection de la sensibilité des personnes les plus faibles peut être vu comme légitime*, le lien entre la prévention de l'accès à des contenus illégaux et la protection de la morale semble en revanche très faible, spécialement en Europe, puisque les personnes y signalent généralement les contenus illégaux afin que des investigations puissent être menées sur ces derniers. Dans ce contexte, il semble utile de rappeler (comme indiqué plus haut) que la plus grande majorité des contenus signalés sont, en réalité, non illégaux.

- **Le but de prévention des infractions**

  Un autre objectif, pouvant motiver une mesure de filtrage d'Internet visant les contenus illégaux, peut être la répression des infractions.

  - La consultation régulière d'images à caractère pédopornographique pourrait conduire certaines personnes à devenir pédophiles alors qu'elles ne l'étaient pas, même s'il n'existe que très peu de preuves d'une telle hypothèse ;

  - Le filtrage d'Internet peu perturber le commerce de la pédopornographie, et dès lors prévenir la commission d'infractions, si le secteur commercial en question n'a pas mis en œuvre les technologies lui permettant de contourner la mesure.

- **Le but de répression des infractions**

  Généralement, le filtrage d'Internet n'a pas pour but de réprimer les infractions, puisqu'une mesure de filtrage ne permet pas de retirer le contenu illégal du réseau. Le filtrage d'Internet peut toujours être contourné et ne facilite pas les investigations destinées à trouver les producteurs, les distributeurs ou les victimes des contenus concernés.

  Certains pays pourraient toutefois décider d'empêcher certaines personnes d'accéder à Internet en sanction d'un crime ou d'une autre infraction. Une telle sanction pourrait aussi concourir au but de prévention des infractions.

Le principe de nécessité dans une société démocratique

Le troisième et dernier principe que comprend la clause d'ordre public est le principe de « nécessité », que la Cour européenne des droits de l'Homme interprète comme impliquant qu'une ingérence dans les droits et libertés, « *dans une société qui entend demeurer démocratique* », réponde à un « *besoin social impérieux* » et soit « *proportionnée au but légitime poursuivi* ». Le principe de nécessité implique dès lors deux éléments : un besoin social impérieux et la proportionnalité de l'ingérence au but légitime qu'elle poursuit.

- **Un besoin social impérieux**

  Selon la Cour européenne des droits de l'Homme, « *l'adjectif "nécessaire" (…) implique l'existence d'un "besoin social impérieux"* » ; il « *n'est pas synonyme d'"indispensable",*

il n'a pas non plus la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun" ». Une mesure de filtrage d'Internet doit dès lors correspondre à un besoin réel de la société, son efficacité à satisfaire ce besoin devant également être démontrée.

Un tel besoin social impérieux pourrait notamment avoir pour objet :

- La protection des droits de propriété intellectuelle ;
- La sauvegarde de la morale et la protection des personnes sensibles contre la vue de contenus à caractère pédopornographique ;
- La protection des victimes ;
- La prévention des infractions, pouvant elle-même inclure la prévention du passage à l'acte chez les non-pédophiles, l'entrave au modèle économique du commerce de la pédopornographie, et la prévention des échanges de pédopornographie ;
- La répression des infractions.

- **La proportionnalité de la mesure au but légitime poursuivi**

  L'ingérence que constitue une mesure de filtrage d'Internet dans l'exercice d'une liberté fondamentale doit être proportionnée au but légitime poursuivi par cette mesure, en plus d'être prévue par la loi pour poursuivre l'un des objectifs *limitativement* énumérés par la CEDH, et de répondre à un « besoin social impérieux ». Un certain nombre de facteurs permettent de « déterminer où se trouve l'équilibre » dans un cas particulier. L'un de ces facteurs est « **l'effet général d'une limitation donnée** ». Un autre de ces facteurs est de savoir « **s'il existait des raisons suffisantes de croire qu'un intérêt particulier était en péril** ». La Cour européenne des droits de l'Homme peut également apprécier la proportionnalité du « *comportement précis* » qui se trouve ainsi limité.

Le filtrage d'Internet et le critère de proportionnalité

L'analyse de la proportionnalité des initiatives de filtrage aux buts qu'elle poursuivent, à la lumière de l'ensemble des critères que nous avons analysés ci-dessus, requiert de distinguer entre chacune de ces mesures selon leurs objectifs.

- **Le filtrage du spam**

  Le filtrage du spam est justifié par un réel péril mettant en danger les services de messagerie électronique, tandis que le comportement précis qui se trouve limité est le droit d'envoyer des messages électroniques sans respecter les règles mises en place pour éviter le spam. Cette ingérence semble raisonnable, au regard du danger qui existe, pour l'utilisateur, de ne plus jamais pouvoir envoyer de messages électroniques, ou de perdre confiance dans les services de messagerie. Enfin, il ne semble pas, à cette heure, qu'une ***mesure moins restrictive*** puisse préserver le but poursuivi par une mesure de filtrage du spam.

- **Le filtrage du pair à pair ou du web <u>dans l'intérêt des industries culturelles</u>**

  Une mesure de filtrage du web ou du pair à pair (P2P) qui servirait les intérêts des titulaires de droits aurait probablement un effet général plus négatif.

  - Premièrement, si le filtrage du pair à pair conduisait au chiffrement des communications de pair à pair de manière à empêcher l'ensemble ou la plupart des actions de surveillance des contenus, il deviendrait quasiment ou totalement impossible de surveiller ces communications, même lorsqu'une telle opération serait autorisée sous conditions.

- Deuxièmement, une telle mesure génèrerait des coûts importants pour l'industrie de l'accès à Internet, le gouvernement et les utilisateurs d'Internet.
- Troisièmement, une telle mesure conduirait au blocage de fichiers conformes à la loi.

S'agissant du critère commandant qu'il y ait « *des raisons suffisantes de croire* » que les intérêts des titulaires de droits sont « *en péril* », nous pouvons dire qu'il n'existe aucune preuve d'un tel danger. Il n'existe aucune preuve de la nature et de l'étendue des pertes potentielles qu'auraient souffertes les titulaires de droits en raison de la violation de leurs droits sur le web ou par l'intermédiaire du P2P, en ce que les études, sur ce point, restent insuffisantes ou démontrent la thèse inverse.

- **Le filtrage de contenus illégaux présents sur le web ou un réseau de pair à pair <u>dans le but de protéger l'image de la victime</u>**

La proportionnalité d'une telle mesure semble acceptable en termes d'« effet général », à condition que cette mesure n'ait pas pour effet de filtrer d'autres contenus. Malheureusement, d'autres types de contenus seront probablement bloqués, en raison de la faiblesse des systèmes de filtrage d'Internet, et car une image à caractère pédopornographique peut tout à fait refléter la scène d'un crime sans pour autant permettre la reconnaissance de la victime.

S'agissant des « *raisons de croire* » que les intérêts de la victime sont « *en péril* », les intérêts des victimes pourraient également être servis par une meilleure information du public sur les crimes qu'elles ont soufferts, afin d'encourager les signalements aux services chargés de les réceptionner, de stimuler une augmentation de la pression des citoyens sur les gouvernements afin que ces derniers agissent contre ces crimes, et, en conséquence, d'améliorer les investigations et les ressources qui leur sont dédiées.

La proportionnalité du comportement qui est d'accéder à des contenus à caractère pédopornographique et d'en voir les victimes peut être analysée à la lumière de l'intérêt du public à identifier de telles victimes, et dépendra de la motivation de chaque personne qui verra le contenu concerné. Ces motivations peuvent être un désir ou une volonté de voir un crime par curiosité, comportement qui ne semble pas proportionné ; le désir d'en savoir plus à propos d'un crime, afin d'agir contre lui ; ou inexistantes, au delà du souhait de voir ces images signalées pour investigations.

- **Le filtrage de contenus illégaux présents sur le web ou un réseau de pair à pair <u>dans le but de protéger la morale</u>, ou <u>dans le but de protéger les personnes sensibles</u>**

Une mesure de filtrage mise en place dans l'un de ces buts pourrait conduire à empêcher les personnes protégées d'accéder à des contenus non controversés, en raison de la faiblesse des mécanismes de filtrage. Elle ne permettrait pas, plus loin, d'empêcher l'accès des délinquants à ces mêmes contenus. En conséquence, l'effet général de la mesure pourrait être une dépréciation du droit à la liberté d'expression, tandis que les délinquants auraient toujours accès aux contenus illégaux immoraux ou choquants bloqués, et tandis que les personnes protégées auraient toujours accès aux contenus immoraux ou choquants non bloqués. Il semble qu'une telle situation ne serait pas proportionnée.

- **Le filtrage de contenus illégaux présents sur le web ou un réseau de pair à pair <u>dans le but de prévenir les infractions</u>**

L'objectif de prévention des infractions devrait avoir pour objet d'empêcher les personnes de commettre ou d'encourager une infraction en achetant, téléchargeant ou vendant des contenus illégaux. La proportionnalité de la mesure de filtrage qui aurait un tel effet dépendrait toutefois du pourcentage de la population qui cesserait de commettre des infractions après avoir été préservée de l'accès à des contenus illégaux,

au regard du volume de restrictions apportées aux libertés par la mesure de filtrage. L'effet de cette mesure ne pourrait pas consister en une réduction significative de la liberté d'expression ou de la liberté de la vie privée de *chaque* citoyen.

Il n'existe actuellement aucune preuve qu'une mesure de filtrage conduirait à réduire le taux d'infractions, tandis qu'elle serait de nature à réduire certains comportements légitimes et proportionnés.

- **Le blocage de l'accès à Internet d'une personne <u>dans un but de prévention et de répression des infractions</u>**

  L'effet général attaché au filtrage d'une personne dans un but de répression et de prévention des infractions est d'empêcher cette personne d'accéder à Internet, et parfois même aux services de téléphone et de télévision. Un tel effet est particulièrement lourd puisqu'il prive complètement la personne concernée de sa liberté de recevoir et de communiquer des informations électroniques, de sa liberté d'exercer son droit à une vie privée et familiale, et de sa liberté de correspondre, dans l'univers électronique. Une telle sanction ne peut être considérée comme proportionnée que si elle se trouve justifiée au regard de l'infraction commise et du but poursuivi au travers de la répression de cette dernière, voire de sa prévention.

Les autres conséquences du principe de stricte nécessité des ingérences

Plusieurs mesures de filtrage peuvent autoriser des immixtions additionnelles dans les libertés, en raison de la nature des mécanismes qui sont utilisés pour les mettre en œuvre. A titre d'exemple, certains mécanismes de filtrage du spam peuvent permettre à un prestataire de services de scanner tout message envoyé ou reçu, ce qui autorise d'autres ingérences telles que la conservation de données personnelles en relation avec l'ensemble du message ou certains mots de son contenu.

Toute mesure qui constitue une ingérence dans l'exercice de certaines libertés doit voir sa proportionnalité évaluée, en premier lieu, au regard du but légitime qui lui a été assigné, et, en second lieu, au regard de son effet général, lequel ne doit pas aller au delà de ce qui est nécessaire pour atteindre le but poursuivi et, dans tous les cas, lequel doit **« *ménager un certain périmètre* » pour l'exercice de la liberté qui se voit ainsi limitée, et non « *provoquer (l') extinction* » de cette dernière**.

Chaque fois qu'une mesure de filtrage est autorisée, certaines garanties doivent être prises afin que cette mesure ne soit pas utilisée d'une manière qui pourrait provoquer, dans les libertés, une ingérence plus grande que celle qui est nécessaire pour atteindre le but poursuivi. Ce principe s'applique également aux mesures poursuivant un but légitime dont les fonctionnalités de base ne limitent pas les libertés de manière disproportionnée. Une mesure est toujours susceptible de présenter l'un des risques analysés au premier paragraphe de la présente sous-section. Ces garanties peuvent être techniques, et consister en la mise sous contrôle des fonctionnalités qui pourraient menacer plus avant les libertés, ou juridiques, et consister en la prohibition des fonctionnalités concernées elles-mêmes ou de leur utilisation, lorsque ces dernières ne sont pas essentielles au fonctionnement du mécanisme de blocage. Un juge doit chaque fois être mis en mesure de contrôler la proportionnalité de toute mesure spécifique de filtrage.

La compétence du juge pour contrôler la proportionnalité des ingérences dans l'exercice des libertés fondamentales

La Cour européenne des droits de l'Homme procède au contrôle des mesures, prises par les Etats contractants, qui constituent des ingérences dans l'exercice de libertés fondamentales, ainsi qu'au contrôle de leur évaluation par les juges nationaux. Les juridictions nationales sont également compétentes pour connaître des contestations relatives à la mise en place d'une

mesure de filtrage, appliquée par exemple à un citoyen, ou à un contenu que ce citoyen aurait souhaité envoyer, recevoir ou consulter.

Toutefois, si avoir le droit de remettre en cause une décision qui limite l'une de ses libertés est pour le citoyen un droit fondamental, l'exercice de ce droit suppose que la liberté en cause a d'ores et déjà connu une limitation, dont le citoyen a déjà dû subir les effets. Pour cette raison, il est essentiel que, dans certaines situations, un juge puisse intervenir avant que la décision de limiter un droit ne soit prise. S'agissant du filtrage d'Internet, ces situations sont celles dans lesquelles il est nécessaire, d'une part, d'évaluer puis de constater l'illégalité d'un contenu ou d'une action, et, d'autre part, d'apprécier la proportionnalité de la réponse à apporter à une situation illégale.

En conséquence de cette analyse, détaillée dans le chapitre 7 du présent rapport, il semble que les seules mesures de filtrage pouvant être mises en place sans l'obtention d'une décision de justice soient les mesures de *filtrage du spam* et de *filtrage dans un but de protection de la morale*, bien que cette dernière soulève plusieurs objections juridiques et pratiques.

Les conditions dans lesquelles le filtrage pourrait être acceptable

Les démocraties libérales doivent respecter les libertés fondamentales et les conditions de leur limitation que pose la Cour européenne des droits de l'Homme. Une mesure de filtrage d'Internet ne peut être mise en œuvre correctement que si les étapes suivantes sont respectées.

Etape n° 1 Mettre en œuvre le filtrage d'Internet de manière à ne pas entraîner une violation des autres droits et libertés ;

Etape n° 2 Identifier les droits et libertés qui se trouveront limités ;

Etape n° 3 Déterminer l'ampleur de l'ingérence ;

Etape n° 4 Déterminer précisément le ou les buts poursuivis ;

Etape n° 5 S'assurer que le but assigné à la mesure de filtrage corresponde à une réalité ;

Etape n° 6 Déterminer si la mise en place d'une mesure de filtrage dans le but qui lui a été assigné répond à un besoin social impérieux ;

Etape n° 7 Apprécier la proportionnalité de l'ingérence au but poursuivi ;

Etape n° 8 Tenir compte du principe qui doit gouverner le filtrage, déduit de la lecture des critères de légitimité posés par la Cour européenne des droits de l'Homme (nécessité dans une société démocratique, besoin social impérieux...) ;

Etape n° 9 Déterminer si une loi est nécessaire aux fins de prévenir l'utilisation de certaines fonctionnalités du mécanisme de filtrage ;

Etape n° 10 Prévoir la mesure de filtrage au sein d'une loi.

Etudes requises

Au cours de notre analyse de la manière d'équilibrer les libertés fondamentales, plusieurs études ont été identifiées comme nécessaires, pour permettre une évaluation adéquate de certaines mesures de filtrage au regard des critères posés par la Cour européenne des droits de l'Homme. En l'absence de telles recherches, la légitimité de ces mesures ne peut pas être montrée. Ces études portent notamment sur les mesures suivantes :

- Le filtrage d'Internet visant à prévenir la pédophilie,
- Le filtrage d'Internet visant à entraver le modèle économique du commerce de la pédopornographie,
- Le filtrage d'Internet visant à réduire les échanges de pédopornographie,
- Le filtrage d'Internet visant à protéger les personnes sensibles ou la morale,

- Le filtrage d'Internet visant à protéger les intérêts des victimes,
- Le filtrage d'Internet visant à protéger les droits de propriété intellectuelle.

1.7 Conclusion

Il est urgent que les sociétés comprennent l'impact fondamental qu'ont les activités de filtrage d'Internet sur notre droit de communiquer librement, même si le sens habituellement donné à la notion de filtrage d'Internet semble clair, au premier abord. Bien que les nombreuses motivations pouvant conduire une société à envisager d'imposer le filtrage d'Internet puissent être sous-tendues par les meilleures intentions, le filtrage pose des problématiques très complexes sur le terrain des droits de l'Homme, du droit, de la politique et de la technique. Des confusions et des attentes déçues, concernant l'efficacité ou même le(s) but(s) des sytèmes de filtrage, sont souvent constatées dans le cadre de la mise en œuvre de ces derniers. Le filtrage d'Internet a également des implications majeures s'agissant de la vie privée et de la sécurité de l'ensemble des citoyens. Le présent rapport s'intéresse à la signification de la notion de filtrage d'Internet et se penche sur les conséquences pratiques et juridiques d'une telle mesure.

Ce rapport décrit les motivations qui peuvent sous-tendre une mesure de filtrage d'Internet et les raisons pour lesquelles d'autres approches apparaissent avoir échoué. Il s'intéresse à la qualité des personnes ou entités qui mettent en œuvre le filtrage, à ce qui pourrait être filtré, à la manière dont la question du filtrage peut être approchée et aux personnes visées par les initiatives de filtrage d'Internet.

Un panorama technique des principaux systèmes de filtrage actuellement en place et de la manière dont ces systèmes sont appliqués à différents services Internet permet de mesurer l'ampleur, croissante, des contenus et services dont le filtrage est envisagé. Une analyse de l'efficacité des systèmes de filtrage d'Internet met en relief le grand nombre de questions qui n'ont pas reçu de réponses, s'agissant du succès de ces systèmes et de leur capacité à atteindre les objectifs qui leur ont été assignés. Quasiment tous les systèmes ont un impact technique sur la résilience d'Internet, et ajoutent une couche supplémentaire de complexité au sein d'un réseau déjà complexe. Tous les systèmes peuvent être contournés, et parfois uniquement avec de modestes connaissances techniques. De plus en plus de solutions logicielles dont l'objet est de fournir une assistance au contournement des filtres sont disponibles sur Internet.

Un résumé détaillé de la question du filtrage d'Internet face à la loi, spécialement en ce qui concerne les droits de l'Homme, les libertés fondamentales et les libertés publiques, montre que les systèmes de filtrage actuellement en place génèrent des inquiétudes majeures. Cet examen juridique inclut une analyse des instruments nationaux et internationaux, et s'attache à identifier les droits fondamentaux qui se trouvent en opposition avec le filtrage d'Internet, d'une part, et les droits fondamentaux qui sont de nature à soutenir le filtrage d'Internet, d'autre part. L'équilibre, délicat à atteindre, des différents droits qui se trouvent en conflit, doit être évalué par les juges, qui sont entraînés à gérer de telles complexités.

Les fournisseurs d'accès à Internet sont des entités commerciales à but lucratif, qui sont de plus en plus sollicitées pour mettre en œuvre des politiques sociales, sans qu'une surveillance ou des responsabilités corrélatives ne soient prévues. Ils opèrent parfois dans des circonstances très déroutantes, en raison d'exigences légales concurrentes, voire contradictoires. Il en est par exemple ainsi de l'exigence de fournir un haut niveau de qualité de l'accès à Internet, d'une part, et de filtrer l'accès à des services, d'autre part.

Répondre à la problématique principale qui est de trouver l'équilibre entre les libertés fondamentales en présence, lorsque différents droits sont en conflit, suppose une analyse détaillée de la méthode suivie par la Cour européenne des droits de l'Homme pour analyser les affaires qui lui sont soumises. Au travers de cette méthode, la Cour propose indirectement des lignes directrices sur la manière dont les mesures de filtrage d'Internet peuvent être

mises en œuvre, lorsqu'elles sont considérées comme appropriées, proportionnées et techniquement réalisables. Cette méthode inclut l'application aux cas d'espèce de la stricte clause d'ordre public, dont l'un des éléments est le principe de nécessité dans une société démocratique. Ces lignes directrices sont appliquées dans la présente étude à différentes initiatives de filtrage, notamment différenciées selon leurs objectifs, afin d'analyser la manière dont ces mesures pourraient être jugées par la Cour européenne des droits de l'Homme. Nous y voyons qu'un examen de la légitimité du but de ces initiatives de filtrage est également nécessaire, et que la validité de certains systèmes, utilisés de nos jours, peut être remise en cause.

Une mesure de filtrage d'Internet ne peut pas être mise en œuvre techniquement sans égards à plusieurs considérations. La réflexion sur cette mise en œuvre doit notamment tenir compte de l'impact réel de la mesure sur l'infraction que cette dernière a pour objet de prévenir. Elle doit encore évaluer la précision et l'efficacité de la mesure, et identifier clairement les conséquences négatives que cette dernière peut avoir sur les contenus et les usages d'Internet *conformes à la loi*. L'évaluation de l'efficacité technique doit être explicitement apportée en contribution, lors de l'évaluation de l'équilibre des droits en présence.

De nombreuses mesures de filtrage sont faciles à contourner, et sont dès lors totalement inefficaces pour répondre à une majorité d'objectifs. De manière étonnante, l'un des systèmes les plus faciles à contourner, soit volontairement soit accidentellement, est celui qui recourt au filtrage DNS, et qui est pourtant aujourd'hui mis en œuvre dans de nombreux pays au niveau national. Il est reconnu que certaines frustrations substantielles existent, tenant au manque d'efficacité de la coopération internationale actuelle en matière de cybercriminalité et au manque de réponses, de la part de certains pays, à des problématiques juridiques significatives que sont par exemple la pédopornographie, les discours de haine ou le terrorisme. Toutefois, au lieu de capituler et de s'en remettre à des stratégies nationales protectionnistes, nous avons besoin d'améliorer ces systèmes internationaux et de les rendre efficaces au 21ème siècle.

Très peu de mesures de filtrage d'Internet actuellement mises en œuvre sont le résultat d'un débat public éclairé, ayant pris place de manière transparente et responsable, malgré les problématiques complexes tenant au droit et aux droits de l'Homme que génère l'adoption de telles mesures. En conséquence, le présent rapport propose une série d'étapes à suivre aux fins d'évaluer la légitimité de ces mesures, dans une société démocratique.

Il est étrange que des contenus illégaux tels que les contenus à caractère pédopornographique, lesquels sont largement réprimés par la loi dans de très nombreux pays, et spécialement les contenus qui sont condamnés de manière universelle et qui sont réprimés par la loi de manière quasi-universelle[8], soient autorisés à rester en ligne pour certains utilisateurs, qui peuvent dès lors y accéder et les télécharger. Il est également étrange que l'industrie et des représentants non élus soient autorisés et encouragés par des gouvernements à mettre largement en œuvre des mesures de filtrage des contenus, sans transparence ni responsabilité y associée. Au terme de recherches appropriées et d'une analyse juridique, il doit revenir au pouvoir législatif de spécifier clairement, lorsque le principe du filtrage est adopté, la nature de ce qui peut être filtré sur Internet, la manière dont le filtrage doit être effectué, la manière dont le système de filtrage doit être audité et la manière dont il peut en être répondu publiquement. Il est surprenant que de nombreux gouvernements, au sein de l'Union européenne, qui n'ont pas le pouvoir de légiférer en matière de filtrage d'Internet, continuent d'encourager et de soutenir les initiatives de l'industrie en la matière. Ironiquement, dans ces pays, les listes noires (« *blocking lists* ») destinées à être utilisées aux fins de filtrage sont parfois générées par des organisations soutenues par l'Etat, sans pour autant faire l'objet d'un audit indépendant.

[8] Depuis décembre 2008, 193 pays ont ratifié la Convention des Nations Unies sur les droits de l'enfant, dont tous les membres des Nations Unies, hormis les Etats-Unis et la Somalie. Toutefois, même les Etats-Unis ont une législation destinée à lutter contre la pédopornographie.

La préoccupation majeure, dans le cadre de toute mesure de filtrage d'Internet, est la proportionnalité de cette mesure. L'impact de cette dernière, proportionnellement, ne doit pas être plus important sur les contenus et activités conformes à la loi qu'il ne l'est sur les contenus et les activités illégales. Une telle mesure doit encore être prévue par la loi et doit être mise en œuvre de sorte que d'autres droits et libertés ne soient pas violés.

Schématiquement, le filtrage d'Internet repose sur des solutions techniques qui sont inadéquates en elles-mêmes, et dont l'utilité est encore affaiblie par la disponibilité de protocoles alternatifs à celui sur lequel elles sont mises en œuvre, qui permettent d'accéder à des ressources illégales et de les télécharger. En conséquence, l'évaluation de la proportionnalité de la mesure ne doit pas seulement tenir compte de l'équilibre qui doit être trouvé entre les différents droits en jeu, mais également des insuffisances de la technologie à protéger ces droits, comme des impacts non souhaités que cette technologie peut avoir. Ces impacts peuvent consister en une pression politique réduite en faveur de solutions complètes, et en un risque que les prestataires de sites web illégaux introduisent de nouvelles stratégies pour éviter le filtrage, lesquelles pourraient rendre les investigations des services en charge de l'application de la loi encore plus difficiles à l'avenir.

Les résultats de la présente étude montrent que les problématiques pratiques, techniques et juridiques qui entourent la question du filtrage confirment que la question ne se résume pas à un choix de « filtrer ou de ne pas filtrer ». Les pays qui ont déjà mis en œuvre divers types de mécanismes de filtrage, et ceux qui projettent de le faire, doivent prendre deux mesures concrètes :

- Le fait que le filtrage soit l'une des options à l'étude revient à reconnaître, sinon à accepter tacitement, l'existence d'échecs en matière de coopération internationale sur une question touchant à la dignité fondamentale de l'être humain et à la protection des personnes les plus vulnérables de la société (dans la mesure où l'initiative concerne la pédopornographie sur Internet).

  Améliorer la qualité de la réponse apportée à ces échecs implique que la nature exacte de ces derniers fasse l'objet d'une analyse appropriée. Sur la base de cette dernière, tous les pays devraient fournir des rapports officiels sur les efforts qu'ils ont fait pour respecter les termes de l'article 34 de la Convention des Nations Unies sur les droits de l'enfant. Ces rapports seraient publiés annuellement et inclus dans les rapports périodiques que les Etats doivent présenter conformément à l'article 44 de ce même instrument. Une telle initiative serait de nature à encourager les pays à devenir plus actifs en la matière. En conséquence, plus de sites seraient retirés de leurs serveurs d'hébergement et donc rendus inaccessibles au public, et plus d'enfants seraient extraits de situations abusives.

- Un examen de l'impact pratique de la mesure (sur les accès accidentels, sur les accès délibérés, sur le « commerce » de la pédopornographie et sur l'usage de méthodes alternatives de distribution de contenus illégaux) est possible et nécessaire, en utilisant les données produites par les systèmes de filtrage existants. Sans un tel examen, la proportionnalité du filtrage – et dès lors sa légalité au regard des instruments fondamentaux de protection des droits de l'Homme – reste hautement discutable. Echouer à procéder un tel examen revient à susciter, pour de nombreux Etats, une interrogation à long terme sur leur engagement à respecter les principes clefs de l'Etat de droit.

- Les systèmes de filtrage doivent être mis en œuvre en vertu d'une loi nationale, ou ne pas être mis en œuvre du tout. Les systèmes de filtrage mis en place dans un contexte d'auto-régulation ne présentent pas la transparence et les conditions d'une responsabilité corrélative appropriées.

Chapitre 2 DELIMITATION DU SUJET

Le présent rapport reflète l'opinion de ses auteurs sur le filtrage que pratiquent les prestataires de services Internet en divers endroits du monde. Il est le résultat de l'expertise et de l'expérience combinées de ces auteurs, depuis 30 ans, dans les domaines d'Internet, de la régulation, de l'autorégulation, du droit, de la cybercriminalité, des investigations en matière de cybercriminalité et des nouvelles technologies.

Dans le cadre de leurs travaux, ces auteurs analysent les systèmes de filtrage d'Internet qui sont déjà mis en œuvre dans différents pays, sur la base d'informations provenant de ces mêmes pays.

Le chapitre 3 de la présente étude s'intéresse à la signification de la notion de filtrage d'Internet, et en étudie différentes appréhensions.

Le chapitre 4 s'attache aux raisons pour lesquelles la société croit que les tentatives de filtrage pourraient résoudre certaines problématiques sociétales majeures, et aux raisons pour lesquelles d'autres approches n'apparaissent pas très efficaces. Il s'intéresse à la qualité des personnes ou entités qui mettent en œuvre le filtrage, à ce qui pourrait être filtré, à la manière dont la question du filtrage peut être approchée et aux personnes visées par les initiatives de filtrage d'Internet. Ce chapitre dresse également une liste de pays qui ont déjà adopté des systèmes de filtrage d'Internet.

Le chapitre 5 passe en revue, sous une approche technique, les principaux systèmes de filtrage actuellement utilisés sur Internet. Il montre la manière dont ces systèmes sont appliqués à différents services Internet et engage une discussion sur l'impact de ces systèmes et sur les défis techniques que ces derniers posent. Il inclut une présentation des méthodes utilisées pour contourner ces systèmes de filtrage et une analyse de l'efficacité de ces systèmes.

Le chapitre 6 propose un panorama détaillé de la question du filtrage d'Internet face à la loi et passe en revue les instruments juridiques qui peuvent avoir une incidence sur un système de filtrage. Le rôle crucial que jouent les démocraties libérales modernes, de par leur respect actif des libertés fondamentales et des libertés publiques, y est clairement identifié. Cette étude inclut l'analyse des instruments nationaux et internationaux pertinents, et s'attache à identifier les droits fondamentaux qui se trouvent en opposition avec le filtrage d'Internet, d'une part, et les droits fondamentaux qui sont de nature à soutenir le filtrage d'Internet, d'autre part. Elle aborde la question du rôle des prestataires de services Internet et celle des circonstances déroutantes dans lesquelles ces derniers opèrent parfois, en raison d'exigences légales concurrentes, voire contradictoires. Ce chapitre accueille encore une présentation de la complexité de ces instruments juridiques et de la manière dont ces derniers s'appliquent aux services Internet et aux initiatives de filtrage d'Internet.

Le chapitre 7 développe la question de la mise en équilibre des libertés fondamentales lorsque différents droits sont en opposition, et, au terme d'une analyse détaillée de la méthode retenue par la Cour européenne des droits de l'Homme pour analyser les affaires qui lui sont soumises, propose des lignes directrices permettant de guider la mise en place de mesures de filtrage d'Internet. Cette méthode inclut l'application aux cas d'espèce de la stricte « clause d'ordre public », dont l'un des éléments est le principe de nécessité dans une société

démocratique. Ces lignes directrices sont alors appliquées à différentes initiatives de filtrage, notamment différenciées selon leurs objectifs, afin d'analyser la manière dont ces mesures pourraient être jugées par la Cour européenne des droits de l'Homme. Ce chapitre propose dans ce cadre un examen de la légitimité du but de ces mesures de filtrage, et interroge la validité de certains systèmes. Il met en évidence, en conclusion, une série d'étapes pouvant être suivies aux fins d'évaluer la légitimité, dans une société démocratique, de toute mesure de filtrage d'Internet.

2.1 Objectif

L'objectif de cette étude est triple :

- Stimuler le débat public et encourager un processus de prise de décision qui soit plus transparent et plus responsable ;
- Produire des informations détaillées relatives à l'efficacité des solutions actuelles, et décrire des solutions alternatives ;
- Mettre en évidence les dommages collatéraux, existants ou potentiels, qui peuvent impacter l'équilibre établi entre le maintien de la sécurité et la préservation des droits, ou qui peuvent avoir lieu lorsque la mesure de filtrage est étendue à des domaines autres que celui de la pédopornographie.

Ce document entend identifier les problématiques et sujets majeurs dont la prise en compte est importante dans le cadre de l'évaluation des systèmes de filtrage d'Internet tels que pratiqués par les prestataires de services Internet au niveau national ou international.

Afin que cette étude soit la plus objective possible, le présent rapport procèdera à une analyse minutieuse de l'efficacité des systèmes actuels et aménagera une place importante à la discussion de solutions alternatives.

Il passera rapidement en revue les différents forums qui débattent de ces questions, des systèmes de filtrage et de la manière dont ces systèmes sont adoptés.

L'objectif de ce rapport sera atteint s'il permet à ses lecteurs d'être plus avertis, ou mieux éclairés et informés, sur le sujet complexe des systèmes de filtrage d'Internet.

2.2 Avant propos

Dans divers pays, spécialement dans les pays membres de l'Union européenne, le filtrage de sites web proposant des images d'abus sur enfants est soit déjà en place (par exemple en Australie, au Canada, en Finlande, en Nouvelle Zélande, en Suède et au Royaume-Uni), soit projeté (par exemple en France, en Allemagne ou en Irlande).

La liste de contenus à filtrer ou liste noire (« *blocking list* ») est parfois préparée par le service d'assistance en ligne qui reçoit les signalements de ces sites (comme au Royaume-Uni), parfois préparée par la police (comme en Finlande, en Suède, au Danemark, ou, ainsi qu'il est projeté, en Belgique), parfois préparée par une entité officielle nationale tel que le régulateur des communications (comme en Australie), et parfois préparée par des entreprises individuelles (comme AOL).

Le débat actuel met en lumière l'intérêt qu'ont les Etats, comme les organisations internationales, à restreindre l'accès à certaines informations. En raison de la différence qui existe entre les normes juridiques de chaque pays, le filtrage est vu comme une alternative au processus de retrait du contenu à sa source, celui-ci impliquant d'utiliser la voie de la coopération internationale et de l'investigation en matière de cybercriminalité, lesquelles se révèlent plus consommatrices de temps et parfois infructueuses. Dans ce contexte, les technologies de filtrage d'Internet sont souvent utilisées pour tenter de « reterritorialiser » Internet dans sa globalité.

2.3 Résultats

Le résultat de cette étude est un document détaillé, proposant une analyse de l'état actuel de la situation concernant le filtrage d'Internet, une présentation de l'environnement juridique et réglementaire relatif à ce filtrage, ainsi que des observations relatives à l'efficacité d'une telle mesure et à son impact, tant sur la lutte contre la cybercriminalité, que sur le maintien de la démocratie et de la sécurité des individus.

La question de savoir où se trouve le meilleur équilibre entre la protection de l'enfance et la protection des libertés démocratiques est très complexe, et doit être tranchée in fine à un niveau national, dans chaque pays, au terme d'un large débat entre les acteurs concernés, débat tenant compte des instruments internationaux contraignants, tels que la Convention européenne des droits de l'Homme (CEDH).

Le présent rapport analysera l'efficacité des systèmes de filtrage, ainsi que l'impact de ces derniers sur les objectifs qui leur ont été assignés, sur les activités délictueuses ou criminelles et sur les utilisateurs d'Internet. Il accueillera une discussion sur l'approche qui offre les meilleurs bénéfices et s'interrogera sur le caractère approprié ou non, dans une société moderne, de ces systèmes de filtrage.

2.4 Le filtrage d'Internet et les droits fondamentaux

Du point de vue de la démocratie, les tentatives de filtrage d'Internet peuvent se révéler problématiques à deux niveaux fondamentaux.

- Premièrement et essentiellement, le filtrage d'Internet apparaît comme ayant une efficacité limitée. Il peut se révéler contre-productif dans la lutte contre les sites web illégaux (incluant ceux proposant des images d'abus sur enfants). Le danger pour la démocratie est que, puisque le filtrage n'est pas complètement efficace :
    i) Les principes de nécessité/de proportionnalité (provenant de la CEDH) pourraient ne pas être respectés, dans le cadre des dommages collatéraux que provoque la mesure au détriment de la protection d'autres libertés ;
    ii) Le danger existe de voir les gouvernements et les prestataires de services Internet se féliciter de leur succès dans la lutte contre la pédopornographie, alors même qu'en pratique les contenus concernés seraient toujours en ligne. Une telle situation pourrait conduire, dans certains cas, à une réduction de la pression politique visant à combattre les contenus à leur source au travers d'une coopération internationale, opération qui s'avère plus difficile. En conséquence, la mesure pourrait une fois encore restreindre les autres droits et libertés de manière excessive et disproportionnée.
- A un second niveau, le filtrage d'Internet présente le risque d'être un premier pas vers :
    iii) Une sorte de « normalisation » de la situation dans laquelle les prestataires de services Internet se voient confier le (ou s'investissent du) rôle de décider ce à quoi les consommateurs peuvent ou non avoir accès ;
    iv) Un élargissement de l'éventail des contenus à bloquer et un élargissement du rôle que jouent les prestataires de services Internet en matière de « maintien de l'ordre ».

La proposition de décision cadre 2009 du Conseil de l'Union européenne (qui n'a finalement pas été adoptée) faisait par exemple allusion à « l'identification » et au « blocage » des contenus illégaux. Cela aurait élargi le périmètre du filtrage, même dans les pays qui ont déjà mis en œuvre de telles mesures.

L'analyse détaillée que propose le présent rapport était nécessaire et urgente, en ce qu'elle montre définitivement que le filtrage est loin d'être la solution complète qu'il est annoncé être. Ce rapport pourrait permettre de :

- Réduire l'engouement pour le filtrage, lequel provient actuellement d'une grande variété de sources différentes ;
- Encourager un débat public sur les problématiques qui sont en jeu ;
- Aider à répondre au problème de risques de « dérives », puisque le filtrage est, de manière exponentielle, considéré comme étant la solution à apporter à un large éventail de problématiques, allant des questions de terrorisme ou de droits d'auteur à celle de l'anorexie.

Le filtrage est actuellement soit soutenu, soit discuté dans le cadre de réunions intergouvernementales, de l'Union internationale des télécommunications, du Conseil de l'Europe, du Conseil de l'Union européenne, et dans le cadre d'initiatives individuelles telles que le projet CIRCAMP (« *COSPOL Internet Related Child Abusive Material Project* » – Projet du COSPOL relatif aux ressources en ligne véhiculant des abus sur enfants).

2.5 Audiences ciblées

L'audience ciblée par ce document inclut en premier lieu les personnes qui sont responsables du développement et/ou de la mise en œuvre de la législation ou de la réglementation en matière de filtrage d'Internet, qu'elles considèrent la question au niveau national ou au niveau international. Cette audience comprend encore les gouvernements et les administrations nationaux, les hommes et femmes politiques, l'industrie de l'Internet fixe et mobile, les organisations gouvernementales transnationales, les organisations de protection de l'enfance et des droits de l'enfant, les autorités en charge de l'application de la loi au niveau national et international, les médias, les internautes de chaque pays et le grand public.

2.6 Limites du rapport

Le présent rapport compare, dans le détail, les technologies de filtrage du web avec celles qui sont mises en place sur d'autres services Internet, tels que la messagerie électronique ou les serveurs de news, pour une meilleure compréhension de la question. Toutefois, une analyse approfondie des autres types de filtrage n'a pu être faite dans le temps et l'espace impartis. De telles études additionnelles pourraient être produites à l'avenir, si nécessaire.

Chapitre 3 QU'EST-CE QUE LE FILTRAGE D'INTERNET ?

3.1 Vue d'ensemble

Lorsque l'on interroge quiconque au sujet de son expérience d'Internet, la réaction que l'on obtient est généralement très positive, et souvent doublée d'une stupéfaction quant aux capacités et à la flexibilité du réseau. Toutefois, certains des contenus et des activités qui peuvent être constatés en ligne sont illégaux au regard de la loi nationale, et, parfois, des traités internationaux.

Selon les membres du Parlement européen, le libre accès à Internet, sans ingérence, est tout simplement mais indubitablement un droit d'une considérable importance. Internet est « *une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information*», dont l'accès se trouve protégé par le droit à la liberté d'expression, même s'il n'est pas actuellement considéré comme un droit fondamental autonome[9].

Certains contenus disponibles sur Internet sont considérés comme étant préjudiciables. De nombreuses réponses peuvent être apportées à ce type de contenus, selon l'audience ciblée et le niveau de préjudice potentiel que ces contenus présentent. L'élaboration d'une définition de ce qui est préjudiciable[10] divise de nombreuses personnes et fait l'objet de recherches et de débats intensifs. La notion de contenu préjudiciable ne peut être parfaitement comprise que par référence à la définition plus large de ce qui présente un « risque de porter préjudice », laquelle s'étend aux comportements et contenus problématiques qui se rencontrent dans le cadre de l'utilisation de nouveaux services de communication (par exemple le harcèlement en ligne ou « *cyber bullying* », ou le vidéolynchage ou « *happy slapping* »), tant en ligne que hors ligne. La question des contenus préjudiciables n'est pas le thème principal de la présente étude, mais elle est abordée au chapitre 6, s'agissant de ses aspects juridiques.

Ces dernières années, certains Etats démocratiques ont promu l'usage de technologies de filtrage d'Internet visant différents types de contenus. Ils ont invoqué l'intérêt général pour requérir la mise en œuvre de mesures spécifiques de filtrage, en vue d'assurer le respect de divers aspects de leur politique publique, dans un contexte où les caractéristiques d'Internet rendent l'application de la loi difficile (au niveau international). Les contenus visés sont variés et concernent tant la disponibilité d'objets nazis sur des sites de vente en ligne, que l'hébergement de sites de jeux d'argent dans des Etats dont les législations sont libérales sur la question. De manière analogue, certains Etats, au régime moins ouvert sur l'information, ont déjà adopté le filtrage, et l'utilisent comme une ressource technique qui leur permet d'étendre leur pratique du contrôle de l'information aux médias électroniques.

Le présent chapitre propose un aperçu de la situation relative au filtrage d'Internet. Sa section 3.2 accueille une brève description de ce qu'est ce filtrage, et de certaines méprises qui

[9] Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe, 2007/2153(INI), § 23, accessible à cette adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//FR. Voir infra, sous-section 6.6.2.2.

[10] http://www.coe.int/t/dghl/standardsetting/media/mc-s-is/MC-S-IS%282005%29012_fr.pdf.

peuvent couramment survenir à l'abord de la notion. Sa section 3.3 présente les différents systèmes techniques qui permettent d'identifier les contenus à filtrer sur Internet.

3.2 Le filtrage d'Internet

Le filtrage d'Internet[11] n'est pas une activité récente. Il en est question depuis plusieurs années. Toutefois, la notion recouvre une si large gamme de pratiques, de matériels informatiques, de logiciels et de services, qu'il serait une erreur de croire que tous les types de filtrage sont les mêmes ou qu'ils sont d'efficacité équivalente, ou même qu'un système donné pourrait aisément être utilisé pour cibler plus d'un type de contenus.

Le premier objectif du filtrage d'Internet est d'empêcher un contenu d'atteindre un ordinateur personnel ou un poste informatique, à l'aide d'un produit logiciel ou matériel dont la fonction est de surveiller l'ensemble des communications Internet (requêtes d'accès à des contenus web incluses) et de déterminer s'il y a lieu d'empêcher la réception et/ou l'affichage de contenus spécifiquement ciblés.

Par exemple, un message électronique peut être bloqué car il est suspecté d'être un spam, un site web peut être filtré parce qu'il est suspecté de contenir des logiciels malveillants, ou une session de pair à pair (« *peer-to-peer* » ou P2P) peut être interrompue parce qu'elle est suspectée de véhiculer un échange de contenus à caractère pédopornographique.

L'expression « filtrage d'Internet » elle-même paraît quelque peu inappropriée, car elle semble suggérer que le filtrage du réseau est simple à mettre en œuvre et qu'il se résume à la possibilité de choisir de l'activer ou de le désactiver, aussi simplement que s'il s'agissait d'utiliser un interrupteur. Rien ne peut être plus éloigné de la réalité, en ce que les technologies de filtrage d'Internet sont particulièrement complexes et peuvent souvent être contournées avec une grande facilité. Il y a plusieurs raisons à cela, la plus essentielle étant qu'Internet a été conçu pour être décentralisé, et qu'il a été doté d'une capacité intrinsèque à assurer que les données puissent circuler « en contournant » toute barrière qui pourrait être mise sur leur route. Le complexe éventail des problématiques techniques est abordé au chapitre 5 de la présente étude.

Le filtrage d'un contenu Internet mis légalement à disposition hors d'un pays, mais considéré comme étant illégal dans ce dernier, peut parfois être considéré comme une option, permettant au dit pays de tenter de maintenir ses propres standards culturels nationaux, dans une situation d'accès global.

Il peut être dit que le filtrage d'Internet commença il y a vingt ans avec le filtrage des messages électroniques non sollicités (spams). Cette initiative vit le jour pour plusieurs raisons, mais était initialement destinée à éviter la saturation des réseaux. Elle a constitué un domaine constant de recherche et de développement, et a été au cœur d'une compétition soutenue entre les initiatives anti-spam et les activités de spamming.

Malgré les efforts considérables que la lutte contre le spam a impliqués sur une longue période de temps, tout utilisateur des services de messagerie électronique sait aujourd'hui que le filtrage du spam n'a pas été un franc succès, puisqu'il n'a pas permis d'éradiquer ce type de messages du réseau. Toutefois, les faux-négatifs[12] constituent un inconvénient mineur pour la plupart des internautes, en ce que le bénéfice qu'ils obtiennent du blocage de la plupart des messages qu'ils ne souhaitent pas recevoir l'emporte sur les problèmes qu'ils rencontreraient si aucun filtrage du spam n'était tenté.

A l'aide de différentes technologies, le filtrage d'Internet fut ensuite mis en œuvre à l'égard de tous types de logiciels malveillants (dont les virus, les logiciels espions ou « *spyware* », ou les chevaux de Troie), puis, plus tard, à l'égard des contenus illégaux véhiculés dans les groupes de news (« *newsgroups* ») du réseau Usenet.

[11] Parfois, l'expression « filtrage » est remplacée par celle de « blocage ».

[12] Un faux négatif est un message électronique qui se trouve autorisé à passer au travers du filtre anti-spam, car lors de son contrôle il est noté comme étant négatif, c'est-à-dire comme ne contenant pas de spam, alors qu'il s'agit effectivement d'un spam. D'où l'expression de faux-négatif.

Ces dernières années, différentes technologies de filtrage ont été mises en œuvre, avec des degrés de succès divers, sur une large palette de réseaux, pour tenter d'empêcher certains accès ou certaines activités, dans divers domaines des services et technologies Internet.

La priorisation des flux (« *traffic shaping* »)[13] est devenue une pratique ordinaire dans l'univers des services électroniques. Elle a lieu lorsque les fournisseurs d'accès à Internet, plus spécialement ceux qui proposent des offres « triple play »[14], tâchent de gérer activement les flux de données relatifs aux différents services Internet, en utilisant des priorités et des bandes passantes différentes.

L'ampleur de l'ingérence que peuvent constituer les mesures énumérées ci-dessus dans les droits de l'Homme et les libertés fondamentales doit être déterminée en tenant compte des éléments ci-dessous :

- Les caractéristiques, inhérentes à la mesure, qui pourraient conduire à la limitation de certaines libertés ;
- Les caractéristiques, inhérentes à la mesure, qui pourraient permettre d'implémenter d'autres fonctionnalités pouvant elles aussi conduire à la limitation de libertés, même si le but poursuivi par la mesure n'inclut pas l'implémentation et l'utilisation de ces dernières fonctionnalités ;
- Les caractéristiques et fonctionnalités qui sont attendues de la mesure de filtrage afin d'atteindre un objectif particulier.

Il est important de noter que tous les systèmes de filtrage d'Internet sont sujets à des problèmes de faux-négatifs et de faux-positifs[15], lesquels sont minimisés, dans les systèmes avancés, lors de la conception des technologies de filtrage. Par exemple, dans le cadre du filtrage du spam, le message considéré comme étant un spam est rarement détruit, mais placé dans un sous-dossier, afin de permettre à l'utilisateur d'y accéder pour vérifier qu'il n'a pas été filtré par erreur. Les systèmes de filtrage installés sur l'ordinateur familial permettent de contourner la mesure de blocage lorsqu'elle vise par erreur certains sites web. Un tel degré de conception est plus complexe à obtenir dans le cadre des systèmes de filtrage mis en œuvre au niveau des prestataires de services Internet.

La plupart des systèmes de filtrage d'Internet qui sont utilisés à domicile ou dans des locaux professionnels permettent aux administrateurs du réseau local de régler avec finesse le niveau du filtrage, afin de minimiser les faux-positifs et les faux-négatifs. Malheureusement, il est nécessaire de choisir lequel de ces deux derniers maux est préféré à l'autre, car il s'avère impossible de les éliminer tous les deux complètement.

Toutefois, ces problèmes peuvent devenir plus prononcés et avoir un impact plus important lorsque les systèmes de filtrage sont appliqués au réseau Internet public et imposés à l'ensemble des internautes sur un territoire donné. Ils constituent dès lors une problématique significative pour la société, considérée dans son ensemble. Puisque le contrôle ou le débat public entourant la mise en œuvre de ces systèmes est souvent réduit à son minimum, lorsqu'il n'est pas en outre inadapté, et que cette mise en œuvre a lieu sans la permission

[13] Le « traffic shaping » (aussi connu sous le terme de « packet shaping ») est le contrôle du trafic d'un réseau informatique, dans le but d'optimiser ou de garantir les performances, une latence plus basse et/ou d'augmenter la bande passante utilisable, en retardant les paquets qui correspondent à certains critères. Plus particulièrement, le traffic shaping désigne toute action sur un groupe de paquets (souvent appelé « stream » ou « flow »), qui impose un délai supplémentaire à ces paquets pour qu'ils se conforment à une contrainte prédéterminée (contractuelle ou liée à un certain type de trafic). [Wikipedia].

[14] En télécommunications, le service triple play est un terme marketing désignant la fourniture, par l'intermédiaire d'une seule connexion haut débit, de deux services consommateurs de bande passante que sont l'accès haut débit à Internet et les services de télévision, et d'un service moins consommateur de bande passante (mais plus sensible aux latences) qui est le téléphone. Le triple play répond surtout à un modèle économique, plutôt qu'à un souci de résoudre des problématiques techniques ou de se diriger vers un standard commun.

[15] Un faux-positif est un élément qui ne devrait pas être bloqué mais qui l'est en pratique par le filtre, car ce dernier le note comme étant positif. Puisque ce résultat positif est incorrect, on parle de faux-positif.

directe des utilisateurs des services Internet concernés, il est nécessaire que ces systèmes soient conçus, développés, gérés, mis en œuvre et audités d'une manière bien plus transparente et responsable.

Par exemple, l'une des différences clefs qui existent entre le filtrage d'un message électronique non sollicité (autrement dit d'un contenu qui n'a pas été requis) et le filtrage d'un site web (autrement dit d'un contenu qui a été requis), est que :

- Un message électronique qualifié spam est adressé à un serveur de messagerie connu ; en conséquence, il emprunte un seul et unique chemin, sur la fin de son parcours, pour être délivré au consommateur ;
- Une requête d'accès à un site Internet « filtré » peut emprunter un grand nombre de chemins différents sur Internet, rendant la tâche de filtrer ce site plus complexe et proche de la gageure pour le prestataire d'accès à Internet, lorsque l'utilisateur souhaite en pratique accéder à ce site.

Des systèmes empêchent également la sortie de certains types de contenus sur le réseau, ce qui peut s'avérer particulièrement utile à l'organisation qui serait très sensible à la protection de sa réputation et qui souhaiterait se protéger des impacts que pourraient avoir les activités illégales ou préjudiciables de logiciels malveillants, depuis son parc informatique, ou de ses propres employés – de manière accidentelle ou pour des raisons malveillantes.

3.2.1 Les filtrages privé et public

Internet peut être filtré de différentes manières. Le filtrage personnel et le filtrage sur réseau sont les deux principales méthodes de filtrage à être pratiquées quotidiennement. Il existe également des hybrides de ces deux méthodes.

Le filtrage mis en œuvre au niveau de l'utilisateur final permet de décider des types de contenus qui seront filtrés, sur la base de critères propres à chaque utilisateur. Il peut être adapté et configuré différemment pour répondre aux besoins de plusieurs catégories d'utilisateurs (parents, enfants, enseignants, étudiants, etc.). Ce type de filtrage est le plus précis, mais il n'empêche pas les utilisateurs d'accéder aux contenus qu'ils choisissent de voir ou de télécharger, même si ces contenus sont potentiellement illégaux.

En cas de filtrage placé sur réseau, le prestataire de service (fournisseur d'accès à Internet, employeur, club, etc.) peut déterminer les types de contenus ou d'activités à filtrer pour TOUS les utilisateurs de ce service (parfois, le système peut être configuré pour décider des critères de filtrage en fonction d'utilisateurs identifiés).

Il existe une différence majeure entre les systèmes de filtrage qui sont mis en œuvre sur le réseau dont est propriétaire un établissement d'enseignement, un club ou un employeur, et ceux qui sont mis en œuvre sur un service Internet accessible au public.

- Le club, l'établissement d'enseignement et l'entreprise ont un contrôle total de leur réseau. La configuration de ce dernier, les équipements utilisés et les logiciels qui y sont installés sont choisis par l'organisation concernée.

  En outre, chacune de ces organisations accueille une philosophie ou morale commune aux personnes qui la composent (exprimée par l'exécutif de l'entité), ainsi qu'une communauté d'utilisateurs liés par leur qualité de membre du club, d'employé de l'organisation, de membre du personnel de l'établissement d'enseignement ou d'élève de celui-ci. En conséquence, ces organisations peuvent mettre en œuvre un système de filtrage d'Internet qui tente de refléter cet ethos commun.

  Le filtrage réseau a été adopté par les entreprises et les établissements d'enseignement depuis de nombreuses années. Ces milieux se prêtent plus facilement à la mise en place de systèmes de gestion et de contrôle, puisque l'environnement entier du réseau y est sous le contrôle de l'équipe de direction.

- Le prestataire offrant un accès à Internet au public peut uniquement décider de l'équipement qui est installé et configuré sur le réseau d'accès. De nombreuses technologies différentes sont utilisées sur un réseau accessible au public, sans être placées sous le contrôle d'une organisation unique.

  Le fournisseur d'accès à Internet ne peut généralement revendiquer aucune morale commune qui représenterait les opinions partagées de l'ensemble de la population que constituent ses clients. Il garantit que le service Internet, qui est un service public, reste neutre[16]. Le choix de l'équipement et des services utilisés par les utilisateurs de son service est hors de son contrôle. L'équipement et les utilisateurs peuvent interagir de manière imprévisible. Ces utilisateurs ont des convictions personnelles très diverses et n'ont généralement que peu de traits en commun, sauf peut-être lorsqu'ils appartiennent à une même société.

  La décision de filtrer soit des contenus, soit des services, ou le choix des contenus à filtrer, ne devrait pas relever du prestataire d'accès à Internet, mais de la société qui représente les opinions des individus qui la composent. Lorsque la voie du filtrage est choisie par un prestataire d'accès à Internet, ce choix pouvant être sous-tendu par une variété de motivations ainsi que nous l'exposons dans le chapitre 4, un large éventail de

[16] Voir infra, sous-section 6.8.2.

considérations techniques doit être pris en compte, ainsi que nous l'indiquons dans le chapitre 5, de même qu'un ensemble vaste et complexe de questions et de responsabilités juridiques, qui sont détaillées dans le chapitre 6. La manière dont un conflit entre libertés peut être arbitré et les étapes qui doivent être suivies afin de s'assurer qu'une mesure de filtrage d'Internet est compatible avec les droits fondamentaux sont quant-à-elles analysées dans le chapitre 7.

Le filtrage volontaire des réseaux accessibles au public a été pratiqué de manière croissante ces dernières années. Il prend la forme d'un service rendu au consommateur, et consiste en des produits et services qui offrent à celui-ci une protection avancée. Cette option de sécurité est généralement choisie délibérément par le consommateur, selon ses inquiétudes spécifiques. Ces dernières peuvent par exemple porter sur les différents types de logiciels malveillants, la solution incluant dans ce cas un anti-spam, un anti-phishing et une protection anti-virus.

La décision des organismes concernés d'imposer certains types de filtrage sur le réseau Internet accessible au public fut prise pour la première fois il y a 20 ans, pour des raisons commerciales mais également pour le bénéfice des consommateurs et de la société. La tendance actuelle s'oriente de plus en plus vers le filtrage de ressources qui ont été sollicitées par les utilisateurs, dépassant ainsi les motivations initiales qui ont sous-tendu le filtrage de contenus (logiciels malveillants, spam, etc.).

3.3 Identifier les contenus à filtrer

Deux problématiques clefs doivent être débattues dans le cadre d'une réflexion sur le filtrage d'Internet :

- Comment spécifions-nous techniquement ce qu'il convient de filtrer ?
- Qui devrait choisir ce qui devrait être filtré sur Internet ?

3.3.1 Comment spécifions-nous techniquement ce qu'il convient de filtrer ?

Le contenu qui est filtré figure souvent dans une liste appelée liste noire (« *blocking list* »). Derrière le filtrage du spam et des logiciels malveillants, le type le plus courant de filtrage d'Internet vise les images pédopornographiques/d'abus sur enfants qui sont hébergées sur des sites web. Les contenus pouvant être filtrés sont restreints aux seuls éléments que comprend la liste noire.

De nombreuses questions doivent être débattues, afin de déterminer si imposer le filtrage d'Internet est la solution adaptée dans un pays donné.

Les processus permettant de collecter, d'examiner, d'évaluer et de cataloguer les contenus, afin d'identifier ceux d'entre eux qui devraient être bloqués, sont complexes et consommateurs de ressources. Ces processus doivent être développés, testés et mis en œuvre, et le personnel qu'ils requièrent doit être identifié et entraîné.

Différentes méthodes sont utilisées pour identifier les contenus à filtrer/bloquer.

3.3.1.1 Les listes noires (« *block-lists* »)

La méthode la plus courante consiste à utiliser une « liste noire » (« *block-list* »), qui indique les contenus qui devraient être bloqués. Une telle liste peut énumérer les contenus à filtrer de manière détaillée.

Certaines listes, appelées « listes blanches » (« *allow lists* »), indiquent les contenus appropriés à une tranche d'âge ou aux salariés d'une entreprise, et permettent de bloquer tous les contenus qui ne figurent PAS sur cette liste.

Cette liste est souvent générée et réexaminée manuellement, les contenus étant vérifiés par des professionnels entraînés.

Il existe de nombreux types de listes, ainsi qu'un grand nombre de méthodes permettant de les générer et de les distribuer. Une liste contenant des liens vers des ressources illégales est particulièrement sensible, et présente une valeur spéciale pour ceux qui sont enclins à la déviance. La sécurité et la confidentialité entourant une telle liste sont d'une importance primordiale.

Les listes noires de ressources à caractère pédopornographique qui ont été générées par l'Autorité australienne des communications et des médias ainsi que par la police finlandaise ont été divulguées sur le réseau Internet public, ce qui constitue une cause majeure d'inquiétudes. L'idée d'une base de données unique et internationale, contenant les URL d'images pédopornographiques/d'abus sur enfants, soulève des questions considérables en termes techniques, juridiques, de sécurité et d'administration.

3.3.1.2 L'identification automatique

Une deuxième méthode d'identification des ressources à filtrer consiste à analyser automatiquement le contenu des images, des textes et/ou des vidéos cibles, afin de déterminer le taux probable d'éléments préjudiciables ou illégaux que ces derniers contiennent, en utilisant des logiciels modernes sophistiqués.

3.3.1.3 Les systèmes de classification (« *Rating Systems* »)

Une troisième méthode de filtrage consiste à s'appuyer sur une classification des contenus Internet, faite de manière individuelle ou par une tierce partie. Chaque ressource est cataloguée (elle est dite « classifiée ») à la lumière de lignes directrices spécifiques et détaillées, qui permettent de déterminer le taux de nudité, de violence, de sexe ou de langage grossier que cette ressource contient. Des catégories spécifiques de contenus peuvent ensuite être bloquées en configurant le système pour les rejeter.

Il n'est pas nécessaire d'utiliser un logiciel, matériel informatique ou système réseau spécifique pour implémenter une liste noire. Les prestataires de services utilisent différentes approches techniques. Chacune de ces approches connaît différents degrés d'efficacité et d'utilité. Les différents systèmes utilisés aujourd'hui connaissent eux-mêmes des niveaux d'efficacité substantiellement différents, et il reste important de spécifier des méthodes propres à les différencier.

Certains pays préfèrent une approche « officielle », dans laquelle les prestataires d'accès à Internet n'acceptent les notifications de ressources à filtrer que de la part des services de police, ou d'un autre corps de l'Etat officiellement habilité.

Les autres pays qui bloquent actuellement l'accès aux images d'abus sur enfants hébergées à l'étranger, en dehors du Royaume-Uni, sont notamment le Canada, le Danemark, la Finlande, l'Italie (l'initiative y est prévue par des textes de droit), la Norvège et la Suède. Aux Etats-Unis, en Irlande, aux Pays-Bas et en Corée du sud, des systèmes de filtrage d'Internet sont en cours de développement.

Dans les pays qui n'ont pas encore commencé à pratiquer le filtrage, l'empressement à respecter un régime de filtrage (ou à prévoir un tel régime dans les textes de droit, comme en Italie), varie de manière significative.

3.3.2 Qui génère et distribue la liste noire (« *blocking-list* ») ?

Une deuxième problématique fondamentale est d'identifier l'organisation nationale ou internationale qui serait considérée comme ayant les compétences et la légitimité nécessaires à l'exploitation d'une base de données destinée à l'usage des autorités en charge d'émettre les notifications de contenus illégaux.

Aucune entité internationale n'a aujourd'hui de mandat pour le faire, mais certaines organisations comme Interpol ou Europol sont actives en la matière. Les pays dont l'approche est formellement législative accepteraient plus vraisemblablement qu'un tel mandat soit donné à un organisme comme Europol plutôt qu'à tout autre organisme volontaire qui n'aurait aucune autorité statutaire.

Nous retenons de l'analyse juridique détaillée proposée aux chapitres 6 et 7 que dans les pays où l'autorité judiciaire est indépendante du pouvoir législatif et du pouvoir exécutif, ce qui devrait être le cas dans toutes les démocraties libérales, seul un juge devrait avoir la compétence de constater l'illégalité d'un contenu, d'une situation ou d'une action. Ce pouvoir exclusif, prévu par le système juridique national, implique que ce contenu, cette situation ou ce comportement, soit qualifié de « potentiellement » illégal jusqu'à ce qu'un juge ait été mis en mesure de se prononcer sur la question de son illégalité. Cette situation génère l'un des défis majeurs que doivent relever les systèmes de filtrage d'Internet. Les procédures juridiques actuelles, nationales comme internationales, sont rarement adaptées au traitement des défis transfrontaliers que pose Internet ou de la vitesse de communication des services Internet. En conséquence, la participation de l'autorité judiciaire aux décisions de filtrage est rarement suffisante.

Quelque soit la méthode utilisée pour identifier et juger les contenus, il existe également un débat sur la question de la création d'une liste unique de contenus illégaux, partagée au niveau international. Certains pays considèrent qu'une telle base de données n'est ni possible ni souhaitable, compte tenu de la différence qui existe entre les législations nationales. Des défis significatifs devraient dès lors être relevés dans le cadre de la conception d'une telle liste internationale, afin de s'adapter aux divers instruments juridiques, langues et interprétations concernés. L'efficacité de cette liste pourrait en souffrir.

Les services de police scandinaves s'échangent des listes noires, ces dernières étant de fait soumises à une double validation (le service destinataire de la liste vérifie celle-ci une seconde fois, afin de s'assurer que le nouveau contenu est de prime abord illégal au regard de la loi locale). Une approche alternative pourrait en conséquence consister en un système informel d'échanges de listes noires, entre les autorités chargées de la notification des contenus qui participeraient au projet, comme en Scandinavie.

Lorsqu'une liste nationale doit être échangée entre de tels pays et d'autres qui ont opté pour l'approche judiciaire (et vice versa), il est important qu'un organe national, chargé de l'application de la loi, soit inclus dans le processus de partage des listes noires entrantes et sortantes. Toutefois, ce rôle doit être clairement défini en fonction de chaque contexte juridique national.

En l'absence d'une base de données internationale unique, certaines organisations utilisent une liste générée dans l'un de leurs pays d'origine, sans qu'il n'y ait de double validation dans le pays cible. L'utilisation d'une liste nationale compilée par d'autres gouvernements ou par des organisations multinationales dans d'autres pays est une source de nombreux problèmes, et implique que la liste soit soigneusement vérifiée. Il s'agit plus, en réalité, d'un problème juridique lié à la souveraineté et à la territorialité nationales, qu'un problème organisationnel. La situation se résume en effet à ce qu'une organisation étrangère décide de ce que les citoyens d'un pays sont autorisés à voir sur Internet. Dans tous les cas, une liste noire doit être régulièrement mise à jour afin d'assurer que des contenus légaux ne seront pas filtrés

(ce qui pourrait arriver lorsque le contenu illégal est retiré et remplacé par un contenu conforme à la loi, à la même URL).

Le réseau international de services d'assistance sur Internet (INHOPE) est actuellement financé par l'Union européenne dans le cadre du Plan d'action pour un Internet plus sûr. Cette organisation développe actuellement une base de données unifiée contenant les URL de ressources à caractère pédopornographique connues. L'objectif d'INHOPE[17] est de lutter contre les contenus et les activités illégaux en ligne, en se concentrant sur la pédopornographie. L'organisation coordonne un réseau de services d'assistance en ligne (« *hotlines* ») implantés dans plus de 30 pays. Chacun de ces services d'assistance permet aux internautes de signaler les contenus illégaux qu'ils trouvent accidentellement au cours de leur navigation sur Internet. Ces services d'assistance ont reçu plus de 500 000 signalements en 2005, 850 000 signalements en 2006 et plus d'un million de signalements en 2007, ces chiffres étant plus élevés chaque année. Les chiffres exacts pour 2008 n'ont pas encore été publiés. Cette augmentation peut être due à un plus grand nombre de personnes utilisant Internet, à un plus grand nombre de personnes signalant des contenus illégaux aux services d'assistance, ou encore à une législation plus stricte ; elle n'indique pas nécessairement une augmentation du taux d'infractions.

Toutefois, une conséquence directe de l'approche basée sur les services d'assistance en ligne est que les internautes ont à expérimenter les conséquences d'avoir vu les images concernées, avant que ces dernières ne soient signalées à un service d'assistance pour traitement. Une telle expérience peut être contrariante pour beaucoup d'individus, et peut être préjudiciable aux jeunes adultes et aux mineurs. Des recherches plus approfondies seraient nécessaires en la matière.

Une organisation qui met en œuvre des services de filtrage d'Internet en utilisant une liste noire que lui transmet le concepteur de cette liste doit réfléchir à la technologie qu'elle utilisera pour collecter, conserver, implémenter, mettre à jour et documenter cette liste.

Aucun système clefs en main ne permet aujourd'hui à un prestataire d'accès offrant ses services au public de mettre en œuvre toutes ces nécessaires fonctionnalités, dans le cadre d'une initiative de filtrage. Certains aspects de ces fonctionnalités sont toutefois disponibles dans les systèmes prêts à l'emploi destinés aux entreprises ou aux établissements d'enseignement.

Le prestataire d'accès à Internet doit donc acheter, installer, configurer, sécuriser, documenter et exploiter les logiciels et matériels informatiques nécessaires à la fourniture de tels services.

Sécurité et intégrité

Une problématique cruciale concernant les listes noires est leur sécurité et leur intégrité. De telles listes sont extrêmement recherchées par les personnes disposées à en expérimenter le contenu. Même sans compter les listes de contenus qui sont publiées sur Internet à la suite d'indiscrétions, des recherches indiquent qu'il pourrait être possible de faire de l'ingénierie inverse sur les listes utilisées par n'importe quel prestataire de services[18]. Le 26 mai 2005, le journal « The Guardian Newspaper »[19], au Royaume-Uni, signalait :

> *« Le système "BT's CleanFeed", qui empêche l'accès à un registre de sites web contenant des images d'enfants à caractère sexuel, peut également être utilisé pour découvrir les contenus que comprend la liste noire secrète, selon de nouvelles recherches.*

[17] http://www.inhope.org.
[18] Richard Clayton, « Failures in a Hybrid Content Blocking System » (« Pannes dans un système hybride de filtrage des contenus »), www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.
[19] http://www.guardian.co.uk/technology/2005/may/26/onlinesupplement (visité pour la dernière fois le 1er septembre 2009).

Les personnes techniquement compétentes qui utilisent le service d'accès à Internet de BT peuvent utiliser le système pour identifier les sites qui se trouvent bloqués, déclare Richard Clayton, autrefois expert Internet auprès du prestataire de services Demon et actuellement doctorant au sein du laboratoire informatique de l'Université de Cambridge. Cela signifie qu'ils sont à même d'avoir accès à une liste noire secrète, fournie par le groupe de veille Internet Watch Foundation (IWF).

Clayton dit que CleanFeed peut être utilisé comme un "oracle" pour obtenir les adresses des sites listés par IWF – en le transformant en réalité en un index de pédopornographie ».

Le filtrage de la pédopornographie sur Internet ne conduit pas à faire cesser les abus sur enfants. Il n'entraîne pas la disparition des images ou leur retrait du réseau.

Il rend parfois plus difficile l'accès à ce type de contenus (selon le système de filtrage retenu), en sorte que seules les personnes les plus déterminées et les plus techniquement averties pourront le trouver (en fonction du logiciel client utilisé). Lorsque les images comprennent des informations permettant d'identifier les victimes, leur filtrage peut également protéger ces dernières d'un nouveau sentiment d'exploitation. Réciproquement, le propriétaire du contenu peut distribuer ce même contenu en utilisant une adresse différente ou par l'intermédiaire d'un autre protocole Internet, ce qui rendra le contenu de nouveau accessible. Cette problématique est discutée plus en détail au chapitre 5 de la présente étude.

Le filtrage d'Internet peut être de nature à faire baisser les flux d'argent à destination des organisations criminelles qui exploitent des sites web à caractère commercial afin de vendre des images d'abus sur enfants dans un but lucratif. Cette circonstance est discutée plus avant au chapitre 4 de la présente étude, car le filtrage peut également aider les délinquants à rester « un pas en avant », en leur montrant qu'ils ont été identifiés comme fournissant des ressources illégales.

La réponse la plus efficace qui puisse être apportée à la pédopornographie/aux images d'abus sur enfants est le retrait de ces dernières du réseau Internet, accompagné d'investigations pénales concernant le producteur des images et d'initiatives aux fins de retirer l'enfant de la situation

EXEMPLE D'UN PAYS – LE ROYAUME-UNI

Au Royaume-Uni, la liste noire de l'Internet Watch Foundation (IWF) a été utilisée par divers membres de l'IWF dans le cadre d'un filtrage, basé sur serveur, d'images d'abus sur enfants. A la fin de l'année 2007, le Ministère de l'intérieur a souhaité que tous les prestataires d'accès à Internet « offrant une connectivité Internet haut-débit au public du Royaume-Uni » mettent en œuvre un tel système. Dans l'hypothèse où cet objectif ne serait pas atteint, le gouvernement s'est réservé le droit de reconsidérer la législation en conséquence.

Dans l'approche du Royaume-Uni, un service d'assistance en ligne, qui est un organisme non gouvernemental et non une autorité en charge de l'application de la loi, fournit directement une liste aux prestataires d'accès à Internet qui en sont membres, en la considérant comme étant l'un des « bénéfices » attachés cette qualité de membre. L'approche de l'IWF a été reprise et adaptée dans d'autres juridictions (comme au Canada). L'IWF procède également à des échanges avec d'autres organisations internationales, dans le cadre d'accords bilatéraux.

Certains membres de l'IWF utilisent la liste pour filtrer les accès de leurs clients dans d'autres juridictions. Au moins un opérateur de télécommunications utilise la liste de l'IWF sur l'ensemble de son réseau européen (il compte parmi les prestataires de services Internet qui sollicitent une « liste européenne » (« *EU-wide list* »).

British Telecom (BT), au Royaume-Uni, fait la promotion active de son système de filtrage d'URL, communément appelé « BT Cleanfeed » (et qui utilise la liste de l'IWF), et met sa technologie à disposition d'autres organisations à l'intérieur du Royaume-Uni et partout dans le monde, sous accord de confidentialité. Le nombre d'organisations qui utilisent cette technologie reste incertain, de même que les pays dans lesquels ces organisations opèrent, et les bases sur lesquelles elles obtiennent la liste de sites à filtrer.

abusive où il se trouve, pour lui prodiguer des soins et lui permettre de récupérer dans un environnement sécurisé.

A la lumière du contexte dans lequel le filtrage d'Internet prend place, il est clair qu'une telle mesure ne peut constituer que l'un des éléments d'une approche plus large, destinée à lutter contre la disponibilité et l'accessibilité en ligne de ressources à caractère pédopornographique. Les autres composantes de cette approche sont l'activité des autorités en charge de l'application de la loi, les services d'assistance en ligne pour le signalement des images d'abus sur enfants, et des programmes pédagogiques.

Néanmoins, divers éléments fonctionnent de concert pour fournir une série de solutions complémentaires, dans le cadre de la lutte contre le problème de la disponibilité sur Internet de ressources à caractère pédopornographique.

Malheureusement, certains des contenus illégaux ayant trait à la pédopornographie et disponibles sur des sites web sont actuellement hébergés dans des pays et auprès de prestataires d'hébergement Internet dont la législation nationale comme le contrôle et l'intervention politiques ne sont pas comparables aux bonnes pratiques actuelles, au regard des standards internationaux. Les procédures de notification directe et de retrait (« *notice-and-take-down* ») des contenus que connaissent ces pays et ces hébergeurs sont également trop peu développées, ou ne fonctionnent pas. Les initiatives destinées à répondre à ces problématiques doivent être encouragées.

Ceci dit, un large volume de ces contenus est également localisé dans des pays qui ont les meilleurs systèmes juridique, réglementaire et d'investigations pénales au monde, mais qui échouent pour l'heure à en empêcher la distribution sur Internet.

Les raisons exactes de cette situation ne sont pas extrêmement claires, bien qu'elles soient souvent attribuées aux différentes philosophies qui entourent les objectifs et les stratégies des autorités en charge de l'application de la loi. Par exemple, certaines de ces dernières mettent l'accent sur l'identification, l'arrestation et la poursuite des responsables d'abus sur enfants, qu'elles font passer avant la prévention de la distribution des contenus, et avant la protection des enfants victimes par le retrait du contenu qui se trouve en ligne. Dès lors, les sites web peuvent rester accessibles et être maintenus en ligne sur une longue période de temps avant leur retrait. C'est particulièrement vrai dans les juridictions qui autorisent les investigations sous couverture. D'autres autorités en charge de l'application de la loi renversent la priorité et cherchent à obtenir le retrait des contenus et à prévenir la revictimisation en ligne des enfants qui figurent dans les images, priorités qu'elles font passer avant les investigations destinées à retrouver les auteurs d'infractions. Bien que les deux stratégies cherchent à atteindre le même objectif final – le retrait des contenus ET la poursuite des auteurs d'infractions, les différentes manières de procéder peuvent être la cause de difficultés sur Internet.

Il est important de noter la nature intrusive de nombreuses stratégies de filtrage, parmi celles qui ont été discutées dans le présent chapitre. Ceci est particulièrement vrai des mécanismes les plus précis de filtrage de contenus, qui requièrent l'analyse du contenu échangé entre les utilisateurs. Cette situation est problématique tant en termes d'investissements (les investissements requis sont invariablement élevés, dans ce type de scénarios), que dans le cadre d'une approche plus large, sociétale.

La proportionnalité d'une mesure de filtrage est généralement difficile à évaluer, car elle dépend essentiellement du « but légitime »[20] particulier qu'il s'agit de préserver dans le cadre de chaque situation factuelle, de l'utilité de la mesure pour atteindre ce but légitime dans des circonstances particulières, et des caractéristiques du mécanisme de filtrage et de leur impact sur les autres droits et libertés.

[20] Voir infra, section 7.4.

Les conséquences d'une mesure de filtrage d'Internet en termes d'ingérence dans l'exercice des libertés fondamentales sont mises en lumière au chapitre 6 de la présente étude. Toutefois, plusieurs mesures de filtrage peuvent autoriser des ingérences additionnelles, en raison de la nature des mécanismes qui sont utilisés pour les mettre en œuvre.

Toute mesure qui constitue une ingérence dans l'exercice de certaines libertés doit voir sa proportionnalité évaluée, en premier lieu, au regard du but légitime qui lui a été assigné, et, en second lieu, au regard de son effet général, lequel ne doit pas aller au delà de ce qui est nécessaire pour atteindre le but poursuivi et, dans tous les cas, lequel doit « *ménager un certain périmètre* » pour l'exercice de la liberté qui se voit ainsi limitée, et non « *provoquer (l') extinction* » de cette dernière.

En conclusion, chaque fois qu'une mesure de filtrage est autorisée en raison de son utilité à préserver un intérêt légitime, son fonctionnement le plus basique ne doit pas limiter les autres libertés d'une manière disproportionnée, et certaines garanties doivent être prises afin que cette mesure ne soit pas utilisée d'une manière qui pourrait menacer ces libertés encore plus avant.

Dans tous les cas, il doit être noté qu'aucune des stratégies identifiées dans le présent rapport ne semble être en mesure de prévenir complètement le sur-blocage (ou filtrage excessif). Cette problématique est de première importance lorsqu'il s'agit d'équilibrer, d'une part le besoin de filtrer les contenus à caractère pédopornographique, et d'autre part le besoin de respecter les droits de l'Homme et la libre expression. Il semble inévitable que des contenus légaux soient bloqués, là où le filtrage est mis en œuvre.

En outre, puisque les contenus électroniques peuvent être échangés par l'intermédiaire de différentes technologies Internet, la pratique de n'appliquer le filtrage qu'à un nombre limité de ces technologies (telle que celle de ne filtrer que le trafic en direction des serveurs web) pourrait sans aucun doute conduire à l'utilisation d'une méthode alternative de distribution de ces contenus. Ceux qui ont à l'esprit de distribuer des contenus illégaux par l'intermédiaire d'Internet disposent d'une myriade d'options pour le faire, en dépit des mesures de filtrage mises en place. D'un point de vue technique, les initiatives de filtrage ne peuvent, en conséquence, qu'assurer la protection des personnes qui pourraient accéder aux contenus par inadvertance. Il semble improbable que les stratégies de filtrage, ainsi que nous le montrons dans le présent document, soient en mesure de prévenir efficacement ou de manière substantielle les infractions ou la « revictimisation ».

Les initiatives de filtrage de contenus peuvent être considérées comme un acte de reterritorialisation, lorsque l'objectif d'un pays est de s'assurer que ses normes nationales s'appliquent à l'ensemble du contenu disponible sur Internet, pour les personnes qui utilisent Internet sur son territoire.

Alors qu'il est important qu'un débat public prenne place, ce débat devra tenir compte des différences fondamentales, d'ordre technique et juridique, qui existent entre chaque type de contenu, ainsi que de la question de la proportionnalité du filtrage, par rapport à d'autres méthodes permettant de réduire les dommages, de prévenir les infractions, ou de procéder à des investigations en matière de cybercriminalité.

Tous les types de filtrage sont différents, tous les types de contenus sont différents, et tous les types d'infractions sont différents.

3.4 Terminologie de base

Interception	Surveillance, sur injonction d'une juridiction de l'ordre judiciaire [ou de toute autre autorité habilitée, *ndlt*], de l'ensemble du trafic émis et reçu par un suspect donné [ou d'une part de ce trafic, *ndlt*].
Procédure de notification et de retrait (« *notice and take down* »)	Procédure par laquelle une entité bien informée et de confiance notifie à un prestataire de services Internet l'existence d'un contenu sur ses serveurs, en lui indiquant la localisation exacte de ce dernier et les raisons juridiques pour lesquelles il devrait être retiré.
Pédopornographie[21]	(a) « enfant » signifie toute personne âgée de moins de dix-huit ans ; (b) « pédopornographie » signifie tout matériel pornographique représentant de manière visuelle : (i) un enfant réel participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne d'un enfant, ou (ii) une personne réelle qui paraît être un enfant participant ou se livrant au comportement visé au point i), ou (iii) des images réalistes d'un enfant qui n'existe pas participant ou se livrant au comportement visé au point i) ; (c) « système informatique » signifie tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données; (d) « personne morale » signifie toute entité ayant ce statut en vertu du droit applicable, exception faite des États ou des autres entités publiques dans l'exercice de leurs prérogatives de puissance publique et des organisations internationales publiques.
Images d'abus sur enfants	Voir ci-dessus.
Fournisseur de contenu	Un fournisseur de contenu est une organisation/un utilisateur qui met une information à disposition d'une audience Internet cible. Il peut s'agir d'un simple individu connaissant bien certains aspects d'une région géographique donnée, d'un petit groupe de personnes liées par un intérêt particulier, ou une importante société commerciale ayant des produits à vendre. Avec l'arrivée du web 2.0, de nombreux utilisateurs finaux sont devenus des fournisseurs de contenus de leur propre chef. En conséquence, la qualité de fournisseur de contenu doit être divisée en deux sous-catégories, celle des fournisseurs professionnels de contenus, tels qu'une entreprise de presse, et celle des fournisseurs de contenus non-professionnels, tels que les internautes depuis leur domicile.

[21] Cette définition provient de la décision cadre du Conseil de l'Union européenne du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie, disponible à l'adresse : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:FR:HTML.

Prestataire ou fournisseur d'accès à Internet (FAI)	Fournisseurs d'un accès à Internet, sur demande ou dédié (et d'un accès aux services Internet tels que la messagerie électronique, les groupes de news du réseau Usenet, etc. Toutefois, les prestataires de messagerie électronique peuvent ne pas être prestataires d'accès ou prestataires de news. Un utilisateur peut également utiliser un service de messagerie qui n'est pas fourni par son fournisseur d'accès).
Prestataire ou fournisseur d'hébergement Internet	Organisation permettant à des tiers de localiser leurs ordinateurs directement sur Internet en utilisant ses points d'accès au réseau. En général, cette organisation n'opère pas directement une connexion réseau, mais utilise le réseau existant d'un prestataire d'accès à Internet ou d'un opérateur de télécommunications. [Un prestataire d'hébergement peut encore posséder ses propres serveurs et offrir sur ces derniers, à titre gratuit ou onéreux, un espace permettant à autrui d'y localiser les informations qu'il souhaite y stocker, *ndlt*].
Contenu illégal	Contenu internet qui est clairement considéré comme illégal au regard de la loi, et qui est déclaré comme tel par une autorité compétente.
Contenu préjudiciable	Contenu qui est subjectivement ressenti comme portant préjudice. Le niveau de préjudice dépend de la nature du contenu et de la maturité physique, émotionnelle et spirituelle de la personne qui voit ce contenu préjudiciable.
SPAM	Message non sollicité.
URL (Uniform Resource Locator)	Nom d'une séquence de caractères qui identifie précisément le protocole, le nom de domaine, le nom de sous-domaine, les différents répertoires et sous-répertoires, le nom du fichier, le type d'extension du fichier, et, si besoin, les paramètres d'information accédée qui sont retournés via un formulaire web, permettant de récupérer et d'afficher une page web.
DNS (Domain Name System)	Service qui traduit les noms de sites web, qui consistent généralement en une suite de caractères alphanumériques, en séquences de nombres plus connues sous le terme d'« adresses IP ».
Adresse IP (Internet Protocol)	Adresse numérique qui identifie un ordinateur au sein d'un réseau d'ordinateurs donné.
Prestataire ou fournisseur de services Internet	Entreprise qui offre des services Internet à ses clients.
Attaque DDOS (Distributed Denial of Service)	Cyber attaque consistant à adresser tellement de requêtes à un serveur que ce dernier cesse de fonctionner sous le volume du trafic.

Réseau Zombie (« *Botnet* »)	Ensemble d'ordinateurs configurés pour transmettre des messages à d'autres ordinateurs, sur ordre, généralement pour des raisons malveillantes.
Logiciel malveillant (« *Malware* »)	Logiciel malveillant, conçu pour s'infiltrer dans l'ordinateur, pour endommager ce dernier ou pour y collecter des informations personnelles, sans que l'utilisateur en ait conscience.
Cheval de Troie	Logiciel malveillant qui apparaît comme offrant des fonctionnalités utiles, alors qu'il est en fait en train de s'infiltrer dans l'ordinateur.

Chapitre 4 LE DEBAT RELATIF AU FILTRAGE D'INTERNET ET SES MOTIVATIONS

Le débat relatif au « filtrage d'Internet » ne peut pas être limité à une problématique unique. Ce débat est aussi complexe que le sujet lui-même. Le présent chapitre passe en revue les aspects généraux des choix qui s'y présentent. Dans ce contexte, son approche structurée permet de mettre en exergue les très divers domaines de préoccupations et les défis auxquels doivent faire face les décideurs politiques, dans le cadre des réponses qu'ils apportent aux problèmes posés par les contenus électroniques.

L'objet est de souligner l'éventail complexe des approches et des motivations qui sous-tendent les initiatives de filtrage d'Internet, afin de permettre une comparaison de ces différentes approches.

La section 4.2 s'attache à l'analyse de l'endroit où, sur Internet, le filtrage peut être tenté. La section 4.3 se concentre sur la personne qui choisit ce qui devrait être bloqué, et sur les niveaux de connaissances et de compétences que doivent posséder les différents utilisateurs et organisations qui entendent organiser le filtrage de contenus électroniques. La section 4.4 propose une description des différents problèmes que suscitent les contenus électroniques sur Internet et de la manière dont certains gouvernements en arrivent à considérer le filtrage comme constituant une réponse possible à ces problèmes. La section 4.5 trace les contours des motivations premières qui conduisent les décideurs politiques à envisager le filtrage d'Internet, et des raisons pour lesquelles, dans certains cas, des approches alternatives apparaissent avoir échoué. La section 4.6 se concentre sur les cibles des initiatives de filtrage – soit les producteurs, soit les consommateurs de contenus illégaux - et s'attache à décrire l'effet de l'initiative de filtrage sur ces cibles. La section 4.7 récapitule clairement les conclusions qui peuvent être tirées de cette recherche concernant le filtrage d'Internet. Enfin, la section 4.8 énumère brièvement un certain nombre de pays qui, de par le monde, ont déjà mis en place des mesures de filtrage d'Internet.

4.1 Les lieux où la question du filtrage d'Internet est débattue

4.1.1 Le milieu académique

Le filtrage fait actuellement l'objet d'intenses discussions dans l'enceinte académique[22]. La discussion n'y est pas limitée aux aspects juridiques du filtrage, mais en couvre également les aspects techniques[23].

4.1.2 L'Union européenne

La question de savoir si les fournisseurs d'accès à Internet devaient ou non être contraints d'empêcher les utilisateurs de leurs services de mettre à disposition ou de télécharger des fichiers protégés par le droit d'auteur par l'intermédiaire de systèmes de partage de fichiers a fait l'objet d'une controverse à l'occasion du débat sur la réforme de la législation sur les télécommunications[24]. Suite aux critiques formulées par le Parlement européen à l'encontre de telles obligations[25], la Commission décida de ne pas inclure celles-ci dans le texte de loi

---

[22] Deibert, Palfrey, Rohozinski et Zittrain, Access Denied : The Practice and Policy of Global Internet Filtering (Accès refusé : la pratique et la politique de filtrage mondial d'Internet), 2008 ; Lonardo, « Italy: Service Provider's Duty to Block Content » (« Italie : le devoir des prestataires de services de filtrer les contenus»), Computer Law Review International, 2007, pages 89 et s. ; Sieber et Nolde, Sperrverfuegungen im Internet, 2008 ; Gercke, « The Role of Internet Service Providers in the Fight Against Child Pornography » (« Le rôle des prestataires de services Internet dans la lutte contre la pédopornographie »), Computer Law Review International, 2009, pages 65 et s. ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, Filteren van kinderporno op internet, 2008 ; Edwards et Griffith, « Internet Censorship and Mandatory Filtering » (« La censure d'Internet et le filtrage imposé »), NSW Parliamentary Library Resarch Service, nov. 2008 ; Zittrain et Edelman, « Documentation of Internet Filtering Worldwide » (« Présentation de l'état du filtrage d'Internet à travers le monde »), disponible à l'adresse : http://cyber.law.harvard.edu/filtering/ ; Reidenberg, « States and Internet Enforcement » (L'Etat et la régulation d'Internet »), University of Ottawa Law & Technology Journal, Vol. 1, n° 213, 2004, pages 213 et s., disponible à l'adresse : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965 ; S'agissant de la discussion relative au filtrage dans différents pays, voir : Taylor, « Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime » (« Les prestataires de services Internet et leur responsabilité au regard des contenus dans le nouveau régime français »), Computer Law & Security Report, vol. 20, fascicule (issue) 4, 2004, pages 268 et s. ; « Belgium ISP Ordered By The Court To Filter Illicit Content » (« Les prestataires d'accès à Internet contraints par une juridiction de filtrer les contenus illicites ») , EDRI News, n° 5.14, 18 juin 2007, disponible à l'adresse : http://www.edri.org/edrigram/number5.14/belgium-isp ; Enser, « Illegal Downloads : Belgian court orders ISP to filter » (« Téléchargements illégaux : une juridiction Belge impose le filtrage aux FAI »), OLSWANG E-Commerce Update, nov. 2007, page 7, disponible à l'adresse : http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf ; Standford, « France to Require Internet Service Providers to Filter Infringing Music » (« La France demande aux fournisseurs d'accès à Internet de filtrer la musique contrefaite »), 27 nov. 2007, Intellectual Property Watch, disponible à l'adresse : http://www.ip-watch.org/weblog/index.php?p=842 ; Zwenne, « Dutch Telecoms wants to force Internet safety requirements » (« Le régulateur des télécommunications néerlandais veut imposer des règles de sécurité sur Internet »), Wold Data Protection Report, fascicule (issue) 09/07, page 17 – disponible à l'adresse : http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf ; Le document de L'IFPI de 2007 concernant les options techniques permettant de lutter contre les violations du droit d'auteur en ligne (Technical options for addressing online copyright infringement) – disponible en anglais à l'adresse : http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf ; S'agissant des approches d'auto-régulation voir : « ISPA Code Review : Self-Regulation of Internet Service Providers » (« Examen du Code de l'association des prestataires de services Internet : auto-régulation des prestataires de services Internet »), 2002, disponible à l'adresse : http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf ; Zittrain, Harvard Journal of Law & Technology, 2006, vol. 19, n° 2, pages 253 et s.

[23] Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008, pages 50 et s. ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008, pages 10 et s. ; Pfitzmann, Koepsell et Kriegelstein, « Sperrverfuegungen gegen Access-Provider, Technisches Gutachten », disponible à l'adresse : http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrervuegungen.pdf ; Pursch et Baer, « Sperrverfuegungen gegen Internet-Provider », Deutscher Bundestag, Wissenschaftlicher Dienst, 2009, disponible à l'adresse : http://www.ccc.de/press/releases/2009/20090212/bundestag_filter-gutachten.pdf ; Clayton, Murdoch et Watson, « Ignoring the Great Firewall of China » (« Passer outre le grand pare-feu de la Chine »), disponible à l'adresse : http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf ; Ayre, *Internet Filtering Options Analysis : An Interim Report (Analyse des options de filtrage d'Internet : un rapport provisoire)*, 2006.

[24] Horten, « The Telecoms Package and "3 strikes" – voluntary cooperation to restrict downloads » (« Le Paquet Télécom et le modèle des 3 avertissements - coopération volontaire pour limiter le téléchargement »), 2008.

[25] Vote du Parlement européen du 24 septembre 2008.

présenté en novembre 2008[26]. Le débat fut récemment rouvert dans le cadre des discussions sur de nouvelles initiatives législatives en matière de commerce électronique. En outre, la proposition[27] de décision cadre du Conseil de l'Union européenne relative à la lutte contre la pédopornographie et abrogeant la décision-cadre 2004/68/JAI, qui fut présentée en mars 2009 par la Commission, prévoit par exemple l'obligation, pour les Etats membres, de prendre les mesures nécessaires permettant aux autorités judiciaires ou policières compétentes d'ordonner, ou d'obtenir par un moyen similaire, le blocage de l'accès par les internautes aux pages internet contenant ou diffusant de la pédopornographie[28].

4.1.3 Le Conseil de l'Europe

La question du filtrage a été intensément discutée dans le cadre de l'élaboration des « lignes directrices visant à aider les fournisseurs de services Internet »[29], de même que dans le cadre de l'élaboration de la « recommandation sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres Internet »[30], et reste à l'agenda du Conseil de l'Europe.

Dialogue européen sur la gouvernance d'Internet de 2009/Forum 2009 sur la gouvernance d'Internet

Le filtrage des contenus illégaux a été discuté au sein de l'atelier n° 4, durant le dialogue européen sur la gouvernance d'Internet[31], et sera l'un des sujets qui seront débattus lors de l'IGF [*Internet Governance Forum* - Forum sur la gouvernance d'Internet, *ndlt*] 2009.

[26] Voir le communiqué de presse de la Commission, « Réforme du cadre des télécommunications : la Commission présente de nouveaux textes législatifs pour préparer la voie à un compromis entre le Parlement et le Conseil », 7 nov. 2008.

[27] Proposition de décision-cadre du Conseil relative à l'exploitation et aux abus sexuels concernant les enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI, COM (2009) 135.

[28] Article 18 – Blocage de l'accès aux sites internet contenant de la pédopornographie : « *Chaque État membre prend les mesures nécessaires pour permettre aux autorités judiciaires ou policières compétentes d'ordonner ou d'obtenir par un moyen similaire le blocage de l'accès par les internautes aux pages internet contenant ou diffusant de la pédopornographie, sous réserve de garanties appropriées, notamment pour faire en sorte que le blocage soit limité au strict nécessaire, que les utilisateurs soient informés de la raison de ce blocage et que les fournisseurs de contenu soient informés de la possibilité de le contester* ».

[29] Lignes directrices visant à aider les fournisseurs de services Internet, développées par le Conseil de l'Europe en coopération avec l'Association européenne des fournisseurs de services Internet (EuroISPA), 2008.

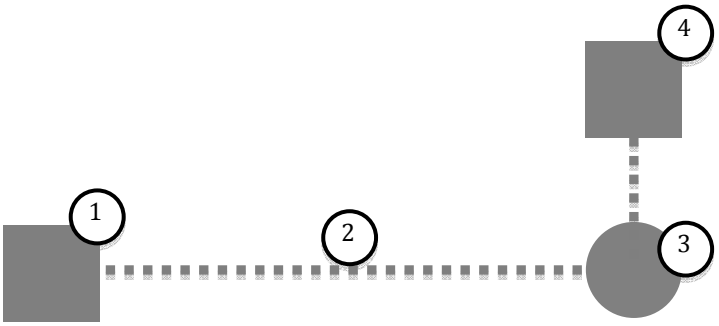
[30] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, adoptée par le Comité des Ministres le 26 mars 2008 lors de la 1022e réunion des Délégués des Ministres.

[31] L'« EuroDIG » s'est déroulé à Genève les 14 et 15 septembre 2009.

4.2 L'endroit, sur Internet, où le filtrage peut être entrepris

L'un des critères pouvant être utilisés pour différencier les différentes approches qui sous-tendent le filtrage est la cible de l'outil de filtrage. Il existe en général quatre cibles de filtrage différentes, correspondant aux approches suivantes :

- L'approche basée sur le service ;
- L'approche basée sur le contenu ;
- L'approche basée sur l'utilisateur ;
- L'approche basée sur les moteurs de recherche.



4.2.1 L'approche basée sur le service

En premier lieu, l'une des approches les plus populaires est le filtrage de sites web, qui est particulièrement discuté dans le contexte du filtrage de la pédopornographie[32], et qui cible les services Internet. Puisque le fournisseur d'accès à Internet est responsable de la transmission des requêtes d'accès à un site web que forment les utilisateurs, il est techniquement capable

[32] S'agissant des obligations/approches relatives aux filtres, voir Lonardo, « Italy: Service Provider's Duty to Block Content » (« Italie : le devoir des prestataires de services de filtrer les contenus»), Computer Law Review International, 2007, pages 89 et s. ; Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008 ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008 ; Edwards et Griffith, « Internet Censorship and Mandatory Filtering » (« La censure d'Internet et le filtrage imposé »), NSW Parliamentary Library Resarch Service, nov. 2008 ; Zittrain et Edelman, « Documentation of Internet Filtering Worldwide » (« Présentation de l'état du filtrage d'Internet à travers le monde »), disponible à l'adresse : http://cyber.law.harvard.edu/filtering/ ; Reidenberg, « States and Internet Enforcement » (« L'Etat et la régulation de l'Internet »), University of Ottawa Law & Technology Journal, vol. 1, n° 213, 2004, pages 213 et s., disponible à l'adresse : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965 ; S'agissant de la discussion relative au filtrage dans différents pays, voir Taylor, « Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime » (« Les prestataires de services Internet et leur responsabilité au regard des contenus dans le nouveau régime français »), Computer Law & Security Report, vol. 20, fascicule (issue) 4, 2004, pages 268 et s. ; « Belgium ISP Ordered By The Court To Filter Illicit Content » (« Les prestataires d'accès à Internet contraints par une juridiction de filtrer les contenus illicites »), EDRI News, n° 5.14, 18 juin 2007, disponible à l'adresse : http://www.edri.org/edrigram/number5.14/belgium-isp ; Enser, « Illegal Downloads: Belgian court orders ISP to filter » (« Téléchargements illégaux : une juridiction Belge impose le filtrage aux FAI »), OLSWANG E-Commerce Update, nov. 2007, page 7, disponible à l'adresse : http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf ; Standford, « France to Require Internet Service Providers to Filter Infringing Music » (« La France demande aux fournisseurs d'accès à Internet de filtrer la musique contrefaite »), 27 nov. 2007, Intellectual Property Watch, disponible à l'adresse : http://www.ip-watch.org/weblog/index.php?p=842 ; Zwenne, « Dutch Telecoms wants to force Internet safety requirements » (« Le régulateur des télécommunications néerlandais veut imposer des règles de sécurité sur Internet »), Wold Data Protection Report, fascicule (issue) 09/07, page 17, disponible à l'URL : http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf ; Le document de L'IFPI de 2007 concernant les options techniques permettant de lutter contre les violations du droit d'auteur en ligne (Technical options for addressing online copyright infringement), disponible en anglais à l'adresse : http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf ; S'agissant des approches d'autorégulation, voir « ISPA Code Review : Self-Regulation of Internet Service Providers » (« Examen du Code de l'association des prestataires de services Internet : auto-régulation des prestataires de services Internet »), 2002, disponible à l'adresse : http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf ; Zittrain, Harvard Journal of Law & Technology, 2006, vol. 19, n° 2, pages 253 et s.

de vérifier (les considérations juridiques faisant l'objet d'une analyse séparée) si ce site web figure ou non sur une liste noire (« *block-list* »). Différentes solutions techniques permettant de s'assurer que les sites web connus seront bloqués font actuellement l'objet de discussions. Ces solutions vont de la manipulation du serveur de noms de domaine (DNS) et de l'utilisation de serveurs proxy à des solutions hybrides qui combinent différentes approches[33]. Les aspects techniques de ces approches sont détaillés au chapitre 5.

4.2.2 L'approche basée sur le contenu

Une deuxième approche consiste à filtrer certains contenus pendant le processus de leur transfert. A la condition que l'utilisateur ne transmette pas ou ne reçoive pas de contenus chiffrés, le prestataire d'accès à Internet a, à tout le moins dans certains cas, la possibilité technique (les considérations juridiques faisant l'objet d'une analyse séparée) d'analyser le contenu transmis. Cette approche est différente de l'approche basée sur le service que nous avons mentionnée plus haut, laquelle est limitée à des services connus qui sont inscrits sur une liste noire (« *block-list* »). A l'instar du prestataire d'hébergement (en ce qui concerne les contenus qui sont mis à disposition sur ses serveurs), le prestataire d'accès pourrait utiliser des techniques de recherche basées sur des valeurs de hachage afin d'identifier les images connues de pédopornographie[34], ou des techniques de recherche par mots-clefs[35].

4.2.3 L'approche basée sur l'utilisateur

En troisième lieu, les prestataires d'accès à Internet ont, dans une certaine limite, la possibilité technique d'empêcher les consommateurs d'utiliser leurs services. S'ils ajoutent un consommateur à une liste noire - « *block list* » - (les considérations juridiques faisant l'objet d'une analyse séparée), ce dernier ne sera plus en mesure d'utiliser leurs services, dans le futur, pour commettre des infractions.

Un exemple d'une telle approche, s'agissant d'un prestataire d'hébergement, est l'affaire qui a impliqué le fournisseur d'hébergement Yahoo! en 2001, lequel s'est vu ordonner par une juridiction française (alors qu'il était basé aux Etats-Unis) d'empêcher l'accès des utilisateurs français à des contenus nazis[36]. L'approche basée sur l'utilisateur a également été discutée

---

33 Pour un panorama des aspects techniques, voir Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008, pages 50 et s. ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008, pages 10 et s. ; Pfitzmann, Koepsell et Kriegelstein, « Sperrverfuegungen gegen Access-Provider, Technisches Gutachten », disponible à l'adresse : http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrervuegungen.pdf ; Pursch et Baer, « Sperrverfuegungen gegen Internet-Provider », Deutscher Bundestag, Wissenschaftlicher Dienst, 2009, disponible à l'adresse : http://www.ccc.de/press/releases/2009/20090212/bundestag_filter-gutachten.pdf ; Clayton, Murdoch et Watson, « Ignoring the Great Firewall of China » (« Passer outre le grand pare-feu de la Chine »), disponible à l'adresse : http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf ; Ayre, *Internet Filtering Options Analysis : An Interim Report (Analyse des options de filtrage d'Internet : un rapport provisoire)*, 2006.

34 Gordon, Hosmer, Siedsma et Rebovich, *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime* (*Evaluation des technologies, des méthodes et des informations permettant de commettre des infractions en ligne et de lutter contre la cybercriminalité*), 2002, page 57 ; Forsyth, Malik, Fleck, Greenspan, Leung, Belongie, Carson et Bregler, « Finding Pictures of Objects in Large Collections of Images » (« Identifier des photos et des objets au sein d'une large collection d'images »), Proceedings of the International Workshop on Object Representation in Computer Vision II, 1996, pages 335 et s. ; *Pornography Image – Filter Effectiveness* (*Images pornographiques – efficacité des filtres*), Pinkblock Whitepaper, 2007, disponible à l'adresse : http://www.pinkblock.com/downloads/Filter%20Effectiveness%5B1%5D.pdf.

35 Voir Vacca, *Computer Forensics, Computer Crime Scene Investigation* (*Informatique légale, Investigation d'une scène de crime informatique*), 2ème éd., 2005, page 48 ; Lange et Nimsger, *Electronic Evidence and Discovery* (*administration des preuves électroniques*), 2004, 9 ; Gordon, Hosmer, Siedsma et Rebovich, *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime* (*Evaluation des technologies, des méthodes et des informations permettant de commettre des infractions en ligne et de lutter contre la cybercriminalité*), 2002, page 63.

36 Voir Greenberg, « A Return to Lilliput : The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market » (« Un retour sur Lilliput : l'affaire Licra c/ Yahoo! et la réglementation des contenus en ligne dans le marché mondial »), Berkeley Technology Law Journal, vol. 18, page 1191 et s. ; Van Houweling, « Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra » (« Application des jugements étrangers, le Premier amendement et l'expression sur Internet : note pour la prochaine affaire Yahoo! c/ Licra »), Michigan Journal of International Law, 2003, pages 697 et s. ;

dans la controverse (et rejetée tant par le Parlement européen que par la Commission européenne au cours des débats sur la réforme de la législation sur les télécommunications[37]). En 2008, la France introduisit un projet de loi qui aurait imposé aux fournisseurs d'accès à Internet de proscrire l'utilisation de leurs services aux utilisateurs qui auraient été considérés comme persistant dans leur entreprise de violation de droits d'auteur après des avertissements écrits répétés[38]. Cette approche aurait été critiquée par la Commission européenne[39].

4.2.4 L'approche basée sur les moteurs de recherche

Une quatrième approche, discutée dans le contexte du filtrage, consiste à imposer aux moteurs de recherche de ne pas répondre aux requêtes relatives à la pédopornographie (les considérations juridiques faisant l'objet d'une analyse séparée). Les prestataires de moteurs de recherche offrent des services de recherche qui permettent aux internautes d'identifier les documents qui les intéressent, en en spécifiant certains critères. Le moteur de recherche va chercher les documents pertinents qui correspondent aux critères fournis par l'utilisateur. Les moteurs de recherche jouent un rôle important dans le succès du développement d'Internet. Les contenus disponibles sur un site web mais qui ne sont pas indexés par un moteur de recherche ne peuvent faire l'objet d'un accès que si la personne qui souhaite les visiter en connait l'URL complète. M. Introna et Mme Nissenbaum considèrent que « *sans beaucoup d'exagération, il peut être dit qu'exister correspond à être indexé par un moteur de recherche* » [40].

L'obligation de ne pas traiter les requêtes relatives à la pédopornographie est en conséquence, à tout le moins s'agissant du résultat obtenu, comparable aux approches techniques.

Toutefois, si un site web proposant des contenus à caractère pédopornographique choisit de se cacher des moteurs de recherche, mais qu'il est connu par ceux qui recherchent ce type de contenus, l'information qu'il contient demeure facilement accessible.

« Development in the Law, The Law of Media » (« Evolution de la loi, la loi des médias »), Harvard Law Review, vol. 120, page 1041.

[37] Horten, « The Telecoms Package and "3 strikes" – voluntary cooperation to restrict downloads » (« Le Paquet Télécom et le système des 3 avertissements - coopération volontaire pour limiter le téléchargement »), 2008.

[38] Voir Ozimek, « France gets closer to "three strike" downloader web ban » (« la France est sur le point d'exclure du web les téléchargeurs ayant fait l'objet de trois notifications »), The Register, 12 juin 2008, disponible à l'adresse : http://www.theregister.co.uk/2008/06/12/france_music_law/.

[39] Voir « Loi antipiratage sur Internet: les observations de Bruxelles », La Tribune, 27 nov. 2008, disponible à l'adresse : http://www.latribune.fr/entreprises/communication/telecom-internet/20081127trib000314818/loi-antipiratage-sur-internet-les-observations-de-bruxelles-.html.

[40] Traduit de l'anglais. Introna et Nissenbaum, « Shaping the Web : Why the politics of search engines matters » (« Façonner le web : pourquoi la politique des moteurs de recherche compte »), page 5, disponible à l'adresse : http://www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

4.3 Qui choisit ce qu'il faut filtrer ?

Un deuxième critère pouvant être utilisé pour différencier les différentes approches du filtrage d'Internet est la qualité du décideur. Le décideur est la personne ou l'institution qui prend la décision relative à ce qui devrait être filtré.

4.3.1 Décision individuelle

Les individus peuvent choisir de se protéger, ou de protéger les personnes qu'ils ont à charge, contre certains types de contenus qu'ils sélectionnent eux-mêmes. Différents produits logiciels disponibles permettent aux utilisateurs de restreindre l'accès à certains sites web et services. Ces outils, souvent appelés « outils de contrôle parental », peuvent par exemple être utilisés pour restreindre les services disponibles sur les ordinateurs utilisés par des mineurs.

Le trait caractéristique des approches basées sur une « décision individuelle » est que la décision de mettre en œuvre le filtrage y est prise par l'utilisateur concerné lui-même, ou par son représentant. En partant du postulat selon lequel ce filtrage est volontaire par nature et qu'il ne fait l'objet d'aucune pression juridique extérieure, cette approche paraît offrir le système le plus ouvert, le plus responsable, le plus équilibré et le plus efficace. Bien entendu, il existe certaines inquiétudes quant à la compétence de l'utilisateur pour installer et configurer de tels systèmes logiciels.

Le problème que pose le filtrage géré par l'utilisateur est qu'il n'a pas d'effet sur les internautes qui recherchent délibérément des contenus illégaux. La présente étude identifie cette dernière caractéristique comme étant l'une des principales problématiques rencontrées dans tout système de filtrage d'Internet.

4.3.2 Décision institutionnelle

Parmi les approches destinées à protéger les mineurs, les approches basées sur des décisions institutionnelles sont largement mises en œuvre. Les établissements d'enseignement, par exemple, utilisent des technologies de filtrage pour s'assurer que les étudiants n'accèderont pas à certains services considérés comme préjudiciables.

De nombreuses bibliothèques publiques installent également de telles solutions afin de protéger leurs visiteurs contre tous les types de contenus illégaux ou préjudiciables. Aux Etats-Unis, les bibliothèques publiques doivent utiliser des technologies de filtrage pour obtenir des financements de la part du gouvernement américain.

Les cybercafés qui rendent souvent leurs services accessibles aux mineurs utilisent des technologies similaires. Même en dehors des considérations de protection de l'enfance, de telles technologies sont mises en œuvre.

Un autre exemple est le filtrage des sites web qui ne sont pas liés au travail, tels que les sites web populaires de jeux d'argent en ligne, par des entreprises souhaitant empêcher leurs employés d'y accéder[41].

Les solutions ne sont pas limitées aux technologies mises à disposition de l'utilisateur final. Les prestataires de services Internet eux-mêmes ont commencé à faire la promotion de solutions d'accès à Internet embarquant des restrictions par filtres[42].

---

[41] Voir par exemple, dans ce contexte, l'étude de l'entreprise Websense sur l'addiction au web des employés, 2008, disponible en anglais à l'adresse : http://files.shareholder.com/downloads/WBSN/0x0x156252/cdc85544-7f16-410b-90b8-7711faefbc36/WBSN_News_2002_8_21_General.pdf.

[42] Voir par exemple Nominum, COLT Case Study, « COLT Prevents Access to Illegal Web Sites » (Etude de cas concernant COLT, « COLT empêche l'accès aux sites web illégaux »), 2009, http://www.nominum.com/pdf/case-studies/Colt_CaseStudy_7_30_09.pdf (visité pour la dernière fois le 1er septembre 2009)

4.3.3 Législateur / Cours et tribunaux

Les récents débats portant sur le filtrage des sites web à caractère pédopornographique ne retiennent pas, pour la plupart, l'approche individuelle ou institutionnelle. Ils concluent plutôt à la nécessité d'imposer le filtrage, que celui-ci soit directement prévu par le législateur, ou qu'il résulte d'une décision de justice ou d'une autre autorité étatique compétente.

Toutefois, les compétences du législateur, des tribunaux et des autorités étatiques sont limitées par des contraintes constitutionnelles. Pour cette raison, d'abondantes discussions et un dynamisme politique ont soutenu l'idée d'un transfert de responsabilités entre l'Etat et des organisations généralement commerciales à but lucratif, qui ferait du filtrage une décision non plus étatique, mais institutionnelle. Un exemple en est l'accord de filtrage volontaire signé par plusieurs prestataires de services Internet allemands, qui fut proposé et promu par le gouvernement allemand. Dans la mesure où ce transfert de responsabilités va de pair avec un contournement des limitations posées par la Constitution, une telle approche génère de sérieuses inquiétudes pour la société.

Il est également nécessaire de s'interroger sur la réalité du caractère volontaire de ces activités de filtrage d'Internet, compte tenu du niveau de pression politique qui peut être observé dans certains pays, tels que le Royaume-Uni. Cette pression politique est inattendue et surprenante, puisque d'un point de vue juridique, un gouvernement ne peut imposer de telles initiatives autrement que par la loi, ce que nous expliquerons plus en détail au chapitre 7 de la présente étude. Il semble en effet extraordinaire que des entités commerciales puissent pratiquer le filtrage, quand la plupart des constitutions empêchent l'Etat lui-même d'imposer de telles mesures publiques. Lorsqu'une société a cru nécessaire, dans le passé, de mettre en place des mécanismes constitutionnels de nature à limiter les pouvoirs du gouvernement, il est étonnant que l'Etat permette à des acteurs privés de contourner ces mêmes limites, et qu'il les encourage parfois à le faire.

Il est fondamentalement nécessaire de se demander s'il est moralement et juridiquement acceptable que des prestataires d'accès à Internet puissent choisir de bloquer certains contenus, sans avoir à produire d'information sur les dommages et préjudices qu'entrainent leurs décisions. Ceci, en tenant compte des motivations commerciales pouvant potentiellement sous-tendre de tels choix.

Cette question se pose particulièrement pour les organisations à but lucratif qui se sont vues attribuer le statut juridique de « transporteurs » (qui implique une absence de responsabilité au regard des contenus illégaux qui circulent sur leurs réseaux lorsque cette illégalité n'est pas concrètement connue).

4.4 Que filtrer ?

Le filtrage d'Internet est considéré comme étant la solution technique à apporter à un éventail étendu d'activités illégales. Dans une large mesure – mais ce n'est pas toujours le cas – ces activités font l'objet d'incriminations pénales dans le pays qui entend mettre en œuvre ou qui a déjà mis en œuvre la technologie de filtrage. La pédopornographie relève de ces catégories de contenus qui, concernés par le filtrage, font l'objet de dispositions pénales. La présente section dresse un panorama des activités illégales les plus communes pour lesquelles se pose la question du filtrage.

4.4.1 Le spam

Phénomène

La lutte anti-spam est l'une des initiatives motivant le filtrage du trafic Internet les plus anciennement connues. La notion de « spam » renvoie à l'émission de messages non sollicités – parfois envoyés en masse, parfois de nature commerciale[43]. Bien que ces messages puissent véhiculer des tentatives variées d'escroqueries (« *scams* »), la plupart d'entre eux sont de simples messages électroniques, faisant souvent la publicité d'un produit ou d'un service, que leurs responsables envoient aux internautes par millions. En outre, le spam est souvent utilisé pour diffuser des logiciels malveillants. Depuis que le premier spam fut envoyé en 1978[44], le volume des spams a augmenté de manière dramatique[45]. Les organisations de prestataires de messagerie électronique signalent qu'au moins 85 à 90 pour cent de l'ensemble des messages électroniques envoyés sont actuellement des spams[46]. En 2007, les sources principales de spam étaient les Etats-Unis (19,6 pour cent du total enregistré), la République populaire de Chine (8,4 pour cent) et la République de Corée (6,5 pour cent)[47].

Considérations relatives au filtrage d'Internet

La plupart des prestataires de messagerie électronique ont répondu à la hausse du niveau de spam par l'installation de filtres anti-spam. Ces technologies identifient les spams en utilisant des filtres basés sur des mots-clefs ou des listes noires d'adresses IP de spammeurs[48]. Bien que les technologies de filtrage continuent à se développer, les spammeurs ont également développé des méthodes de contournement des systèmes techniques de protection – par exemple, en évitant d'utiliser certains mots-clefs. Les spammeurs ont trouvé de nombreuses

---

[43] Pour une définition plus précise, voir l'étude de l'UIT de 2005 sur les législations et les autorités anti-spam dans le monde (ITU Survey on Anti-Spam Legislation Worldwide 2005), page 5, disponible en anglais à l'adresse : http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[44] Tempelton, « Reaction to the DEC Spam of 1978 » (« Réaction au spam de (l'entreprise) DEC de 1978 »), disponible à l'adresse : http://www.templetons.com/brad/spamreact.html.

[45] S'agissant du développement du spam, voir Sunner, « Security Landscape Update 2007 » (« Mise à jour 2007 du paysage de sécurité »), page 3, disponible à l'adresse : http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[46] Le MAAWG (Messaging Anti-Abuse Working Group) rapporta en 2005 que plus de 85 pour cent de tous les messages électroniques étaient des spams. Voir son rapport, en langue anglaise, à l'adresse suivante : http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. Le prestataire Postini publia un rapport en 2007, lequel identifia plus de 75 pour cent de spams : voir http://www.postini.com/stats/. Le comparatif de filtres anti-spam « The Spam-Filter-Review » comptabilise quant-à-lui plus de 40 pour cent de spams : voir http://spam-filter-review.toptenreviews.com/spam-statistics.html. Voir également l'article « 2006: The year we were spammed a lot » (« 2006 : l'année où nous fûmes beaucoup spammés »), The Sydney Morning Herald, 16 décembre 2006, http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html.

[47] Rapport 2007 de Sophos sur les pays relais de spam, disponible en anglais à l'adresse : http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

[48] Pour plus d'informations sur les technologies utilisées pour identifier les spams, voir Hernan, Cutler et Harris, « Email Spamming Countermeasures: Detection and Prevention of Email Spamming » (« mesures défensives contre le spam par e-mail : détection et prévention du spam »), disponible à l'adresse : http://www.ciac.org/ciac/bulletins/i-005c.shtml ; Pour une présentation des différentes approches, voir le document de discussion du BIAC et de l'ICC sur le spam (BIAC ICC Discussion Paper on SPAM), 2004, disponible à l'adresse : http://www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf.

manières d'évoquer le « viagra », l'un des produits les plus populaires dont les spams font la promotion, sans en utiliser le nom de marque[49]. S'agissant du débat relatif au filtrage, il est très important de différencier entre les deux approches techniques permettant de filtrer les messages électroniques. Le filtrage peut être entrepris sur la base de l'analyse des données de trafic, ou sur la base de l'analyse du contenu des messages. La différence est importante car les lois nationales comme les instruments juridiques internationaux ne protègent pas de la même manière le contenu d'un message et les données de trafic. La plupart des mesures de filtrage du spam sont mises en œuvre avec le consentement entier du consommateur[50].

[49] Lui et Stamm, « Fighting Unicode-Obfuscated Spam » (« Lutter contre le spam en obscurcissant son texte grâce à l'unicode »), 2007, page 1, disponible à l'adresse : http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

[50] Le filtrage du spam basé sur l'adresse IP expéditrice est parfois mis en œuvre sans le consentement direct du consommateur. Le serveur expéditeur reçoit dans ce cas une notification de rejet.

4.4.2 Les ressources érotiques et pornographiques

Phénomène

Le filtrage des ressources présentant un caractère sexuel est souvent pris en considération par les décideurs politiques dans le contexte de la prévention de l'accès des mineurs aux contenus considérés comme préjudiciables. Ce filtrage peut être obtenu en installant des solutions logicielles[51] sur l'ordinateur du mineur, ou en utilisant les services d'accès à Internet d'un prestataire qui limite l'accessibilité de telles ressources.

Les contenus présentant un caractère sexuel ont compté parmi les premières ressources à être distribuées commercialement sur Internet. Ce réseau offre plusieurs avantages aux détaillants de contenus érotiques et pornographiques, dont :

- La possibilité d'échanger des ressources (telles que des images, des films, des reportages en direct) sans frais excessifs[52] ;
- Un accès mondial[53], permettant de toucher un nombre de consommateurs largement plus important que ne le pourraient des magasins de vente au détail ;
- Internet est souvent considéré comme étant un média anonyme (et souvent, de manière erronée[54]) – aspect que les consommateurs de pornographie apprécient, compte tenu de l'opinion sociale dominante. De récentes recherches ont identifié jusqu'à 4,2 millions de sites web pornographiques qui peuvent être disponibles sur Internet à toute heure[55]. A côté des sites web, les ressources pornographiques peuvent être distribuées :

---

[51] Il a été récemment signalé qu'en Chine, l'installation de logiciels de filtrage sur tous les ordinateurs personnels vendus sur le territoire est obligatoire. Voir Heise-News, « Bericht: Computer sollen in China nur noch mit Filtersoftware verkauft werden », 8 juin 2009, faisant référence à un rapport publié par le Wall Street Journal.

[52] Selon la disponibilité d'un accès haut-débit.

[53] L'accès est, dans certains pays, limité par des technologies de filtrage. S'agissant des obligations ou des approches du filtrage, voir Zittrain et Edelman, « Documentation of Internet Filtering Worldwide » (« Présentation de l'état du filtrage d'Internet à travers le monde »), disponible à l'adresse : http://cyber.law.harvard.edu/filtering/ ; Reidenberg, « States and Internet Enforcement » (« L'Etat et la régulation d'Internet »), University of Ottawa Law & Technology Journal, vol. 1, n° 213, 2004, pages 213 et s., disponible à l'adresse : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965 ; S'agissant de la discussion relative au filtrage dans différents pays, voir Taylor, « Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime » (« Les prestataires de services Internet et leur responsabilité au regard des contenus dans le nouveau régime français »), Computer Law & Security Report, vol. 20, fascicule (issue) 4, 2004, pages 268 et s. ; « Belgium ISP Ordered By The Court To Filter Illicit Content » (« Les prestataires d'accès à Internet contraints par une juridiction de filtrer les contenus illicites »), EDRI News, n° 5.14, 18 juin 2007, disponible à l'adresse : http://www.edri.org/edrigram/number5.14/belgium-isp ; Enser, « Illegal Downloads: Belgian court orders ISP to filter » (« Téléchargements illégaux : une juridiction Belge impose le filtrage aux FAI »), OLSWANG E-Commerce Update, nov. 2007, page 7, disponible à l'adresse : http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf ; Standford, « France to Require Internet Service Providers to Filter Infringing Music » (« La France demande aux fournisseurs d'accès à Internet de filtrer la musique contrefaite »), 27 nov. 2007, Intellectual Property Watch, disponible à l'adresse : http://www.ip-watch.org/weblog/index.php?p=842 ; Zwenne, « Dutch Telecoms wants to force Internet safety requirements » (« Le régulateur des télécommunications néerlandais veut imposer des règles de sécurité sur Internet »), Wold Data Protection Report, fascicule (issue) 09/07, page 17, disponible à l'adresse : http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf ; Le document de L'IFPI de 2007 concernant les options techniques permettant de lutter contre les violations du droit d'auteur en ligne (Technical options for addressing online copyright infringement), disponible en anglais à l'adresse : http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf ; S'agissant des approches d'autorégulation, voir « ISPA Code Review : Self-Regulation of Internet Service Providers » (« Examen du Code de l'association des prestataires de services Internet : auto-régulation des prestataires de services Internet »), 2002, disponible à l'adresse : http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

[54] S'agissant des traces électroniques qui sont laissées et des instruments permettant de suivre la trace des délinquants, voir infra, chapitre 5.

[55] Ropelato, « Internet Pornography Statistics » (« Statistiques relatives à la pornographie sur Internet »), disponible à l'adresse : http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

- en utilisant des systèmes de partage de fichiers[56] ;
- dans des salles de discussion privées.

Tous les pays n'appréhendent pas juridiquement l'érotisme et la pornographie de la même manière[57]. Certains d'entre eux permettent l'échange de ressources pornographiques entre adultes et limitent les incriminations aux situations dans lesquelles des mineurs ont accès à ces ressources[58], dans un but de protection de l'enfance[59]. Des recherches indiquent que l'accès des enfants à des ressources pornographiques pourrait influencer de manière négative le développement et le bien-être émotionnels de ces derniers[60]. Afin de permettre le respect de ces lois, des « systèmes de vérification de l'âge adulte » (« *adult verification systems* ») ont été développés[61]. D'autres pays font tomber sous le coup de la loi pénale tout échange de pornographie, même entre adultes[62], sans se concentrer sur des groupes particuliers de personnes.

Considérations relatives au filtrage d'Internet

Dans les pays qui incriminent l'accès à des ressources à caractère pornographique, empêcher l'accès à de telles ressources est un vrai défi. Hors ligne, les autorités peuvent se reposer sur les structures existantes pour détecter et poursuivre les violations de l'interdiction qu'elles ont posée. Sur Internet, toutefois, l'application de la loi est difficile, puisque les ressources à caractère pornographique qui y sont présentes sont souvent mises à disposition légalement, sur des serveurs hébergés hors du pays. Même lorsque les autorités sont capables d'identifier des sites web à caractère pornographique, elles peuvent n'avoir aucun pouvoir d'exiger le retrait de ces ressources auprès des prestataires qui les hébergent[63]. Ce défi est une conséquence directe de l'hétérogénéité des différentes normes nationales qui réglementent la mise en ligne de ce type de contenus.

La tentative de filtrage visant un contenu qui est légalement mis à disposition hors du pays, mais qui est considéré comme illégal à l'intérieur de ce même pays, pourrait être vue comme une option permettant à ce dernier d'œuvrer au maintien de ses propres standards culturels, dans une situation d'accès global.

---

[56] Environ le tiers des fichiers téléchargés à l'aide de systèmes de partage de fichiers contiennent de la pornographie. Ropelato, « Internet Pornography Statistics » (« Statistiques relatives à la pornographie sur Internet »), disponible à l'adresse : http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

[57] Voir Gercke, Comprendre la cybercriminalité : Guide pour les pays en développement (Understanding Cybercrime: A Guide for Developing Countries), ITU, 2009, pages 132 et s., disponible en français à partir de l'adresse : http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[58] Un exemple de cette approche peut être trouvé à la section 184 du Code pénal allemand (Strafgesetzbuch) : Section 184 - Diffusion d'écrits pornographiques : « *(1) Toute personne qui, s'agissant d'écrits pornographiques (Section 11, sous-section (3)): 1. les offre, les donne ou les rend accessibles à une personne âgée de moins de dix-huit ans ; […]* » (traduit de l'anglais).

[59] S'agissant de cet aspect, voir le Programme mondial cybersécurité de l'UIT / Groupe d'experts de haut niveau, Rapport stratégique mondial (Global Strategic Report), 2008, page 36, disponible en anglais à l'adresse suivante : http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[60] Voir Nowara et Pierschke, *Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter*, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerderten Modellprojekten, 2008.

[61] Voir Siebert, « Protecting Minors on the Internet: An Example from Germany » (« Protéger les mineurs sur Internet : un exemple provenant d'Allemagne »), in *Governing the Internet Freedom and Regulation in the OSCE Region*, page 150, disponible à l'adresse : http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[62] Un exemple est le projet de loi égyptien de 2006 intitulé « Réglementer la protection des données et de l'information électroniques et combattre les crimes d'information » (« Regulating the protection of Electronic Data and Information and Combating Crimes of Information ») : Sec. 37 : « *Le fait pour toute personne de fabriquer, d'imiter, d'obtenir ou de posséder, dans le but de leur distribution, de leur publication ou de leur commerce, des images ou des dessins publiquement immoraux traités par un procédé électronique, est puni d'un emprisonnement ne pouvant être inférieur à six mois, et d'une amende ne pouvant être inférieure à cinq cent mille livres égyptiennes, sans pouvoir excéder sept cent mille livres égyptiennes, ou de l'une de ces deux peines* » (traduit de l'anglais).

[63] Voir également, dans ce contexte, le chapitre 6 de la présente étude.

4.4.3 La pédopornographie

Phénomène

Contrairement à la pornographie, qui fait l'objet de différents points de vue, la pédopornographie est universellement condamnée et est largement reconnue comme étant une infraction pénale[64]. Diverses organisations internationales sont engagées dans la lutte contre la pédopornographie en ligne[65] et plusieurs instruments juridiques internationaux ont vu le jour, dont la Convention des Nations Unies relative aux droits de l'enfant de 1989[66], La décision-cadre du Conseil de l'Union européenne relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie de 2003[67], et la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels de 2007[68].

Malgré les efforts et les coûts considérables qu'elles ont impliqués, ces initiatives, visant à contrôler la distribution en réseau de contenus à caractère pédopornographique, ont démontré n'avoir eu que peu d'effet dissuasif sur les auteurs d'infractions, qui utilisent Internet pour communiquer et s'échanger des ressources de cette nature. Des recherches américaines relatives au comportement des délinquants en matière de pédopornographie montrent que 15 pour cent des personnes arrêtées alors qu'elles étaient en possession de contenus à caractère pédopornographique provenant d'Internet détenaient plus de 1000 images sur leur ordinateur ; que 80 pour cent d'entre elles possédaient sur leur ordinateur des images d'enfants entre 6 et 12 ans[69] ; que 19 pour cent d'entre elles détenaient des images d'enfants d'un âge inférieur à 3 ans[70] ; et que 21 pour cent d'entre elles étaient en possession d'images dépeignant la violence[71].

Les motivations des personnes qui exploitent des sites web à caractère pédopornographique sont significativement différentes, selon que cette exploitation a lieu à titre commercial ou à titre non commercial. La vente de pédopornographie peut être extrêmement profitable[72], des collectionneurs étant prêts à payer des sommes significatives pour obtenir des vidéos et des

---

[64] Gercke, *Comprendre la cybercriminalité : Guide pour les pays en développement*, ITU, 2009, page 134 et s ; Programme mondial cybersécurité de l'UIT / Groupe d'experts de haut niveau, Rapport stratégique mondial (Global Strategic Report), 2008, page 34, disponible en anglais à l'adresse suivante : http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[65] Voir par exemple le « Communiqué du G8 », Sommet de Gênes, 2001, disponible à l'adresse : http://g8.gc.ca/fr/a-propos-du-g8/sommets-passes/sommet-de-genes-2001/communique/.

[66] Convention des Nations Unies relative aux droits de l'enfant, A/RES/44/25, disponible à l'adresse : http://www2.ohchr.org/french/law/crc.htm. S'agissant de l'importance d'une législation sur la cybercriminalité, voir le Programme mondial cybersécurité de l'UIT / Groupe d'experts de haut niveau, Rapport stratégique mondial (Global Strategic Report), 2008, page 35, disponible en anglais à l'adresse suivante: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[67] Décision-cadre du Conseil relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie, 2004/68/JAI, disponible à l'adresse : http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2004/l_013/l_01320040120fr00440048.pdf.

[68] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, STCE n° 201, disponible à l'adresse suivante : http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=2/28/2008&CL=FRE.

[69] Voir Wolak, Finkelhor et Mitchell, « Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study » (« Des possesseurs de pédopornographie arrêtés pour des infractions en relation avec Internet : conclusions de l'étude nationale sur la victimisation des enfants en ligne »), 2005, page 5, disponible à l'adresse : http://www.missingkids.com/en_US/publications/NC144.pdf.

[70] Voir Wolak, Finkelhor et Mitchell, « Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study » (« Des possesseurs de pédopornographie arrêtés pour des infractions en relation avec Internet : conclusions de l'étude nationale sur la victimisation des enfants en ligne »), 2005, page 5, disponible à l'adresse : http://www.missingkids.com/en_US/publications/NC144.pdf.

[71] Pour de plus amples informations, voir *Child Pornography: Model Legislation & Global Review (Pédopornographie : législation modèle et bilan mondial)*, 2006, page 2, disponible à l'adresse : http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[72] Voir Walden, Computer Crimes and Digital Investigations (Infractions informatiques et investigations numériques), page 66.

images représentant des enfants dans un contexte de nature sexuelle[73]. Il y a quelques années, les moteurs de recherche pouvaient trouver ce type de ressources très rapidement[74]. Les contenus sont souvent échangés dans des forums privés protégés par mot de passe, auxquels les autres internautes et les services en charge de l'application de la loi peuvent rarement accéder. Cette situation pose des problèmes majeurs dans le cadre des investigations et des opérations contrôlées sous couverture, lesquelles se révèlent parfois vitales dans le contexte de la lutte contre la pédopornographie en ligne[75].

Considérations relatives au filtrage d'Internet

En raison de l'hétérogénéité significative qui existe entre les différentes réglementations et procédures d'enquête nationales relatives à la publication de pédopornographie, cette question a été l'une des premières à soulever d'intenses discussions sur le filtrage, considéré comme une solution pouvant lui être apportée.

Aujourd'hui, le débat relatif au filtrage des contenus illégaux se concentre plus particulièrement sur la question de la protection de l'enfance[76].

[73] Il est possible de faire des profits importants en une période de temps assez courte en proposant de la pédopornographie – c'est l'un des moyens utilisés par les cellules terroristes pour financer leurs activités sans dépendre de donations.

[74] « Police authorities and search engines forms alliance to beat child pornography » (« Les autorités de police et les moteurs de recherche s'allient pour combattre la pédopornographie »), disponible à l'adresse : http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/ ; « Google accused of profiting from child porn » (« Google accusé de tirer profit de la pédopornographie »), disponible à l'adresse : http://www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

[75] Voir ABA, International Guide to Combating Cybercrime (Guide international pour combattre la cybercriminalité), page 73.

[76] A propos de ce débat, voir Gercke, « Obligations of Internet Service Provider in the Fight Against Child Pornography » (« Les obligations des fournisseurs de services Internet dans le cadre de la lutte contre la pédopornographie »), Computer Law Review International, 2009, page 65.

4.4.4 Les sujets politiques controversés / les discours de haine / la xénophobie

Phénomène

La discussion relative au filtrage n'est pas limitée aux contenus qui sont largement reconnus comme constituant par nature des infractions. De fait, le débat qui n'évoque que la question de la pédopornographie est potentiellement trompeur. La question du filtrage est également discutée au regard de contenus dont le caractère délictueux ou criminel est moins évident, ou qui sont moins largement considérés comme illégaux. Un exemple est le débat relatif au filtrage de sujets politiques controversés. Certains pays comme l'Allemagne et l'Autriche répriment pénalement la publication de haine raciale, de violence et de xénophobie, tandis que de tels contenus peuvent être légalement publiés dans d'autres pays qui garantissent une forte protection de la liberté d'expression, comme les Etats-Unis. D'autres pays ont été signalés comme allant même au delà, en ce qu'ils tentent de filtrer les commentaires critiques relatifs à des sujets politiques[77].

Le blocage de sites web exploités par des organisations (politiques) radicales compte parmi les aspects les plus controversés du filtrage, car il s'avère difficile de distinguer (tout du moins dans quelques pays légitimes) entre la pénalisation des contenus politiquement inacceptables et la censure des opinions politiques. Les groupes radicaux utilisent les systèmes de communication de masse comme Internet pour propager leur propagande[78]. Récemment, le nombre de sites web proposant des contenus à caractère raciste ou des discours haineux a augmenté[79] – une étude de 2005 évoquait une augmentation de 25 pour cent du nombre des pages web faisant la promotion de la haine raciale, de la violence et de la xénophobie, entre 2004 et 2005[80]. En 2006, plus de 6 000 sites web de cette nature existaient sur Internet[81].

La distribution sur Internet offre divers avantages à ceux qui souhaitent publier ce type de contenus, dont des coûts de distribution moins élevés, une absence de nécessité d'avoir recours à un équipement de spécialiste et une audience mondiale. Parmi les sites web incitant à la haine se trouvent par exemple ceux qui proposent des instructions sur la manière de fabriquer des bombes[82]. A côté de la propagande, Internet est utilisé pour vendre certains objets, relatifs par exemple au nazisme, ces derniers pouvant prendre la forme de drapeaux flanqués de symboles, d'uniformes ou de livres, et étant aisément disponibles sur des plateformes de vente aux enchères et magasins web spécialisés[83]. Internet est encore utilisé pour envoyer des messages électroniques et des lettres d'information, ainsi que pour distribuer des vidéo-clips et des manifestations télévisées par l'intermédiaire d'archives populaires telles que YouTube.

Tous les pays n'incriminent pas ces agissements[84]. Dans certains pays, ces derniers peuvent être protégés par le principe de liberté d'expression[85]. Les opinions divergent sur la question

---

[77] Heise-News, « Skype in China filtert und speichert politische Mitteilungen », 2 oct. 2008.

[78] Les groupes radicaux américains reconnaissent les avantages d'Internet pour développer leur audience initiale. Voir Markoff, « Some computer conversation is changing human contact » (« Un peu de conversation informatique modifie les rapports humains »), NY-Times, 13 mai 1990.

[79] Sieber, « Organised crime situation report 2004 » (« Rapport 2004 sur la situation en matière crime organisé »), Rapport du Conseil de l'Europe, page 138.

[80] Akdeniz, « Governance of Hate Speech on the Internet in Europe » (« La gouvernance des discours de haine sur Internet en Europe »), in *Governing the Internet Freedom and Regulation in the OSCE Region*, page 91, disponible à l'adresse : http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[81] Voir *Digital Terrorism & Hate 2006 (Terrorisme et haine numériques en 2006)*, disponible à l'adresse : http://www.wiesenthal.com.

[82] Whine, *Online Propaganda and the Commission of Hate Crime (La propagande en ligne et la commission de crimes de haine)*, disponible à l'adresse : http://www.osce.org/documents/cio/2004/06/3162_en.pdf.

[83] Voir ABA, International Guide to Combating Cybercrime (Guide international pour combattre la cybercriminalité), page 53.

[84] S'agissant de l'incrimination de ces actes aux Etats-Unis, voir Tsesis, « Prohibiting Incitement on the Internet » (« Interdire l'incitation sur Internet »), Virginia Journal of Law and Technology, Vol. 7, 2002, disponible à l'adresse : http://www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.

[85] S'agissant du principe de la liberté d'expression, voir Tedford, Herbeck et Haiman, Freedom of Speech in the United States (Liberté d'expression aux Etats-Unis), 2005 ; Barendt, Freedom of Speech (Liberté

de savoir jusqu'où le principe de liberté d'expression doit s'appliquer s'agissant de certains sujets, en ce qu'il fait parfois obstacle aux investigations internationales. Un exemple de conflit de lois peut se retrouver dans l'affaire qui a impliqué le prestataire de services Yahoo! en 2001, lequel s'est vu ordonner par une juridiction française (alors qu'il était basé aux Etats-Unis) d'empêcher l'accès des utilisateurs français à des contenus nazis[86]. La vente de tels objets est légale aux Etats-Unis, sur le fondement du premier amendement de la Constitution de ce pays. Suivant ce premier amendement, une Cour américaine décida que l'ordre juridique français n'était pas applicable à Yahoo! sur le sol des Etats-Unis[87].

Les disparités qui existent entre les pays, sur la question, furent évidentes dans le cadre de la rédaction de la Convention sur la cybercriminalité du Conseil de l'Europe. La Convention a pour objectif d'harmoniser les législations relatives à la cybercriminalité, afin d'assurer que les investigations internationales ne soient pas entravées par des conflits de lois[88]. Les parties engagées dans les négociations ne furent pas en mesure de se mettre d'accord sur l'incrimination de la diffusion de ressources xénophobes. En conséquence, ce sujet fut exclu dans son ensemble de la Convention, pour être traité dans un premier protocole séparé[89]. Si cela n'avait pas été le cas, certains pays (incluant les Etats-Unis) n'auraient pas été en mesure de signer la Convention.

Considérations relatives au filtrage d'Internet

En Europe, le contexte de ce débat est né avec la Directive de l'Union européenne de 2000 sur le commerce électronique[90]. Face aux défis posés par la dimension internationale d'Internet, les rédacteurs de la Directive décidèrent de développer des standards, qui permettraient de fournir un cadre juridique au développement global de la société de l'information, et par là-même de soutenir tant un développement économique général que le

---

d'expression), 2007 ; Baker, Human Liberty and Freedom of Speech (La liberté humaine et la liberté d'expression) ; Emord, Freedom, Technology and the First Amendment (Liberté, technologie et le Premier amendement), 1991 ; S'agissant de l'importance du principe dans le contexte de la surveillance électronique, voir Woo et So, « The case for Magic Lantern : September 11 Highlights the need for increasing surveillance » (« L'affaire de la lanterne magique : le 11 septembre met à jour le besoin d'accroitre la surveillance »), Harvard Journal of Law & Technology, vol. 15, n° 2, 2002, pages 530 et s. ; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, (La liberté d'expression en droit australien ; une plante délicate), 2000 ; Volokh, « Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law » (« Liberté d'expression, loi sur le harcèlement religieux et loi sur l'aménagement religieux »), Loyola University Chicago Law Journal, vol. 33, 2001, pages 57 et s., disponible à l'adresse : http://www.law.ucla.edu/volokh/harass/religion.pdf ; Cohen, « Freedom of Speech and Press: Exceptions to the First Amendment » (« La liberté d'expression et de la presse : exceptions au Premier amendement »), CRS Report for Congress 95-815, 2007, disponible à l'adresse : http://www.fas.org/sgp/crs/misc/95-815.pdf.

[86] Voir Greenberg, « A Return to Lilliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market » (« Un retour sur Lilliput : l'affaire Licra c/ Yahoo! et la réglementation des contenus en ligne dans le marché mondial »), Berkeley Technology Law Journal, vol. 18, pages 1191 et s ; Van Houweling, « Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra » (« Application des jugements étrangers, le Premier amendement et l'expression sur Internet : note pour la prochaine affaire Yahoo! c/ Licra »), Michigan Journal of International Law, 2003, pages 697 et s. ; « Development in the Law, The Law of Media » (« Evolution de la loi, la loi des médias »), Harvard Law Review, vol 120, page 1041.

[87] Voir l'affaire « Yahoo Inc. v. La Ligue Contre Le Racisme et l'Antisémitisme », 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001), disponible à l'adresse : http://www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=213138298941949941944938934938937961519199 1.

[88] Gercke, « The Slow Wake of a Global Approach against Cybercrime » (« Le lent réveil d'une approche mondiale contre la cybercriminalité »), Computer Law Review International, 2006, 144.

[89] Voir le « Rapport explicatif » du Protocole additionnel à la Convention sur la cybercriminalité, § n° 4, disponible à l'adresse suivante : http://conventions.coe.int/Treaty/FR/Reports/Html/189.htm.

[90] Directive 2000/31/CE du Parlement européen et du Conseil du 8 Juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché interieur (« Directive sur le commerce électronique »), Journal officiel L 178 du 17 juillet 2000, p. 0001 – 0016. Pour une analyse comparée des droits américain et européen relatifs à la réglementation du commerce électronique (incluant la Directive de l'Union européenne sur le commerce électronique), voir Pappas, « Comparative U.S. & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation » (« Comparaison des approches américaine et européenne de la régulation du commerce électronique : juridiction, contrats électroniques, signature électronique et taxation »), Denver Journal of International Law and Policy, vol. 31, 2003, pages 325 et s., disponible à l'adresse : http://www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

travail des services chargés de l'application de la loi[91]. La réglementation relative à la responsabilité est basée sur le principe d'une responsabilité graduée.

Des dispositions de la Directive limitent la responsabilité de certains prestataires de services[92]. Selon l'article 12 de la Directive, la responsabilité des prestataires d'accès et des opérateurs de réseaux est complètement exclue, dès lors que ces derniers respectent les trois conditions posées par le texte. Le paragraphe 3 de l'article souligne toutefois que cette limitation de responsabilité « *n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation* ». Cette clause fut par exemple utilisée par les autorités allemandes pour ordonner à des prestataires d'accès à Internet d'empêcher l'accès à des sites web contenant des ressources xénophobes[93].

[91] Voir Lindholm/Maennel, *Computer Law Review International* (*Revue internationale du droit de l'informatique*), 2000, 65.
[92] Articles 12 à 15 de la Directive de l'Union européenne sur le commerce électronique.
[93] Voir à ce sujet Mankowski, *Multimedia und Recht*, 2002, pages 277 et s. ; Stadler, *Multimedia und Recht*, 2002, pages 343 et s.

4.4.5 Les jeux d'argent en ligne illégaux

Phénomène

Bien qu'affectés par la crise financière globale, les jeux d'argent en ligne constituent toujours un marché émergent ; les jeux et les jeux d'argent représentent l'un des domaines d'Internet qui se développent le plus vite[94]. Linden Labs, le développeur du jeu en ligne Second Life[95], rapporte avoir enregistré environ dix millions de comptes utilisateurs[96]. Des rapports montrent que certains de ces jeux ont été utilisés pour commettre des infractions, incluant[97] :

- L'échange et l'exposition de pédopornographie[98] ;
- La fraude[99] ;
- Les jeux d'argent dans les casinos en ligne[100] ; et
- La diffamation (par exemple, en laissant des messages diffamatoires).

Certaines estimations projettent une croissance des revenus provenant des jeux d'argent en ligne de 3,1 milliards de dollars en 2001 à 24 milliards de dollars en 2010[101] (quoi que ces estimations restent relativement faibles, comparées aux revenus provenant des jeux d'argent traditionnels[102]).

La réglementation des jeux d'argent, sur Internet ou hors ligne, varie selon les pays[103]- point faible qui a été exploité par les délinquants comme par les entreprises respectant la loi et les casinos. L'effet que produit l'existence de différentes réglementations est évident à Macao. Après avoir été rendue à la Chine par le Portugal en 1999, Macao est devenue l'une des plus

---

[94] Concernant l'ampleur grandissante du jeu d'argent en ligne, voir Landes, « Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation » (« Escales et cargos : l'interdiction des jeux d'argent en ligne, proposition d'un système de régulation »), disponible à l'adresse : http://www1.law.nyu.edu/journals/lawreview/issues/vol82/no3/NYU306.pdf ; Brown et Raysman, « Property Rights in Cyberspace Games and other novel legal issues in virtual property » (« Les droits de propriété dans le cadre des cyber jeux et autres questions de propriété immatérielle liées à certains jeux virtuels »), The Indian Journal of Law and Technology, vol. 2, 2006, pages 87 et s., disponible à l'adresse : http://www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

[95] http://www.secondlife.com.

[96] Nombre des comptes publié par Linden Lab. Voir : http://www.secondlife.com/whatis/. S'agissant de Second Life en général, voir Harkin, « Get a (second) life » (« Ayez une (seconde) vie »), Financial Times, disponible à l'adresse : http://www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

[97] Heise News, 15 nov. 2006, disponible à l'adresse : http://www.heise.de/newsticker/meldung/81088 ; DIE ZEIT, 4 janv. 2007, page 19.

[98] BBC News, 9 mai 2007, « Second Life 'child abuse' claim » (« Second Life accusé "d'abus sur enfants" »), disponible à l'adresse : http://news.bbc.co.uk/1/hi/technology/6638331.stm.

[99] Leapman, « Second Life world may be haven for terrorists » (« Le monde de Second Life pourrait être un paradis pour les terroristes »), Sunday Telegraph, 14 mai 2007, disponible à l'adresse : http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml ; Reuters, « UK panel urges real-life treatment for virtual cash » (« Un groupe d'experts du Royaume-Uni exhorte à traiter l'argent virtuel de la même manière que dans la vie réelle »), 14 mai 2007, disponible à l'adresse : http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

[100] See Olson, « Betting No End to Internet Gambling » (« Pari contre la fin des jeux d'argent en ligne »), Journal of Technology Law and Policy, vol. 4, fascicule (issue) 1, 1999, disponible à l'adresse : http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[101] Christiansen Capital Advisor. Voir http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

[102] Les revenus des casinos américains en 2005 (hors jeux d'argent en ligne) dépassaient 84 milliards de dollars, voir Landes, « Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation » (« Escales et cargos : l'interdiction des jeux d'argent en ligne, proposition d'un système de régulation ») , page 915, disponible à l'adresse : http://www1.law.nyu.edu/journals/lawreview/issues/vol82/no3/NYU306.pdf.

[103] Voir, par exemple, GAO, « Internet Gambling - An Overview of the Issues » (« Jeux d'argent en ligne – un panorama des problématiques »), disponible à l'adresse : http://www.gao.gov/new.items/d0389.pdf ; S'agissant des procédures de l'OMC, voir « Etats-Unis - Mesures visant la fourniture transfrontalière de services de jeux et paris », disponible à l'adresse : http://www.wto.org/french/tratop_f/dispu_f/cases_f/ds285_f.htm ; Le Groupe de l'article 21:5 conclut que les Etats-Unis ne s'étaient pas conformés aux recommandations et décisions de l'ORD [Organe de règlement des différends, *ndlt*].

grandes destinations au monde pour pratiquer les jeux d'argent. Avec des revenus annuels estimés à 6,8 milliards de dollars en 2006, elle détrône Las Vegas (6,6 milliards de dollars[104]). Le succès de Macao vient du fait que les jeux d'argent sont interdits en Chine[105], des milliers de joueurs s'y rendant depuis le reste du territoire chinois pour y jouer.

Internet permet aux personnes de contourner les restrictions liées aux jeux d'argent[106]. Les casinos en ligne y sont largement accessibles, la plupart d'entre eux étant hébergés dans des pays dont la réglementation concernant les jeux d'argent sur Internet est libérale, voire inexistante. Les utilisateurs peuvent y ouvrir des comptes en ligne, y transférer de l'argent et y jouer à des jeux de hasard[107]. Les casinos en ligne peuvent également être utilisés pour blanchir de l'argent ou financer le terrorisme[108]. Si les délinquants utilisent des casinos dans lesquels la phase de mise en jeu (lorsque les paris sont mis sur la table) ne fait pas l'objet d'une conservation de données, ou si les casinos eux-mêmes sont localisés dans un pays qui ne possède pas de législation sur le blanchiment d'argent, il est difficile, pour les services en charge de l'application de la loi, de déterminer l'origine des fonds utilisés.

Considérations relatives au filtrage d'Internet

Les pays restreignant la pratique des jeux en ligne ont des difficultés à contrôler l'utilisation des casinos en ligne ou les activités de ces derniers. Internet affaiblit l'effectivité des restrictions juridiques posées par certains pays concernant l'accès de leurs citoyens aux jeux d'argent en ligne[109]. Plusieurs initiatives législatives ont tenté de prévenir la participation à ces jeux[110] : notamment, la loi américaine de 2006 prohibant les jeux d'argent sur Internet (« *Internet Gambling Prohibition Enforcement Act* ») cherche à limiter les jeux d'argent illégaux en ligne, en organisant la poursuite des prestataires de services financiers qui procèdent au règlement de transactions associées à des jeux d'argent illégaux[111]. Le filtrage technique de l'accès à de tels sites web est parfois discuté comme pouvant être un instrument de lutte complémentaire[112].

---

[104] Pour de plus amples informations, voir BBC News, « Tiny Macau overtakes Las Vegas », à l'adresse : http://news.bbc.co.uk/2/hi/business/6083624.stm.

[105] Voir l'article 303 du Code pénal chinois : « Le fait, pour toute personne, dans le but d'en tirer profit, de réunir des personnes pour s'engager dans les jeux d'argent, d'exploiter une maison de jeux d'argent, ou de faire du jeu d'argent sa profession, est puni d'une peine maximale de trois ans d'emprisonnement à terme fixe, d'une détention pénale ou d'une mise sous surveillance, en plus d'une amende ». [Traduit de l'anglais. Selon le droit pénal chinois, la détention pénale ne peut être inférieure à un mois et ne peut être supérieure à six mois ; la mise sous surveillance, assurée par un organe public, ne peut être inférieure à trois mois et ne peut être supérieure à deux ans : articles 38 à 44 du Code pénal chinois – *ndlt*].

[106] Parallèlement aux jeux d'argent qui sévissent à Macao, les chinois ont commencé à fréquenter les jeux d'argent en ligne de manière intensive. Voir « Online Gambling challenges China's gambling ban » (« Les jeux d'argent en ligne lancent un défi à l'embargo chinois sur les jeux d'argent »), disponible à l'adresse : http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[107] Pour de plus amples informations, voir : http://en.wikipedia.org/wiki/Internet_casino.

[108] Voir le rapport du GAFI [Groupe d'action financière sur le blanchiment de capitaux, *ndlt*] sur les typologies du blanchiment de capitaux 2000 – 2001, page 3, disponible en anglais à l'adresse suivante : http://www.fatf-gafi.org/dataoecd/32/11/35396679.pdf ; Coates, « Online casinos used to launder cash » (« Les casinos en ligne utilisés pour blanchir de l'argent »), disponible à l'adresse : http://www.timesonline.co.uk/tol/news/politics/article620834.ece?print=yes&randnum=1187529372681.

[109] Voir, par exemple, « Online Gambling challenges China's gambling ban » (« Les jeux d'argent en ligne lancent un défi à l'embargo chinois sur les jeux d'argent »), disponible à l'adresse : http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[110] Pour une vue d'ensemble de la législation antérieure des Etats-Unis, voir Olson, « Betting No End to Internet Gambling » (« Pari contre la fin des jeux d'argent en ligne »), Journal of Technology Law and Policy, vol. 4, fascicule (issue) 1, 1999, disponible à l'adresse : http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[111] Voir le § 5367 de l'Internet Gambling Prohibition Enforcement Act.

[112] L'Italie a introduit l'obligation de filtrer les sites web de jeux en ligne, illégaux ou sans licence. S'agissant de la réponse de l'industrie, voir par exemple COLT Case Study, « COLT Prevents Access to Illegal Web Sites » (Etude de cas concernant COLT, « COLT empêche l'accès aux sites web illégaux »), 2009, disponible à l'adresse : http://www.nominum.com/pdf/case-studies/Colt_CaseStudy_2_19_09.pdf ; Concernant la législation sur les jeux en Italie, voir Sbordoni, Celesti et Dionisi, « Sanctions for Infringements of Gambling Laws in Italy » (« Les sanctions pour violation de la loi sur les jeux d'argent en Italie »), ERA Forum 2007, 413.

4.4.6 La diffamation et la publication de fausses informations

Phénomène

Internet peut aisément être utilisé pour diffuser des renseignements erronés[113]. Les sites web peuvent afficher des informations fausses ou diffamatoires, particulièrement dans les forums et les salles de discussion, lorsque les messages qui y sont postés par les utilisateurs ne sont pas vérifiés par un modérateur[114]. Les mineurs utilisent de manière croissante les forums sur le web et les réseaux sociaux, où de telles informations peuvent également être postées[115]. Les infractions[116] concernées peuvent inclure (par exemple) la publication de photographies intimes, ou la publication de fausses informations relatives à un comportement sexuel[117].

Dans la plupart des cas, les auteurs de ces infractions profitent du fait que les prestataires proposant un service de publication gratuit ou peu onéreux ne requièrent pas l'identification des auteurs ou ne vérifient pas l'identité de ces derniers[118]. Ceci rend l'identification des délinquants compliquée. En outre, les contenus postés sur les forums peuvent être peu, voire non régulés par des modérateurs. Ces avantages n'ont pas empêché le développement de projets de valeur, tels que l'encyclopédie en ligne Wikipedia[119], générée par les utilisateurs, où les contenus sont régulés sur la base de procédures strictes. Toutefois, la même technologie peut également être utilisée par les délinquants pour :

- Publier des fausses informations (par exemple à propos d'un concurrent) [120] ;
- Diffamer (par exemple en laissant des messages diffamatoires)[121] ;

---

[113] Voir Reder et O'Brien, « Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking The Identity Of Anonymous Employee Internet Posters » (« Cyberdiffamation d'une entreprise : les employeurs portent plainte contre X pour diffamation, cherchant à connaître l'identité de l'employé anonyme responsable d'un post »), Mich. Telecomm. Tech. L. Rev. 195, 2002, page 196, disponible à l'adresse : http://www.mttlr.org/voleight/Reder.pdf.

[114] Concernant cette situation dans les blogs, voir Reynolds, « Libel in the Blogosphere: Some Preliminary Thoughts » (« Diffamation dans la blogosphère : quelques réflexions préliminaires ») Washington University Law Review, 2006, pages 1157 et s., disponible à l'adresse : http://ssrn.com/abstract=898013 ; Solove, « A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere » (« L'histoire de deux blogueurs : libre expression et vie privée dans la blogosphère »), Washington University Law Review, vol. 84, 2006, pages 1195 et s., disponible à l'adresse : http://ssrn.com/abstract=901120 ; Malloy, « Anonymous Bloggers And Defamation: Balancing Interests On The Internet » (« Blogueurs anonymes et diffamation : équilibrer les intérêts sur Internet »), Washington University Law Review, vol. 84, 2006, pages 1187 et s., disponible à l'adresse : http://law.wustl.edu/WULR/84-5/malloy.pdf.

[115] S'agissant des problématiques de vie privée posées par ces réseaux sociaux, voir Hansen et Meissner (éditeurs), *Linking digital identities (Lier les identités numériques)*, page 8 – Une synthèse du rapport est disponible en anglais pages 8 et 9. Le rapport est disponible en allemand à l'adresse suivante : https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf [titre original : Verkettung digitaler Identitäten, *ndlt*].

[116] Concernant la controverse relative à la pénalisation de la diffamation, voir « Freedom of Expression, Free Media and Information, Statement of Mr. McNamara » (« Liberté d'expression, médias et information libres, déclaration de M. McNamara »), US Delegation to the OSCE, October 2003, disponible à l'adresse : http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf ; Lisby, « No Place in the Law: Criminal Libel in American Jurisprudence » (« Aucune place dans la loi pour : la diffamation punissable dans la jurisprudence américaine »), 2004, disponible à l'adresse : http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf ; S'agissant de l'évolution de l'infraction, voir Walker, « Reforming the Crime of Libel » (« La réforme de l'infraction de diffamation »), New York Law School Law Review, vol. 50, 2005/2006, page 169, disponible à l'adresse : http://www.nyls.edu/pdfs/NLRVol50-106.pdf ; Kirtley, « Criminal Defamation: An "Instrument of Destruction" » (« La diffamation punissable : un "instrument de destruction" »), 2003, disponible à l'adresse : http://www.silha.umn.edu/oscepapercriminaldefamation.pdf ; « Defining Defamation, Principles on Freedom of Expression and Protection of Reputation » (« Définir la diffamation, les principes de liberté d'expression et de protection de la réputation »), 2000, disponible à l'adresse : http://www.article19.org/pdfs/standards/definingdefamation.pdf.

[117] Voir Sieber, « Organised crime situation report 2004 » (« Rapport 2004 sur la situation en matière crime organisé »), Rapport du Conseil de l'Europe, page 105.

[118] S'agissant de la difficulté qu'il y a à enquêter sur des infractions liées à des services anonymes, voir infra, chapitre 5.

[119] Voir : http://www.wikipedia.org.

[120] Voir Sieber, « Organised crime situation report 2004 » (« Rapport 2004 sur la situation en matière crime organisé »), Rapport du Conseil de l'Europe, page 145.

[121] Voir Sieber, précité, page 145.

- Divulguer des informations confidentielles (par exemple en publiant des secrets d'Etat ou des informations sensibles d'entreprise).

Il est vital de souligner le danger croissant que représente l'information trompeuse ou mensongère. La diffamation peut nuire à la réputation et atteindre la dignité de ses victimes de manière considérable, en ce que les déclarations en ligne sont accessibles à une audience mondiale. A partir du moment où l'information est publiée sur Internet, le ou les auteur(s) de cette dernière en perdent souvent le contrôle. Même si l'information est corrigée ou supprimée peu après sa publication, elle peut avoir été déjà dupliquée (« duplication » - « *mirroring* ») et rendue disponible par des personnes qui ne souhaitent pas la retirer. Dans ce cas, l'information peut rester disponible sur Internet, même si elle a été retirée ou modifiée par sa source de diffusion originelle[122]. Les exemples de telles situations incluent les cas de « gonflement des boites aux lettres » (« *runaway e-mails* »), dans lesquels des millions d'individus peuvent recevoir des messages grivois, trompeurs ou mensongers, relatifs à des personnes ou à des organisations. Le dommage causé à la réputation de ces dernières peut dans ce contexte s'avérer irréparable, nonobstant la vérité ou toute autre information que pouvait contenir le message originel. Dès lors, la liberté d'expression[123] et la protection des victimes potentielles de diffamation doivent être bien équilibrées[124].

Considérations relatives au filtrage d'Internet

Le filtrage de tels contenus est souvent imprudemment considéré comme une approche technique qui permettrait de faire face à la situation. La mesure soulèverait toutefois des questions substantielles, tant techniques que juridiques, qui devraient trouver une réponse. Ces questions sont détaillées aux chapitres 4, 5, 6 et 7 de la présente étude.

[122] Des difficultés similaires peuvent être identifiées en relation avec la disponibilité de l'information via la fonction « cache » des moteurs de recherche et des archives web, telles que http://www.archive.org.

[123] S'agissant du principe de liberté d'expression, voir Tedford, Herbeck et Haiman, Freedom of Speech in the United States (Liberté d'expression aux Etats-Unis), 2005 ; Barendt, Freedom of Speech (Liberté d'expression), 2007 ; Baker, Human Liberty and Freedom of Speech (La liberté humaine et la liberté d'expression) ; Emord, Freedom, Technology and the First Amendment (Liberté, technologie et le Premier amendement), 1991 ; S'agissant de l'importance du principe dans le contexte de la surveillance électronique, voir Woo et So, « The case for Magic Lantern : September 11 Highlights the need for increasing surveillance » (« L'affaire de la lanterne magique : le 11 septembre met à jour le besoin d'accroitre la surveillance »), Harvard Journal of Law & Technology, vol 15, n° 2, 2002, pages 530 et s. ; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant , (La liberté d'expression en droit australien ; une plante délicate), 2000 ; Volokh, « Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law » (« Liberté d'expression, loi sur le harcèlement religieux et loi sur l'aménagement religieux »), Loyola University Chicago Law Journal, vol. 33, 2001, pages 57 et s., disponible à l'adresse : http://www.law.ucla.edu/volokh/harass/religion.pdf ; Cohen, « Freedom of Speech and Press: Exceptions to the First Amendment » (« La liberté d'expression et la presse : exceptions au Premier amendement »), CRS Report for Congress 95-815, 2007, disponible à l'adresse : http://www.fas.org/sgp/crs/misc/95-815.pdf.

[124] Voir dans ce contexte, Reynolds, « Libel in the Blogosphere: Some Preliminary Thoughts » (« Diffamation dans la blogosphère : réflexions préliminaires »), Washington University Law Review, 2006, pages 1157 et s., disponible l'adresse : http://ssrn.com/abstract=898013 ; Solove, « A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere » (« L'histoire de deux blogueurs : libre expression et vie privée dans la blogosphère »), Washington University Law Review, vol. 84, 2006, pages 1195 et s., disponible à l'adresse : http://ssrn.com/abstract=901120 ; Malloy, Anonymous Bloggers And Defamation: « Balancing Interests On The Internet » (« Blogueurs anonymes et diffamation : équilibrer les intérêts sur Internet »), Washington University Law Review, vol 84, 2006, pages 1187 et s., disponible à l'adresse : http://law.wustl.edu/WULR/84-5/malloy.pdf.

4.4.7 Les contenus publiés par les organisations terroristes

Phénomène

Dans les années 1990, la discussion concernant l'utilisation d'Internet par des organisations terroristes se concentrait sur les attaques diligentées depuis le réseau contre des infrastructures critiques, telles que celles des transports ou de l'alimentation en énergie (« cyber terrorisme »), et sur l'utilisation des technologies de l'information dans les conflits armés (« cyber guerre ») [125]. Le succès d'attaques diligentées par des virus et des réseaux de zombies (« *botnet* ») a ceci dit clairement démontré l'existence de faiblesses en matière de sécurité des réseaux. Le succès d'attaques ayant pour base Internet, diligentées par des terroristes, est possible[126], mais il s'avère difficile d'évaluer l'importance de la menace[127]. Par ailleurs, jusqu'à ces dix dernières années au moins, le niveau d'interconnexion était faible comparé à la situation actuelle, et il est très probable que ce soit l'une des principales raisons – au delà de l'intérêt des Etats à conserver la confidentialité de la réussite de telles attaques - expliquant que très peu d'incidents de ce genre furent reportés. Tout du moins dans le passé, les chutes d'arbres présentaient un risque plus important, pour l'alimentation en énergie, que les attaques informatiques réussies[128].

Cette situation changea après les attaques du 11 septembre. Une discussion intensive commença, concernant l'utilisation par les terroristes des technologies de l'information et de la communication (TIC)[129]. Cette discussion fut facilitée par des rapports[130] selon lesquels les

---

[125] Gercke, « Cyberterrorism, How Terrorists Use the Internet » (« Cyber terrorisme : comment les terroristes utilisent Internet »), Computer und Recht, 2007, pages 62 et s.

[126] Rollins et Wilson, « Terrorist Capabilities for Cyberattack » (« La capacité des terroristes en matière de cyber-attaques »), 2007, page 10, disponible à l'adresse : http://www.fas.org/sgp/crs/terror/RL33123.pdf.

[127] La CIA indiqua en 2002 que les attaques contre les infrastructures critiques aux Etats-Unis allaient devenir une option pour les terroristes. Concernant la position de la CIA, voir Rollins et Wilson, « Terrorist Capabilities for Cyberattack » (« La capacité des terroristes en matière de cyber-attaques »), 2007, page 13, disponible à l'adresse :http://www.fas.org/sgp/crs/terror/RL33123.pdf. Toutefois, le FBI déclara que pour l'heure, le potentiel nécessaire à une campagne terroriste significative était insuffisant. S'agissant de la position du FBI, voir Nordeste et Carment, « A Framework for Understanding Terrorist Use of the Internet » (« Un cadre pour comprendre l'utilisation terroriste d'Internet »), 2006, disponible à l'adresse : http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp.

[128] Voir le rapport du Comité consultatif national sur la sécurité des télécommunications, Groupe de travail sur la sécurité des informations, évaluation du risque électrique (National Security Telecommunications Advisory Committee, Information Assurance Task Force, Electric Power Risk Assessment), disponible en anglais à l'adresse : http://www.aci.net/kalliste/electric.htm.

[129] Voir Lewis, « The Internet and Terrorism » (« Internet et le terrorisme »), disponible à l'adresse : http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf ; Lewis, « Cyber-terrorism and Cybersecurity » (« cyber terrorisme et cyber sécurité »), disponible à l'adresse : http://www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf ; Gercke, « Cyberterrorism, How Terrorists Use the Internet » (« Cyber terrorisme: comment les terroristes utilisent Internet »), Computer und Recht, 2007, pages 62 et s. ; Sieber et Brunst, « Cyberterrorism – the use of the Internet for terrorist purposes » (« Cyber terrorisme – l'utilisation d'Internet à des fins terroristes »), Publications du Conseil de l'Europe, 2007 ; Denning, « Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy » (« Activisme, activisme des pirates et cyberterrorisme : Internet en tant qu'outil permettant d'influencer la politique étrangère »), in Arquilla et Ronfeldt, *Networks & Netwars: The Future of Terror, Crime, and Militancy*, pages 239 et s., disponible à l'adresse : http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf ; Embar-Seddon, « Cyberterrorism, Are We Under Siege? » (« Cyberterrorisme, sommes-nous en état de siège ? »), American Behavioral Scientist, vol. 45, pages 1033 et s. ; United States Department of State, « Pattern of Global Terrorism » (Département d'Etat des Etats-Unis, « Modèle de terrorisme mondial »), 2000, in Prados, *America Confronts Terrorism*, 2002, 111 et s. ; Lake, *6 Nightmares (6 cauchemars)*, 2000, pages 33 et s. ; Gordon, *Cyberterrorism (Cyberterrorisme)*, disponible à l'adresse : http://www.symantec.com/avcenter/reference/cyberterrorism.pdf ; US-National Research Council, « Information Technology for Counterterrorism: Immediate Actions and Future Possibilities » (Conseil national de la recherche des Etats-Unis, « les technologies de l'information pour contrer le terrorisme :actions immédiates et possibilités futures »), 2003, pages 11 et s. ; *OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states (Commentaires de l'OSCE et de l'ODIHR sur le traitement législatif de la « cyberterreur » par le droit interne de chaque Etat)*, 2007, disponible à l'adresse : http://www.legislationline.org/download/action/download/id/816/file/82fbe0f348b5153338e15b446ae1.pdf.

[130] Voir Rötzer, Telepolis News, 4 nov. 2001, disponible à l'adresse: http://www.heise.de/tp/r4/artikel/9/9717/1.html.

terroristes utilisèrent Internet dans le cadre de la préparation de leur attaque[131]. Bien que l'attaque du 11 septembre n'ait pas été une cyberattaque, puisque le groupe qui l'a exécutée ne s'est pas livré à une attaque basée sur Internet, ce dernier réseau joua un rôle dans le cadre de la préparation de l'offensive[132]. Dans ce contexte, les différentes manières dont les organisations terroristes utilisent Internet furent découvertes[133]. Aujourd'hui, nous savons que les terroristes utilisent les TIC et Internet à des fins diverses. Dans le cadre du débat sur le filtrage, deux aspects présentent un intérêt particulier : la publication de propagande et la publication d'informations relatives à la commission d'infractions.

En 1998, seules 12 des 30 organisations terroristes étrangères qui se trouvent listées par le Département d'Etat des Etats-Unis (« *United States State Department* ») maintenaient des sites web pour informer le public de leurs activités[134]. En 2004, l'Institut des Etats-Unis pour la paix (« *United States Institute of Peace* ») rapportait que presque toutes les organisations terroristes maintenaient des sites web – dont le Hamas, le Hezbollah, le PKK et Al Qaida[135]. Les terroristes ont également commencé à utiliser les communautés vidéo (comme YouTube) pour distribuer des messages vidéo et de la propagande[136]. L'utilisation de sites web et d'autres forums sont le signe que les groupes subversifs accordent une attention plus professionnelle aux relations publiques[137]. Les sites web et autres médias sont utilisés par ces organisations pour disséminer de la propagande[138], pour publier des justifications[139] détaillées de leurs activités, ainsi que pour contacter leurs membres et donateurs et en recruter[140] de nouveaux.[141] Des sites web ont encore été utilisés pour distribuer des vidéos d'exécutions[142].

En outre, Internet peut être utilisé pour diffuser des ressources permettant de s'entraîner au terrorisme, telles que des instructions sur la manière d'utiliser des armes ou de sélectionner

---

[131] Le texte du message final fut rapporté comme étant : « Le semestre commence dans trois semaines. Nous avons obtenu 19 confirmations pour des études auprès de la faculté de droit, de la faculté de plannification urbaine, de la faculté des beaux-arts et de la faculté d'ingéniérie ». Le nom des facultés était apparemment le code de différentes cibles. Pour plus de détails voir Weimann, « How Modern Terrorism Uses the Internet » (« Comment le terrorisme moderne utilise Internet »), The Journal of International Security Affairs, Spring 2005, n° 8 ; Thomas, « Al Qaeda and the Internet: The danger of "cyberplanning" » (« Al Qaida et Internet : le danger de la "cyberplannification" »), 2003, disponible à l'adresse : http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6 ; Zeller, « On the Open Internet, a Web of Dark Alleys » (« Sur l'Internet libre, un web de ruelles sombres »), The New York Times, 20 décembre 2004, http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position.

[132] CNN, News, 4 août 2004, disponible à l'URL : http://www.cnn.com/2004/US/08/03/terror.threat/index.html.

[133] Pour un panorama, voir : Sieber et Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, (Cyber terrorisme – l'utilisation d'Internet à des fins terroristes), Publications du Conseil de l'Europe, 2007 ; Gercke, « Cyberterrorism, How Terrorists Use the Internet » (« Cyber terrorisme : comment les terroristes utilisent Internet »), Computer und Recht, 2007, pages 62 et s.

[134] ADL, Terrorism Update 1998, disponible à l'adresse : http://www.adl.org/terror/focus/16_focus_a.asp.

[135] Weimann, in *USIP Report*, « How Terrorists use the Internet » (« Comment les terroristes utilisent Internet »), 2004, page 3. Concernant l'utilisation d'Internet à des fins de propagande, voir également Crilley, « Information warfare: New Battlefields – Terrorists, propaganda and the Internet » (« Guerre de l'information : nouveaux champs de bataille – terroristes, propagande et Internet »), Aslib Proceedings, vol. 53, n° 7 (2001), page 253.

[136] Concernant l'utilisation de YouTube par les organisations terroristes, voir Heise News, article du 11 oct. 2006, disponible à l'adresse : http://www.heise.de/newsticker/meldung/79311 ; Staud, in *Sueddeutsche Zeitung*, 5 oct. 2006.

[137] Zanini et Edwards, « The Networking of Terror in the Information Age » (« La gestion de réseau de la terreur à l'ère de l'information »), in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 2001, page 42.

[138] United States Homeland Security Advisory Council, Report of the Future of Terrorism (Conseil consultatif des Etats-Unis pour la sécurité intérieure, Rapport sur le futur du terrorisme), 2007, page 4.

[139] S'agissant de la justification, voir Brandon*, Virtual Caliphate: Islamic extremists and the internet (Califat virtuel : extrémistes islamiques et Internet)*, 2008, disponible à l'adresse : http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

[140] Brachman, « High-Tech Terror: Al-Qaeda's Use of New Technology » (« Terreur high-tech : l'utilisation par Al-Qaida des nouvelles technologies »), The Fletcher Forum of World Affairs, vol. 30:2, 2006, pages 149 et s.

[141] Voir Conway, « Terrorist Use of the Internet and Fighting Back » (« Utilisation terrorisme d'Internet et résistance »), in *Information and Security*, 2006, page 16.

[142] Les videos montrant l'exécution des citoyens américains Berg et Pearl furent rendues disponibles sur des sites web. Voir Weimann, « How Terrorists use the Internet » (« Comment les teroristes utilisent Internet »), Rapport de l'USIP, 2004, page 5.

des cibles. De telles ressources sont disponibles en ligne à une large échelle[143]. En 2008, les services secrets occidentaux découvrirent un serveur Internet qui permettait l'échange de documents de formation au terrorisme, de même que l'établissement de communications[144]. Différents sites web furent signalés comme étant opérés par des organisations terroristes pour coordonner leurs activités[145].

Considérations relatives au filtrage d'Internet

Actuellement, les options permettant de faire face à ces défis sont intensivement discutées. La question de l'incrimination de la publication de telles ressources a été posée. En 2008, l'Union européenne ouvrit une discussion concernant une proposition de modification de la décision-cadre relative à la lutte contre le terrorisme[146]. Dans l'introduction de sa proposition, l'Union européenne souligne que le cadre juridique existant punit l'incitation à des infractions terroristes et la complicité en la matière, mais ne rend pas punissable la diffusion de savoir-faire terroriste par Internet[147]. Par sa proposition, l'Union européenne entend prendre les mesures de nature à combler les vides juridiques, et conduire les législations des Etats membres à se rapprocher des dispositions de la Convention du Conseil de l'Europe pour la prévention du terrorisme. Sur la base de l'article 3, paragraphe 1 (c)[148] de la proposition, les Etats membres doivent par exemple rendre punissable la publication d'instructions sur la manière d'utiliser des explosifs en sachant que cette information a pour but de servir à la réalisation d'un acte terroriste. Une telle situation ouvre la porte à de nouveaux débats sur le besoin potentiel de filtrer de tels contenus, en plus d'en rendre la publication punissable[149].

[143] Brunst, in Sieber et Brunst, *Cyberterrorism – the use of the Internet for terrorist purposes* (*Cyber terrorisme – l'utilisation d'Internet à des fins terroristes*), publication du Conseil de l'Europe, 2007 ; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force (Conseil consultatif des Etats-Unis pour la sécurité intérieure, Rapport du groupe de travail sur le futur du terrorisme), janvier 2008, page 5 ; Stenersen, « The Internet: A Virtual Training Camp? » (« Internet : un camp d'entraînement virtuel ? »), in *Terrorism and Political Violence*, 2008, pages 215 et s.

[144] Musharbash, « Bin Ladens Intranet » (« L'intranet de Ben Laden »), Der Spiegel, vol. 39, 2008, page 127.

[145] Weimann, « How Modern Terrorism uses the Internet » (« Comment le terrorisme moderne utilise Internet »), 116 Special Report of the United States Institute of Peace, 2004, page 10.

[146] Proposition de décision-cadre du Conseil modifiant la décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme, COM(2007) 650.

[147] « *L'article 4 de la décision-cadre relative à la lutte contre le terrorisme dispose que l'incitation à des infractions terroristes et la complicité en la matière doivent être rendues punissables par les États membres. L'article 2 dudit instrument impose aux États membres de déclarer pénalement responsables les personnes qui dirigent un groupe terroriste ou participent à ses activités. Ces dispositions, toutefois, ne s'appliquent pas explicitement à la diffusion de propagande et de savoir-faire terroristes, notamment par Internet* ».

[148] L'« *entraînement pour le terrorisme* » correspond au « *fait de fournir des instructions pour la fabrication ou l'utilisation d'explosifs, d'armes à feu, d'autres armes ou de substances nocives ou dangereuses, ou pour d'autres méthodes ou techniques spécifiques, en vue de commettre l'un des actes énumérés à l'article 1er, paragraphe 1, en sachant que la formation dispensée a pour but de servir à la réalisation d'un tel objectif* ».

[149] S'agissant de la question du filtrage, voir Conway, « Terrorism and Internet Governance: Core Issues » (« Terrorisme et gouvernance d'Internet : problématiques principales »), ICTs and International Security, Disarmament Forum, 2007, fascicule (issue) 3, page 26 ; Franco Frattini, Press release, 14 sept. 2007, « "The right to privacy of internet users: let's find a balanced way to ensure both the right to exchange information and public security" says Franco Frattini » (« "Le droit à la vie privée des internautes : trouvons le moyen équilibré d'assurer tant le droit d'échanger de l'information que la sécurité publique », déclare Franco Frattini »), http://ec.europa.eu/commission_barroso/frattini/news/archives_2007_en.htm#september.

4.4.8 Les violations de droits d'auteur

Phénomène

Avec le passage de l'analogique au numérique[150], la numérisation[151] a permis à l'industrie du spectacle d'ajouter de nouveaux éléments et services aux films sur DVD, tels que différentes langues, des sous-titres, des bandes-annonces et des bonus. Les CD et DVD ont montré avoir une meilleure longévité que les disques et les vidéocassettes[152].

La numérisation a également ouvert la porte à de nouvelles violations de droits d'auteur. Ces dernières sont actuellement permises par la rapidité et la fidélité de la reproduction. Avant la numérisation, la copie d'un disque ou d'une vidéocassette entraînait toujours une perte de qualité. Aujourd'hui, il est possible de dupliquer des sources numériques sans perte de qualité, et également, de fait, de faire des copies à partir de n'importe quelle copie. Les violations de droits d'auteur les plus courantes incluent :

- La mise à disposition ou l'échange[153] de musiques, fichiers et logiciels protégés par des droits d'auteur, par l'intermédiaire de systèmes de partage de fichiers[154] ;
- Le contournement des systèmes de gestion des droits numériques (« *Digital Rights Management systems* »)[155].

Les systèmes de partage de fichiers sont des services en réseau basés sur la technologie de pair à pair (« *peer-to-peer* »)[156], qui permettent à leurs utilisateurs de partager des fichiers[157],

---

[150] Concernant le processus de transition en cours, voir le résumé du rapport de l'OCDE intitulé « Perspectives des technologies de l'information 2006 : principales conclusions » (Information Technology Outlook 2006, highlights), pages 10 et 11, disponible à l'adresse : http://www.oecd.org/dataoecd/27/58/37487613.pdf (version anglaise disponible à l'adresse : http://www.oecd.org/dataoecd/27/59/37487604.pdf).

[151] Voir Hartstack, « Die Musikindustrie unter Einfluss der Digitalisierung », pages 34 et s.

[152] A côté de ces améliorations, la numérisation a rendu la production des copies plus rapide et en a baissé les coûts, qui étaient l'un des éléments clefs de motivation de l'industrie à engager une transition vers des technologies numériques.

[153] Dans certains pays, il existe des exceptions à l'interdiction de reproduire des fichiers protégés. En conséquence de ces exceptions, le téléchargement peut ne pas être illégal. En France, par exemple, la copie n'est pas illégale lorsqu'elle est réservée à un usage privé, et les juridictions de l'ordre judiciaire ne se sont pas encore réellement prononcées sur la question de savoir si le téléchargement, à partir d'une matrice illégale, était lui-même illégal : sur cette discussion, voir Estelle De Marco, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », 4 juin 2009, Juriscom.net, page 6, disponible à l'adresse : http://www.juriscom.net/uni/visu.php?ID=1133.

[154] Sieber, « Organised crime situation report 2004 » (« Rapport 2004 sur la situation en matière crime organisé »), Rapport du Conseil de l'Europe, page 148.

[155] Les systèmes de gestion des droits numériques renvoient aux technologies de contrôle d'accès qui sont utilisées pour limiter l'utilisation des médias numériques. Pour de plus amples informations, voir : Cunard, Hill et Barlas, « Current developments in the field of digital rights management » (« Développements actuels en matière de systèmes de gestion des droits numériques »), disponible à l'adresse : http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf ; Lohmann, « Digital Rights Management: The Skeptics' View » (« Les systèmes de gestion des droits numériques : l'opinion des sceptiques », disponible à l'adresse : http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf. Baesler, « Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world » (« Les mesures techniques de protection aux Etats-Unis, dans l'Union européenne et en Allemagne : de quel degré de "fair use" avons-nous besoin dans le monde numérique »), Virginia Journal of Law and Technology, vol. 8, 2003, disponible à l'adresse : http://www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

[156] Le Pair à pair (ou Peer-to-Peer, P2P) permet une connectivité directe entre les participants, dans un réseau, se différenciant par là des communications échangées par l'intermédiaire des conventionnelles structures centralisées basées sur serveur. Voir : Schoder, Fischbach et Schmitt, « Core Concepts in Peer-to-Peer Networking » (« Concepts centraux de la gestion de réseau en peer-to-peer »), 2005, disponible à l'adresse : http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf ; Androutsellis-Theotokis et Spinellis, « A Survey of Peer-to-Peer Content Distribution Technologies » (« Une étude des technologies de distribution de contenus en peer-to-peer »), 2004, disponible à l'adresse : http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

[157] GAO, File Sharing, « Selected Universities Report Taking Action to Reduce Copyright Infringement » (« Rapport d'universités sélectionnées pour agir en réduction des infractions aux droits d'auteur »), disponible à l'adresse : http://www.gao.gov/new.items/d04503.pdf ; Ripeanu, Foster et Iamnitchi, « Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design » (« Cartographie du réseau Gnutella : propriété des systèmes de peer-to-peer à grande échelle et implications

souvent avec des millions d'autres utilisateurs[158]. Une fois qu'ils ont installé le logiciel de partage de fichiers, les utilisateurs peuvent sélectionner les fichiers qu'ils souhaitent offrir en partage, et utiliser le logiciel pour chercher d'autres fichiers, mis à disposition par les autres utilisateurs, qu'ils peuvent alors télécharger à partir de centaines de sources différentes. Avant que les systèmes de partage de fichiers ne soient développés, les individus copiaient et s'échangeaient des disques et des cassettes, mais les systèmes de partage de fichiers permettent l'échange de copies entre beaucoup plus d'utilisateurs.

Les technologies permettant le pair à pair jouent un rôle essentiel sur Internet. A l'heure actuelle, plus de 50 pour cent du trafic des abonnés à Internet est généré par les réseaux de pair à pair[159]. Le nombre d'utilisateurs est sans cesse croissant – un rapport publié par l'OCDE estime à quelques 30 pour cent le nombre d'internautes français ayant téléchargé de la musique ou des fichiers à l'aide de systèmes de partage de fichiers[160], les autres pays de l'OCDE présentant des tendances similaires[161]. Bien entendu, certains des fichiers et des musiques échangés par les protocoles de pair à pair sont soit (i) offerts par l'artiste lui-même (qu'il soit ou non émergent), soit (ii) vendus par le producteur sur ce protocole. En conséquence, certains de ces actes de mise à disposition ou de téléchargement sont conformes à la loi. Les systèmes de partage de fichiers peuvent être utilisés pour échanger toutes sortes de données informatiques, musique, films et logiciels inclus[162]. Historiquement, ces systèmes ont été principalement utilisés pour échanger de la musique, mais l'échange de vidéos y devient de plus en plus important[163].

La technologie utilisée dans les services de partage de fichiers est extrèmement sophistiquée et permet l'échange de fichiers de taille importante sur de courtes périodes de temps[164]. Les

---

pour la conception du système »), disponible à l'adresse : http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. Federal Trade Commission des Etats-Unis, « Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues » (« Technologies de partage de fichiers en peer-to-peer : protection du consommateur et questions de concurrence »), page 3, disponible à l'adresse : http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf ; Saroiu, Gummadi et Gribble, « A Measurement Study of Peer-to-Peer File Sharing Systems » (« Une étude de mesure des systèmes de partage de fichiers en peer-to-peer »), disponible à l'adresse : http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

[158] En 2005, 1,8 millions d'internautes utilisaient Gnutella. Voir Mennecke, « eDonkey2000 Nearly Double the Size of FastTrack » (« La taille d'eDonkey2000 atteint quasiment le double de celle de FastTrack »), disponible à l'adresse : http://www.slyck.com/news.php?story=814.

[159] Voir Cisco « Global IP Traffic Forecast and Methodology » (« Trafic IP mondial : prévisions et méthodologie »), 2006-2011, 2007, page 4, disponible à l'adresse : http://www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd806a81aa.pdf.

[160] Voir le rapport 2004 de l'OCDE intitulé « Perspectives des technologies de l'information de l'OCDE – principales conclusions » (Information Technology Outlook, highlights), page 192, disponible en anglais à l'adresse : http://www.oecd.org/dataoecd/22/18/37620123.pdf (résumé en français disponible à l'adresse : http://www.oecd.org/dataoecd/20/60/33952178.pdf).

[161] Un exemple est l'Allemagne, où un rapport régulièrement mis à jour de la fédération de l'industrie phonographique indiquait que, en 2006, 5,1 millions d'utilisateurs en Allemagne téléchargeaient de la musique par l'intermédiaire des systèmes de partage de fichiers. Le rapport est disponible à l'adresse : http://www.ifpi.de/wirtschaft/brennerstudie2007.pdf. S'agissant des Etats-Unis, voir Johnson, McGuire et Willey, « Why File-Sharing Networks Are Dangerous » (« Pourquoi les réseaux de partage de fichiers sont dangereux »), 2007, disponible à l'adresse : http://oversight.house.gov/documents/20070724140635.pdf.

[162] Au delà de la musique, des vidéos et des logiciels, des documents personnels sensibles sont également souvent trouvés sur les réseaux de partage de fichiers. Voir Johnson, McGuire et Willey, « Why File-Sharing Networks Are Dangerous » (« Pourquoi les réseaux de partage de fichiers sont dangereux »), 2007, disponible à l'adresse : http://oversight.house.gov/documents/20070724140635.pdf.

[163] Alors qu'en 2002 les fichiers musicaux représentaient plus de 60% de l'ensemble des fichiers échangés sur les réseaux de partage de fichiers dans les pays de l'OCDE, cette proportion tomba en 2003 à moins de 50%. Voir le rapport 2004 de l'OCDE intitulé « Perspectives des technologies de l'information de l'OCDE » (Information Technology Outlook), page 192, disponible en anglais à l'adresse : http://www.oecd.org/dataoecd/22/18/37620123.pdf (résumé en français disponible à l'adresse : http://www.oecd.org/dataoecd/20/60/33952178.pdf).

[164] Schoder, Fischbach et Schmitt, « Core Concepts in Peer-to-Peer Networking » (« Concepts centraux de la gestion de réseau en peer-to-peer »), 2005, page 11, disponible à l'adresse : http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf ; Cope, « Peer-to-Peer Network » (« Le réseau Peer-to-Peer »), Computerworld, 8 avril 2002, disponible à l'adresse : http://www.computerworld.com/networkingtopics/networking/story/0,10801,69883,00.html ; Fitch, « From Napster to Kazaa: What the Recording Industry did wrong and what options are left » (« De Napster à Kazaa : quelles furent les erreurs de l'industrie du disque et quelles sont les options restantes »), Journal of

systèmes de partage de fichiers de première génération dépendaient d'un serveur central, qui a permis aux services en charge de l'application de la loi d'agir contre les partages de fichiers illégaux dans le réseau Napster[165]. A la différence de ces systèmes de première génération (spécialement le fameux service Napster), les systèmes de partage de fichiers de deuxième génération ne sont plus basés sur un serveur central fournissant la liste des fichiers disponibles entre les utilisateurs[166]. Les tentatives d'empêcher ces derniers systèmes d'opérer est plus difficile, en raison de leur décentralisation. Toutefois, en raison des communications directes qui s'établissent entre les utilisateurs, il reste possible de suivre la trace de ces derniers grâce à leur adresse IP[167]. Les services en charge de l'application de la loi ont rencontré certains succès, dans le cadre d'investigations sur des violations de droits d'auteur commises à l'aide de systèmes de partage de fichiers. Des versions plus récentes de ces systèmes permettent des formes anonymes de communication ainsi qu'un chiffrement facile, ce qui rendra les investigations plus difficiles[168].

Les technologies de partage de fichiers ne sont pas seulement utilisées par des personnes ordinaires et des délinquants, mais également par le monde des affaires[169]. Tous les fichiers échangés sur les réseaux de partage de fichiers ne violent pas des droits d'auteur. Parmi les exemples d'utilisation légitime de ces réseaux, figure l'échange autorisé de copies ou de créations artistiques tombées dans le domaine public[170].

Technology Law and Policy, vol. 9, fascicule (issue) 2, disponible à l'adresse : http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[165] Concernant Napster et la réponse juridique, voir : Rayburn, « After Napster » (« Après Napster »), Virginia Journal of Law and Technology, vol. 6, 2001, disponible à l'adresse : http://www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html ; Penn, « Copyright Law: Intellectual Property Protection in Cyberspace » (« La loi sur le copyright : la protection de la propriété intellectuelle dans le cyberespace »), Journal of Technology Law and Policy, vol. 7, Issue 2, disponible à l'adresse : http://grove.ufl.edu/~techlaw/vol7/issue2/penn.pdf.

[166] S'agissant de la technologie sous-jacente, voir : Fischer, « The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities » (« Internet au 21ème siècle : une photocopieuse numérique : analyse du droit d'auteur, questions et options »), Virginia Journal of Law and Technology, vol. 7, 2002, disponible à l'adresse : http://www.vjolt.net/vol7/issue3/v7i3_a07-Fisher.pdf ; Sifferd, « The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology » (« La révolution peer-to-Peer : une analyse post-Napster de la technologie à développement rapide de partage de fichiers », Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93 ; Ciske, « For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services » (« Pour l'heure, les FAI doivent rester sur leur position et délivrer : une analyse de l'affaire in *re* Recording Industry Association of America c/ Verizon Internet Services »), Virginia Journal of Law and Technology, vol. 8, 2003, disponible à l'adresse : http://www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf ; Herndon, « Who's watching the kids? – The use of peer-to-peer programs to Cyberstalk children » (« Qui surveille les enfants ? – l'utilisation des programmes peer-to-peer pour cybertraquer les enfants »), Oklahoma Journal of Law and Technology, vol. 12, 2004, disponible à l'adresse : http://www.okjolt.org/pdf/2004okjoltrev12.pdf ; Fitch, « From Napster to Kazaa: What the Recording Industry did wrong and what options are left » (« De Napster à Kazaa : quelles furent les erreurs de l'industrie du disque et quelles sont les options restantes »), Journal of Technology Law and Policy, vol. 9, fascicule (issue) 2, disponible à l'adresse : http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[167] Pour plus d'informations concernant les investigations sur les réseaux peer-to-peer, voir « Investigations Involving the Internet and Computer Networks » (« Investigations impliquant Internet et les réseaux informatiques »), NIJ Special Report, 2007, pages 49 et s., disponible à l'adresse : http://www.ncjrs.gov/pdffiles1/nij/210798.pdf.

[168] Clarke, Sandberg, Wiley et Hong, « Freenet: a distributed anonymous information storage and retrieval system » (« Freenet : un système distribué et anonyme de stockage et de transfert de l'information »), 2001 ; Chothia et Chatzikokolakis, « A Survey of Anonymous Peer-to-Peer File-Sharing » (« Une étude du partage anonyme de fichiers en peer-to-peer »), disponible à l'adresse : http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf ; Han, Liu et Xiao, Xiao, « A Mutual Anonymous Peer-to-Peer Protocol Desing » (« Une conception du protocole peer-to-peer permettant un anonymat mutuel entre les pairs »), 2005.

[169] Concernant les motivations des utilisateurs des technologies de peer-to-peer, voir Belzley, « Grokster and Efficiency in Music » (« Grokster et l'efficacité de l'industrie de la musique »), Virginia Journal of Law and Technology, vol. 10, fascicule (issue) 10, 2005, disponible à l'adresse : http://www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

[170] Pour plus d'exemples, voir l'affaire jugée par la Cour suprême des Etats-Unis, *Metro-Goldwyn-Mayer Studios Inc. c/ Grokster, Ltd, I. B.*, disponible à l'adresse : http://fairuse.stanford.edu/MGM_v_Grokster.pdf.

Quoi qu'il en soit, l'utilisation des systèmes de partage de fichiers est source de défis, pour l'industrie du divertissement[171]. La proportion de la baisse de vente de CD et DVD ainsi que de billets de cinéma due à l'échange de titres sur les systèmes de partage de fichiers n'est pas clairement connue. Les recherches ont identifié des millions d'utilisateurs de réseaux de pair à pair[172], et des milliards de fichiers téléchargés sur ces réseaux[173]. Toute baisse de revenus pourrait provenir d'autres facteurs, tels que la diversification des médias et des supports, tandis que le partage de fichiers pourrait générer d'autres types de revenus, tels que des ventes de billets de concert ou de produits dérivés (T-shirts, jeux, vidéos, etc.). Des copies de films sont apparues sur les réseaux de partage de fichiers avant que ces films ne soient officiellement diffusés au cinéma[174], aux dépens des titulaires de droits. Le développement récent de systèmes de partage de fichiers anonymes et chiffrés rendra le travail des titulaires de droits plus difficile, comme celui des services en charge de l'application de la loi[175].

Considérations relatives au filtrage d'Internet

Tandis que les approches juridiques internationales se concentrent sur la pénalisation des violations de droits d'auteur commises à une « échelle commerciale », les discussions relatives aux approches nationales sont plus larges, et incluent la question d'empêcher les utilisateurs impliqués dans une violation de droits d'auteur en ligne d'accéder à Internet. Cette dernière approche a fait l'objet d'une discussion controversée au cours des débats sur la réforme du cadre des télécommunications[176], et a été rejetée tant par le Parlement européen[177] que par la Commission européenne en première lecture[178]. En 2008, la France introduisit un projet de loi qui aurait imposé aux fournisseurs d'accès à Internet de proscrire l'utilisation de leurs services aux utilisateurs qui auraient été accusés, de manière répétitive, de contrevenir aux droits d'auteur[179]. Cette approche aurait été critiquée par la Commission européenne[180].

[171] S'agissant de l'impact économique, voir Liebowitz, « File-Sharing: Creative Destruction or Just Plain Destruction » (« Partage de fichiers : destruction de valeur créative ou simple destruction »), Journal of Law and Economics, 2006, volume 49, pages 1 et s.

[172] La dernière analyse relative aux activités de partage de fichiers en Allemagne identifia jusqu'à 7,3 millions d'utilisateurs téléchargeant des fichiers musicaux à partir d'Internet. Jusqu'à 80% de ces téléchargements ont été effectués via des systèmes de partage de fichiers. Source : GfK, Brennerstudie 2005.

[173] « The Recording Industry 2006 Piracy Report » (« Rapport 2006 de l'industrie du disque sur le piratage »), page 4, disponible à l'adresse : http://www.ifpi.org/content/library/piracy-report2006.pdf.

[174] Un exemple est le film « Star Wars – épisode 3 », qui apparu sur les réseaux de partages de fichiers quelques heures avant sa première sortie officielle. Voir http://www.heise.de/newsticker/meldung/59762, se référant à un communiqué de presse de la MPAA.

[175] Concernant les systèmes de partage de fichiers anonymes, voir Wiley et Hong, « Freenet: A distributed anonymous information storage and retrieval system » (« Freenet : un système distribué et anonyme de stockage et de transfert de l'information »), in *Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability*, 2000.

[176] Horten, « The Telecoms Package and "3 strikes" – voluntary cooperation to restrict downloads » (« Le Paquet Télécom et le système des 3 avertissements - coopération volontaire pour limiter le téléchargement »), 2008.

[177] Vote du Parlement européen du 24 septembre 2008.

[178] Voir le communiqué de presse de la Commission, « Réforme du cadre des télécommunications : la Commission présente de nouveaux textes législatifs pour préparer la voie à un compromis entre le Parlement et le Conseil », 7 novembre 2008.

[179] Voir Ozimek, « France gets closer to "three strike" downloader web ban » (« la France est sur le point d'exclure du web les téléchargeurs ayant fait l'objet de trois notifications »), The Register, 12 juin 2008, disponible à l'adresse : http://www.theregister.co.uk/2008/06/12/france_music_law/.

[180] Voir : « Loi antipiratage sur Internet : les observations de Bruxelles », La Tribune, 27 nov. 2008, disponible à l'adresse : http://www.latribune.fr/entreprises/communication/telecom-internet/20081127trib000314818/loi-antipiratage-sur-internet-les-observations-de-bruxelles-.html.

4.5 Pourquoi envisager le filtage d'Internet ?

L'étude des motivations qui sous-tendent le filtrage d'Internet montre que ce dernier est souvent utilisé pour répondre à des défis techniques et juridiques. Cette section dresse un panorama de certaines des motivations globales qui se trouvent discutées dans le contexte du filtrage.

4.5.1 Le manque d'instruments de contrôle

L'opérabilité de la plupart des réseaux de communication de masse – des réseaux téléphoniques utilisés pour les appels téléphoniques vocaux à Internet – requiert une administration centrale et l'existence de standards techniques. Les discussions actuelles relatives à la gouvernance d'Internet pourraient suggérer au novice que ce réseau n'est pas différent des autres infrastructures de communication nationales et même transnationales[181]. Internet doit également être gouverné par la loi, et tant les législateurs que les services en charge de l'application de la loi ont commencé à développer des standards juridiques, nécessitant un certain degré de contrôle central.

Internet a été initialement conçu et financé pour le réseau de la Défense[182]. Sa conception est basée sur une architecture réseau décentralisée, cherchant à préserver intactes ses fonctionnalités principales et sa capacité de fonctionnement, même lorsque des parties du réseau sont attaquées. En conséquence, l'infrastructure de réseau d'Internet est résistante aux tentatives extérieures de contrôle. Cette dernière n'a pas été originellement conçue pour faciliter les investigations pénales ou pour prévenir les attaques provenant de l'intérieur du réseau.

Aujourd'hui, Internet est utilisé de manière croissante dans le cadre de services civils. Avec ce passage du monde de la Défense aux services civil, la nature de la demande, en termes d'instruments de contrôle, a changé. Puisque le réseau fonctionne sur la base de protocoles conçus pour les besoins de la Défense, de tels instruments de contrôle centraux sont limités voire inexistants, et il est difficile de les implémenter de manière rétrospective, sans redéfinition conséquente du réseau. L'absence d'instruments de contrôle rend les investigations en matière de cybercriminalité très difficiles[183].

Des initiatives de filtrage pourraient être considérées comme une manière d'implémenter ces instruments de contrôle, qui n'ont pas été prévus dans le cadre du développement du réseau.

4.5.2 La dimension internationale

Un grand nombre des processus de transfert de données concernent plus d'un seul pays[184]. Les protocoles utilisés pour ces transferts de données, sur Internet, se basent sur des politiques de routage qui restent propres à chaque prestataire de service. Ils sont capables de franchir dynamiquement les obstacles si des liaisons directes sont temporairement bloquées[185]. Même lorsque les transferts n'ont lieu qu'au sein d'un même pays, les données

---

[181] Voir par exemple Sadowsky, Zambrano et Dandjinou, « Internet Governance: A Discussion Document » (« Gouvernance d'Internet : un document de discussion »), 2004, disponible à l'adresse : http://www.internetpolicy.net/governance/20040315paper.pdf.

[182] Pour un bref aperçu de l'histoire d'Internet, incluant ses origines militaires, voir Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, Wolff, « A Brief History of the Internet » (« L'histoire d'Internet en bref »), disponible à l'adresse : http://www.isoc.org/internet/history/brief.shtml.

[183] Lipson, « Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues » (« Dépister et remonter la trace des cyberattaques : défis techniques et questions de politique globale »).

[184] S'agissant du volume que représentent les attaques transnationales au sein des cyberattaques qui causent le plus de dommages, voir Sofaer et Goodman, « Cyber Crime and Security – The Transnational Dimension » (« cybercriminalité et sécurité – la dimension transnationale ») in Sofaer et Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, page 7, disponible à l'adresse : http://media.hoover.org/documents/0817999825_1.pdf.

[185] Les premiers protocoles de communication, qui restent aussi les plus importants, sont le protocole TCP (*Transmission Control Protocol*) et le protocole IP (*Internet Protocol*). Pour plus d'informations, voir

peuvent quitter ce pays, être transmises par l'intermédiaire de routeurs se situant à l'extérieur de son territoire, puis être redirigées dans ce même pays vers leur destination finale[186]. Plus loin, de nombreux services Internet se basent sur des services qui sont rendus à l'étranger[187] : par exemple, des fournisseurs d'hébergement peuvent offrir un espace web à la location dans un pays, tandis que leur serveur informatique se trouve dans un autre pays[188]. La mise à disposition de contenus n'impose pas à son responsable d'utiliser des services d'hébergement qui se trouvent dans le pays depuis lequel il agit.

Lorsque les délinquants stockent des informations hors du pays dans lequel ils sont domiciliés, les investigations en matière de cybercriminalité nécessitent la coopération des autorités en charge de l'application de la loi dans chacun des pays concernés[189]. Le principe de souveraineté nationale ne permet pas que des investigations soient diligentées sur le territoire de différents pays sans l'accord des autorités locales de ces pays[190]. La coopération internationale basée sur les principes de la traditionnelle assistance juridique mutuelle est très consommatrice de temps. Les exigences de forme et le temps nécessaires à la collaboration avec les services en charge de l'application de la loi à l'étranger entravent souvent les investigations[191]. Les investigations s'opèrent souvent sur de courtes périodes de temps[192]. Les données qui sont vitales à la traçabilité des infractions sont souvent supprimées après un court délai. Cette courte fenêtre de tir, dont bénéficient les investigations, est problématique, car les régimes traditionnels d'assistance juridique mutuelle prennent souvent du temps pour être organisés[193].

Le filtrage d'Internet pourrait dès lors être considéré comme une manière d'agir, même dans ce type de cas où les limites de la coopération internationale empêchent que des mesures soient prises en un laps de temps approprié. Toutefois, le filtrage ne facilite pas l'obtention de données sur l'infraction, pas plus qu'il ne permet d'en trouver l'auteur.

Tanebaum, *Computer Networks (Les réseaux informatiques)* ; Comer, *Internetworking with TCP/IP – Principles, Protocols and Architecture (Interréseautage avec TCP/IP : principes, protocoles et architecture)*.

[186] Voir Kahn et Lukasik, « Fighting Cyber Crime and Terrorism: The Role of Technology » (« Lutter contre la cybercriminalité et le terrorisme : le rôle des technologies »), présentation à la Conférence de Stanford (Stanford Conference), décembre 1999, page 6 et s. ; Sofaer et Goodman, « Cyber Crime and Security – The Transnational Dimension » (« cybercriminalité et sécurité – la dimension transnationale », in Sofaer et Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, page 6, disponible à l'adresse : http://media.hoover.org/documents/0817999825_1.pdf.

[187] Un exemple de la coopération internationale des entreprises et de la délégation au sein des entreprises internationales, est l'affaire Compuserve. Le dirigeant de la filiale allemande (Compuserve Allemagne) était poursuivi pour avoir rendu disponibles des contenus pédopornographiques, lesquels étaient accessibles à partir du système informatique de la maison mère basée aux Etats-Unis, connecté à l'entreprise allemande. Voir Amtsgericht Muenchen, Multimedia und Recht 1998, pages 429 et s. (note Sieber).

[188] Voir Huebner, Bem et Bem, « Computer Forensics – Past, Present And Future » (« Informatique légale – passé, présent et futur »), n°.6, disponible à l'adresse : http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf ; Concernant les possibilités offertes par les services de stockage en réseau, voir Clark, « Storage Virtualisation Technologies for Simplyfing Data Storage and Management » (« Technologies de stockage par virtualisation pour simplifier le stockage et la gestion de données »).

[189] S'agissant du besoin de coopération internationale dans la lutte contre la cybercriminalité, voir : Putnam et Elliott, « International Responses to Cyber Crime » (« Réponses internationales à la cybercriminalité »), in Sofaer et Goodman, *Transnational Dimension of Cyber Crime and Terrorism*, 2001, pages 35 et s., disponible à l'adresse : http://media.hoover.org/documents/0817999825_35.pdf ; Sofaer et Goodman, « Cyber Crime and Security – The Transnational Dimension » (« Cyberciminalité et sécurité : la dimension transnationale »), in Sofaer et Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, pages 1 et s., disponible à l'adresse : http://media.hoover.org/documents/0817999825_1.pdf.

[190] La souveraineté nationale est un principe fondamental du droit international. Voir Roth, « State Sovereignty, International Legality, and Moral Disagreement » (« Souveraineté de l'Etat, légalité internationale et désagrément moral »), 2005, page 1, disponible à l'adresse : http://www.law.uga.edu/intl/roth.pdf.

[191] Voir Gercke, « The Slow Wake of A Global Approach Against Cybercrime » (« Le lent réveil d'une approche mondiale contre la cybercriminalité »), Computer Law Review International 2006, 142. Pour des exemples, voir Sofaer et Goodman, « Cyber Crime and Security – The Transnational Dimension » (« Cyberciminalité et sécurité : la dimension transnationale »), in Sofaer et Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, page 16, disponible à l'adresse : http://media.hoover.org/documents/0817999825_1.pdf.

[192] Voir supra, chapitre 3.3.2.

[193] Voir Gercke, « The Slow Wake of A Global Approach Against Cybercrime » (« Le lent réveil d'une approche mondiale contre la cybercriminalité »), Computer Law Review International 2006, 142.

4.5.3 L'importance décroissante de l'infrastructure nationale d'hébergement

Lorsque l'on aborde la question des contenus illégaux, le temps n'est pas le seul élément à poser des difficultés. Le principe de double incrimination[194] est également une source de problèmes lorsque l'infraction ne tombe pas sous le coup de la loi pénale dans l'un des pays impliqués dans les investigations[195]. Les auteurs d'infractions peuvent d'ailleurs impliquer délibérément plusieurs pays, dans le cadre de leurs attaques, afin de rendre les investigations plus difficiles[196]. Par exemple, s'ils stockent des contenus illégaux sur des serveurs qui se trouvent dans un pays qui ne rend pas de telles publications punissables, les tentatives juridiques d'obtenir le retrait de l'information à sa source pourraient se révéler infructueuses.

Comme nous le signalions plus haut, la publication de contenus illégaux n'impose pas au responsable de cette publication d'utiliser des services d'hébergement qui se trouvent dans le pays depuis lequel il agit.

Les contenus illégaux ne sont pas toujours appréhendés de la même manière par la loi pénale, selon les pays. La publication d'un contenu peut s'avérer parfaitement conforme à la loi dans un pays, et constituer une infraction pénale dans un autre pays.

Les tentatives de filtrage de contenus peuvent dès lors être considérées comme des actes de reterritorialisation, lorsque l'objectif d'un pays est de s'assurer que ses normes nationales s'appliquent à l'ensemble du contenu disponible sur Internet, pour les personnes qui utilisent Internet sur son territoire.

4.5.4 Evaluation des problématiques dans le contexte du filtrage

Le fait qu'un contenu puisse être stocké à l'extérieur d'un pays qui rend punissable sa publication, sans que cela n'affecte la possibilité, pour les individus de ce même pays, d'y avoir accès, est sans doute l'une des principales raisons pour lesquelles la question du filtrage est examinée.

---

[194] La double incrimination a lieu lorsque l'acte litigieux constitue une infraction sur le sol tant de l'Etat requis que de l'Etat requérant. Les difficultés que peut poser le principe de la double incrimination dans le cadre des investigations internationales constituent actuellement une vraie problématique, dans le cadre d'un certain nombre de conventions et de traités internationaux. Les exemples incluent l'article 2 de la décision-cadre de l'Union européenne du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres (2002/584/JAI).

[195] S'agissant du principe de la double incrimination dans les enquêtes internationales, voir : United Nations Manual on the Prevention and Control of Computer-Related Crime (Manuel des Nations-Unies relatif à la prévention et au contrôle des infractions liées à l'informatique), 269, disponible à l'adresse : http://www.uncjin.org/Documents/EighthCongress.html ; Schjolberg et Hubbard, « Harmonizing National Legal Approaches on Cybercrime » (« Harmoniser les approches juridiques nationales de la cybercriminalité »), 2005, page 5, disponible à l'adresse : http://.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[196] Voir: Lewis, « Computer Espionage, Titan Rain and China » (« Espionnage informatique, "Titan rain" et la Chine », page 1, disponible à l'adresse : http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

4.6 Qui filtrer ?

Les intentions qui sous-tendent les initiatives de filtrage peuvent varier de manière significative. La diversité des objectifs poursuivis est essentiellement due à la grande variété de contenus qui se trouvent concernés par les discussions sur le filtrage[197]. La présente section se concentre sur les intentions qui sous-tendent le filtrage de la pédopornographie.

Dans ce contexte, il est généralement possible de distinguer entre deux centres d'intérêts, qui sont le fournisseur de contenu (le producteur) d'une part, et l'utilisateur (le consommateur) d'autre part.

4.6.1 Le producteur des contenus illégaux – le fournisseur de contenus illégaux

Cadre

Internet est devenu un outil majeur de ***distribution*** de contenus à caractère pédopornographique, en ce qu'il offre un certain nombre d'avantages aux auteurs d'infractions, avantages qui rendent les investigations difficiles[198]. De manière analogue, les appareils photo et les caméscopes numériques modernes sont devenus les premiers outils de ***production*** de pédopornographie.

- La création d'un site web proposant des images à caractère pédopornographique permet de mettre ces ressources à disposition de toute personne qui a accès à Internet, au niveau mondial. Le nombre potentiel de consommateurs s'en trouve augmenté, en comparaison des approches basées sur les échanges physiques traditionnels de pédopornographie[199].

- La publication de contenus illégaux n'impose pas au responsable de cette publication d'utiliser des services d'hébergement qui se trouvent dans le pays depuis lequel il agit. Obtenir le retrait des contenus constitue dès lors un défi substantiel à relever, pour les services en charge de l'application de la loi.

Le débat relatif aux solutions

Le filtrage des services Internet qui sont utilisés à des fins d'échanges de ressources à caractère pédopornographique est en conséquence discuté comme étant une solution qui préviendrait l'utilisation de ces services à de telles fins[200]. Les raisons présidant à la mise en

---

[197] Concernant les différents types de contenus, voir supra, notre section 4.4.

[198] Krone, « A Typology of Online Child Pornography Offending » (« Une typologie des infractions liées à la pédopornographie en ligne »), Trends & Issues in Crime and Criminal Justice, n° 279 ; Cox, « Litigating Child Pornography and Obscenity Cases » (« Porter en justice les affaires de pédopornographie et d'obscénité »), Journal of Technology Law and Policy, vol. 4, fascicule (issue) 2, 1999, disponible à l'adresse : http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB ; Eneman, « A Critical Study of ISP Filtering of Child Pornography » (« Une étude critique du filtrage de la pédopornographie opéré par les FAI »), 2006, disponible à l'adresse : http://is2.lse.ac.uk/asp/aspecis/20060154.pdf ; Gercke, *Comprendre la cybercriminalité : Guide pour les pays en développement (Understanding Cybercrime: A Guide for Developing Countries)*, ITU, 2009, pages 32 et s., disponible en français à partir de l'adresse : http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[199] Gercke et Brunst, « Praxishandbuch Internetstrafrecht », 2009, ref. 259.

[200] Concernant le débat dans son ensemble, voir :: Lonardo, « Italy: Service Provider's Duty to Block Content » (« Italie : le devoir des prestataires de services de filtrer les contenus»), Computer Law Review International, 2007, pages 89 et s. ; Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008 ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008 ; Edwards et Griffith, « Internet Censorship and Mandatory Filtering » (« La censure d'Internet et le filtrage imposé »), NSW Parliamentary Library Resarch Service, nov. 2008 ; Zittrain et Edelman, « Documentation of Internet Filtering Worldwide » (« Présentation de l'état du filtrage d'Internet à travers le monde »), disponible à l'adresse : http://cyber.law.harvard.edu/filtering/ ; Reidenberg, « States and Internet Enforcement » (L'Etat et la régulation d'Internet »), University of Ottawa Law & Technology Journal, vol. 1, n° 213, 2004, pages 213 et s., disponible à l'adresse : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965 ; S'agissant de la discussion relative au filtrage dans différents pays, voir Taylor, « Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime » » (« Les prestataires de services Internet et leur responsabilité au regard des contenus dans le nouveau régime français »), Computer Law & Security

œuvre des technologies de filtrage sont donc ici les mêmes que celles qui justifient l'incrimination pénale de l'échange de ressources à caractère pédopornographique, à savoir la réduction du volume des crimes et délits et la protection des enfants. Dans le cadre du débat actuel relatif au filtrage, les discussions se concentrent énormément sur le filtrage de l'accès à des sites web. Plusieurs solutions techniques sont considérées, afin de prévenir l'accès des utilisateurs à des sites web contenant des ressources à caractère pédopornographique[201]. Nombre de ces approches sont basées sur l'utilisation de listes noires (« *block-lists* »), dans lesquelles sont listés les sites web connus pour présenter un caractère pédopornographique[202].

La pédopornographie relève de l'une des peu nombreuses catégories de contenus qui se trouvent largement pénalisés dans la plupart des pays[203]. A première vue, l'existence de sites web à caractère pédopornographique est dès lors surprenante – spécialement car l'existence de listes noires souligne le fait que ces sites web ont déjà attiré l'attention des services en charge de l'application de la loi.

Il existe quatre raisons, à la difficulté d'obtenir le retrait des contenus.

L'absence d'autorité centrale

Internet est basé sur un concept de décentralisation[204]. A la différence des réseaux centralisés, Internet connaît peu d'institutions de contrôle central[205]. Ces institutions, qui existent, telles que l'Internet Corporation for Assigned Names and Numbers (ICANN, l'organisme central de nommage Internet), ont des pouvoirs très limités lorsqu'il s'agit de

---

Report, vol. 20, fascicule (issue) 4, 2004, pages 268 et s. ; « Belgium ISP Ordered By The Court To Filter Illicit Content » (« Les prestataires d'accès à Internet contraints par une juridiction de filtrer les contenus illicites »), EDRI News, No 5.14, 18 juin 2007, disponible à l'adresse : http://www.edri.org/edrigram/number5.14/belgium-isp ; Enser, « Illegal Downloads: Belgian court orders ISP to filter » (« Téléchargements illégaux : une juridiction Belge impose le filtrage aux FAI »), OLSWANG E-Commerce Update, nov. 2007, page 7, disponible à l'adresse : http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf ; Standford, « France to Require Internet Service Providers to Filter Infringing Music » (« La France demande aux fournisseurs d'accès à Internet de filtrer la musique contrefaite »), 27 nov. 2007, Intellectual Property Watch, disponible à l'adresse : http://www.ip-watch.org/weblog/index.php?p=842 ; Zwenne, « Dutch Telecoms wants to force Internet safety requirements » (« Le régulateur des télécommunications néerlandais veut imposer des règles de sécurité sur Internet »), Wold Data Protection Report, fascicule (issue) 09/07, page 17, disponible à l'URL : http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf ; Le document de L'IFPI de 2007 concernant les options techniques permettant de lutter contre les violations du droit d'auteur en ligne (Technical options for addressing online copyright infringement), disponible en anglais à l'adresse : http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf ; S'agissant des approches d'autorégulation, voir « ISPA Code Review : Self-Regulation of Internet Service Providers » (« Examen du Code de l'association des prestataires de services Internet : auto-régulation des prestataires de services Internet »), 2002, disponible à l'adresse : http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf ; Zittrain, Harvard Journal of Law & Technology, 2006, vol. 19, n° 2, pages 253 et s.

[201] Voir infra, sous-section 5.3.2.

[202] Voir infra, sous-section 5.2.1.

[203] Akdeniz, in Edwards et Waelde, « Law and the Internet: Regulating Cyberspace » (« La loi et Internet : réguler le cyberespace ») ; Williams, in Miller, « Encyclopaedia of Criminology » (« Encyclopédie de criminologie »), page 7. Concernant l'étendue de sa pénalisation, voir : *Child Pornography: Model Legislation & Global Review (Pédopornographie : législation modèle et bilan mondial)*, 2006, disponible à l'adresse : http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. S'agissant de la discussion relative à la pénalisation de la pédopornographie et à la liberté d'expression aux Etats-Unis, voir : Burke, « Thinking Outside the Box: Child Pornography, Obscenity and the Constitution » (« Penser différemment : la pédopornographie, l'obscénité et la Constitution »), Virginia Journal of Law and Technology, vol. 8, 2003, disponible à l'adresse : http://www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf. Sieber, « Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet ». Cette dernière publication compare diverses lois nationales sur le sujet de la pénalisation de la pédopornographie.

[204] Pour un bref aperçu de l'histoire d'Internet, incluant ses origines militaires, voir Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, Wolff, « A Brief History of the Internet » (« L'histoire d'Internet en bref »), disponible à l'adresse : http://www.isoc.org/internet/history/brief.shtml.

[205] S'agissant des défis y relatifs rencontrés dans le cadre des investigations en matière de cybercriminalité, de manière générale, voir Gercke, *Comprendre la cybercriminalité : Guide pour les pays en développement (Understanding Cybercrime: A Guide for Developing Countries)*, ITU, 2009, pages 38 et s., disponible en français à partir de l'adresse : http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

prendre des mesures contre des contenus illégaux, échanges de ressources à caractère pédopornographique via des services Internet inclus.

Souveraineté nationale

Le principe de souveraineté nationale[206] limite la possibilité, pour les services en charge de l'application de la loi, de réagir directement et d'ordonner le retrait des sites web à caractère pédopornographique, si ces derniers sont physiquement hébergés hors du territoire[207]. Dans une telle situation, les services en charge de l'application de la loi doivent débuter une investigation et faire usage des instruments de coopération internationale, afin d'initier le processus de retrait de ces contenus. En raison de ses exigences de forme, la coopération internationale peut être un processus très consommateur de temps[208]. Les tentatives de filtrage visant à prévenir les accès aux sites web à caractère pédopornographique qui ne peuvent pas être retirés en un laps de temps opportun constituent dès lors une **réponse aux difficultés posées par la coopération internationale**.

Dans le cadre du débat sur le filtrage, des tests ont été entrepris aux fins de démontrer que le filtrage d'Internet n'est pas requis, puisque les contenus qu'il vise pourraient, alternativement, être aisément retirés. Après que le contenu de listes noires ait été divulgué, différentes initiatives ont eu pour but de contacter les prestataires d'hébergement dont les services étaient utilisés pour stocker des sites à caractère pédopornographique, afin d'obtenir le retrait de ces contenus illégaux. Dans un grand nombre de cas, le contenu fut retiré immédiatement.

Bien que cet exemple mette en évidence la possibilité d'améliorer les procédures de retrait, afin de les rendre plus appropriées (notamment, un traitement plus rapide des notifications provenant de pays de confiance pourrait aider), **il ne démontre pas en lui-même qu'il existe des moyens plus rapides** de retirer les contenus, qui rendraient les tentatives de filtrage non nécessaires. A la différence des experts privés ou des groupes de défense des libertés publiques, les services en charge de l'application de la loi n'ont généralement pas la permission de contacter directement les entreprises situées en dehors de leur territoire dans l'objectif d'obtenir le retrait de contenus illégaux. Le principe de souveraineté nationale[209] leur interdit de telles approches directes. En outre, de telles interventions non coordonnées pourraient interférer avec des investigations en cours.

---

[206] La souveraineté nationale est principe fondamental du droit international. Voir Martinez, National Sovereignty and International Organizations (Souveraineté nationale et organisations internationales), 1996 ; Sieghart, The International Law of Human Rights (Le droit international des droits de l'Homme), 1984, pages 11 et s. ; Roth, « State Sovereignty, International Legality, and Moral Disagreement » (« Souveraineté de l'Etat, légalité internationale et désagrément moral »), 2005, page 1, disponible à l'adresse : http://www.law.uga.edu/intl/roth.pdf.

[207] Gercke, Comprendre la cybercriminalité : Guide pour les pays en développement (Understanding Cybercrime: A Guide for Developing Countries), ITU, 2009, pages 38 et s., disponible en français à partir de l'adresse : http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[208] Le besoin d'intensifier le processus de coopération internationale est signalé dans le rapport explicatif sur la Convention sur la cybercriminalité. Voir le rapport explicatif sur la Convention sur la cybercriminalité, n° 256 : « *Les données informatiques sont très volatiles. Il suffit de presser sur quelques touches ou d'utiliser un programme automatique pour les effacer, ce qui rend impossible de remonter jusqu'à l'auteur d'une infraction ou détruit les preuves de sa culpabilité. Certains types de données ne sont stockés que pour de courtes périodes avant d'être détruites. Dans d'autres cas, si des preuves ne sont pas recueillies rapidement, des personnes ou des biens peuvent subir un préjudice important. Dans des situations aussi urgentes, la demande comme la réponse doivent être rapides. L'objet du paragraphe 3 consiste donc à faciliter l'accélération du processus visant à garantir l'entraide pour éviter que des informations ou des preuves essentielles ne soient perdues parce qu'elles auraient été effacées avant qu'une demande d'entraide n'ait pu être préparée et transmise et qu'une réponse n'ait pu être reçue* ».

[209] La souveraineté nationale est un principe fondamental du droit international. Voir Martinez, National Sovereignty and International Organizations (Souveraineté nationale et organisations internationales), 1996 ; Sieghart, The International Law of Human Rights (Le droit international des droits de l'Homme), 1984, pages 11 et s. ; Roth, « State Sovereignty, International Legality, and Moral Disagreement » (« Souveraineté de l'Etat, légalité internationale et désagrément moral »), 2005, page 1, disponible à l'adresse : http://www.law.uga.edu/intl/roth.pdf.

Degré d'appréhension par les lois pénales

Malgré un consensus global sur le fait que la pédopornographie est illégale, la manière dont cette dernière est appréhendée par la loi pénale peut différer de manière significative selon les pays. Alors que certains d'entre eux pénalisent la pédopornographie réelle comme la pédopornographie virtuelle[210], d'autres limitent les incriminations aux contenus qui font état de l'abus réel d'un enfant. Certains pays considèrent la victime comme étant un enfant dès lors qu'elle répond à certains critères utilisés pour identifier la qualité de mineur, tandis que d'autres pays requièrent l'identification de la victime pour poursuivre l'auteur de l'infraction. Ces différences locales peuvent sérieusement entraver les initiatives de retrait des contenus, dans le cadre des enquêtes internationales.

Incitation légale

Les services en charge de l'application de la loi auraient maintenu des sites web à caractère pédopornographique pour les utiliser en tant que ce qu'il est convenu d'appeler des « pots de miel », attirant les suspects qui essaient de télécharger des ressources à caractère pédopornographique (généralement, les images sont corrompues ou non réellement illégales, ce qui n'est découvert par l'utilisateur que lorsqu'il s'est enregistré sur un site web faisant la promotion de contenus à caractère pédopornographique).

Les difficultés à obtenir le retrait des contenus illégaux hébergés en dehors du pays renforcent la demande croissante de solutions techniques qui tenteraient de prévenir l'accès à ces ressources pendant le processus, long et pas toujours fructueux, de retrait du contenu à sa source. Les tendances en faveur du stockage décentralisé (« stockage hébergé » - « *cloud storage* ») vont très probablement accroître la difficulté de retirer à temps les contenus, puisque l'importance de la localisation physique du contenu y décroît[211].

[210] S'agissant de la pénalisation de la pédopornographie virtuelle, voir Gercke, Comprendre la cybercriminalité : Guide pour les pays en développement (Understanding Cybercrime: A Guide for Developing Countries), ITU, 2009, page 134 et s., disponible en français à partir de l'adresse : http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[211] Concernant les problématiques de ressort dans les affaires d' « informatique dans les nuages » (« *cloud computing* »), voir Velasco San Martin, « Jurisdictional Aspects of Cloud Computing » (« Aspects juridictionnels de l' "informatique dans les nuages" »), 2009, disponible à l'adresse : http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf.

4.6.2 Le consommateur – l'utilisateur d'Internet

Cadre

En plus de prohiber la production, la publication et la mise à disposition de pédopornographie, un nombre significatif de pays érigent en infraction pénale la possession de pédopornographie[212]. La demande de tels contenus pourrait favoriser leur production de manière suivie[213]. En outre, la possession de telles ressources pourrait encourager les abus sexuels sur enfants. En conséquence, les responsables politiques suggèrent qu'un moyen efficace de réduire la production de pédopornographie est de rendre illégale la ***possession*** de ressources de cette nature[214]. Un exemple en est l'article 9 de la Convention sur la cybercriminalité. Toutefois, cette Convention permet aux Etats parties, au paragraphe 4 du même article, de ne pas rendre punissable la simple possession, et de n'ériger en infraction pénale que la production, l'offre et la distribution de pédopornographie[215].

Par ailleurs, un certain nombre de pays vont au delà de l'incrimination de la possession de ressources à caractère pédopornographique, en prohibant l'action ***d'accéder*** à de telles ressources. Par exemple, l'article 20, paragraphe 1, f, de la Convention du Conseil de l'Europe sur la protection des enfants, suggère d'ériger en infraction pénale le fait d'accéder à de la pédopornographie par le biais d'un ordinateur. Cette incrimination permet aux services en charge de l'application de la loi de poursuivre des suspects lorsqu'elles peuvent démontrer que ces derniers ont visualisé des sites web à caractère pédopornographique, mais qu'elles ne peuvent démontrer qu'ils ont téléchargé des ressources de cette nature. De telles difficultés à collecter des preuves peuvent par exemple survenir lorsque le suspect utilise une technologie de chiffrement pour protéger, sur son matériel de stockage, les fichiers qu'il a téléchargés[216]. Le rapport explicatif sur la Convention sur la protection des enfants indique que cette disposition doit également s'appliquer aux cas dans lesquels une personne ne fait que regarder en ligne des images à caractère pédopornographique, sans télécharger ces images[217]. En général, l'ouverture d'un site web initie automatiquement un processus de téléchargement – souvent sans que l'utilisateur n'en soit conscient[218]. Le cas mentionné dans le rapport explicatif ne correspond donc qu'aux situations dans lesquelles un téléchargement n'a pas lieu en arrière plan.

---

[212] S'agissant de l'incrimination de la possession de pédopornographie en Australie, voir : Krone, « Does thinking make it so? Defining online child pornography possession offences » (« Est-ce que le penser revient à le faire ? Définir les infractions en ligne de possession de pédopornographie ») in *Trends & Issues in Crime and Criminal Justice*, n° 299 ; Sieber, « Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet ». Cet article compare diverses lois nationales en ce qui concerne les infractions liées à la pédopornographie.

[213] Voir : *Child Pornography: Model Legislation & Global Review (Pédopornographie : législation modèle et bilan mondial)*, 2006, page 2, disponible à l'adresse : http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[214] Rapport explicatif sur la Convention sur la cybercriminalité du Conseil de l'Europe, n° 98.

[215] Gercke, *Cybercrime Training for Judges (Formation à la cybercriminalité pour les juges)*, 2009, page 45, disponible à l'URL : http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[216] S'agissant des défis posés par l'utilisation de technologies de chiffrement, voir infra, chapitre 5. Une étude concernant la pédopornographie semblait indiquer que seuls 6 pour cent des possesseurs de pédopornographie arrêtés utilisaient des technologies de chiffrement. Voir Wolak, Finkelhor et Mitchell, *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study (Des possesseurs de pédopornographie arrêtés pour des infractions en relation avec Internet : conclusions de l'étude nationale sur la victimisation des enfants en ligne)*, 2005, page 9, disponible à l'adresse : http://www.missingkids.com/en_US/publications/NC144.pdf.

[217] Voir le rapport explicatif sur la Convention sur la protection des enfants, n° 140.

[218] Le téléchargement est généralement nécessaire pour permettre l'affichage de l'information que propose le site web. Selon la configuration du navigateur, l'information peut être téléchargée dans des dossiers caches et temporaires, ou peut être simplement stockée dans la mémoire vive de l'ordinateur. Concernant les aspects de l'investigation informatique légale liés à ce téléchargement, voir Nolan, O'Sullivan, Branson et Waits, *First Responders Guide to Computer Forensics (Guide de l'investigation numérique pour les personne en charge des premières réponses)*, 2005, page 180, disponible à l'adresse : http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

Diligenter des investigations dans de telles situations va de pair avec plusieurs difficultés :

- Très souvent, les données nécessaires à l'identification d'une connexion qui a été utilisée pour télécharger des ressources à caractère pédopornographique sont rapidement supprimées. C'est spécialement le cas des adresses IP. La mise en place d'obligations en termes de conservation des données (par exemple par la Directive de l'Union européenne sur la conservation des données[219]) ne résout que partiellement ce problème[220].
- La disponibilité de services de communication anonyme permet aux personnes de masquer leur identité, ce qui rend plus difficiles les investigations, pour les services en charge de l'application de la loi.

[219] 2005/0182/COD.

[220] Le fait que la Directive devait couvrir les informations clefs relatives à toute communication sur Internet a conduit à d'intenses critiques de la part des organisations de défense des droits de l'Homme (voir par exemple : « Briefing for the Members of the European Parliament on Data Retention » (« Instructions pour les membres du Parlement européen sur la conservation des données »), disponible à l'adresse : http://www.edri.org/docs/retentionletterformeps.pdf ; CMBA, « Position on Data retention: GILC, Opposition to data retention continues to grow » (« Position sur la conservation des données : GILC, l'opposition à la conservation des données continue de s'accroître »), disponible à l'adresse : http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf ; S'agissant de la question relative à une violation de la Convention européenne des droits de l'Homme, voir Breyer, « Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR » (« La conservation des données relatives aux télécommunications et les droits de l'Homme : la compatibilité de la conservation généralisée des données de trafic avec la CEDH »), European Law Journal, 2005, pages 365 et s.

4.6.3 Résumé

Le filtrage de contenus Internet illégaux peut être vu non seulement comme un instrument dirigé contre les personnes qui sont responsables de la mise en ligne de ces contenus (les producteurs), mais également comme un outil visant à empêcher les utilisateurs de télécharger des contenus illégaux (les consommateurs).

Alors même que le filtrage d'Internet ne permet *pas* de retirer les contenus à leur source et que cette circonstance fait obstacle à la possibilité, pour la mesure, de prévenir les infractions de mise en ligne de tels contenus, cette même mesure, lorsqu'elle est techniquement efficace, a le **potentiel de prévenir les infractions commises par les utilisateurs, qui tentent d'accéder à un site web, soit pour visualiser, soit pour télécharger, un contenu à caractère pédopornographique**. Le succès de cette prévention dépend de l'efficacité des technologies de filtrage mises en place et du niveau de motivation et de connaissances de l'utilisateur.

S'agissant de l'intention de rendre les contenus indisponibles pour les utilisateurs, les arguments principaux qui s'opposent au filtrage sont l'absence de retrait du contenu à sa source et la possibilité de contourner la mesure. Ces aspects ont différentes conséquences :

- Le contenu est toujours accessible par l'intermédiaire d'une connexion qui n'est pas soumise à la mesure de filtrage. Cette situation permet aux utilisateurs d'autres pays, qui n'ont pas imposé le filtrage, d'accéder aux services qui sont utilisés pour distribuer des ressources à caractère pédopornographique. Ces services peuvent même rester disponibles dans les pays qui requièrent généralement leur filtrage, puisque, dans ces pays, les obligations de mettre en place des technologies de filtrage ne s'appliquent souvent qu'aux prestataires de services qui ont un certain nombre de clients. Un exemple en est la section 2 de la loi allemande qui pose des obligations de filtrage à la charge des seuls fournisseurs d'accès à Internet qui ont un minimum de 10 000 clients[221]. En outre, les diverses technologies connaissent des degrés différents d'efficacité, ce qui implique que certains utilisateurs puissent contourner sans le savoir les systèmes de filtrage les plus simples ;
- Dès lors que les technologies de filtrage sont développées et mises en œuvre, elles peuvent être utilisées dans d'autres objectifs. La raison principale de cette inquiétude est l'absence de transparence qui entoure la mise en œuvre de ce type de technologies ;
- Le fait que le contenu ne soit pas supprimé permet aux utilisateurs de rechercher la manière d'y accéder en contournant les solutions techniques de protection ;
- Il existe plusieurs manières de contourner les mesures de filtrage qui ont été jusqu'à présent discutées. L'utilisation de services de communication anonyme, ou de liens sécurisés par chiffrement qui utilisent une connexion https, permet déjà de contourner certains des instruments de contrôle actuellement en discussion. Des instructions détaillant la manière de contourner les différentes mesures de filtrage furent fréquemment publiées dans le cadre des débats nationaux relatifs au filtrage ;
- Le fait que les contenus ne soient pas supprimés suggère à l'utilisateur qu'il s'agit de sites web auxquels il peut accéder avec confiance, puisque les autorités ont clairement

[221] Loi allemande sur la complication de l'accès à des contenus pédopornographiques sur les réseaux de communication (Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen / Zugangserschwerungsgesetz – ZugErschwG) - § 2 (1) : « *(1)Diensteanbieter nach § 8 des Telemediengesetzes, die den Zugang zur Nutzung von Informationen über ein Kommunikationsnetz fur mindestens 10 000 Teilnehmer oder sonstige Nutzungsberechtigte ermöglichen, haben geeignete und zumutbare technische Maßnahmen zu ergreifen, um den Zugang zu Telemedienangeboten, die in der Sperrliste aufgefuhrt sind, zu erschweren* ».

échoué dans leurs tentatives de les faire supprimer et de diligenter des investigations à leur sujet ;

- Les sites web sont seulement l'un des services utilisés pour échanger des ressources à caractère pédopornographique. Les récentes approches techniques se concentrent énormément sur les services web. Les échanges de ressources à caractère pédopornographique par l'intermédiaire de systèmes de partage de fichiers ou de messages électroniques chiffrés ne sont pas couverts par ces approches.

4.7 Conclusions

- Il est vraisemblable que dans la situation actuelle, un laps de temps soit maintenu entre le moment de l'identification d'un contenu illégal et le moment du retrait de ce contenu des serveurs qui l'hébergent. Si des initiatives de filtrage pouvaient être mises en place en sorte de fonctionner techniquement de manière effective et efficace, elles constitueraient dès lors une approche possible pour prendre en charge cette difficulté, sous réserve de leur proportionnalité.

- Au regard du fait que le filtrage ne conduit pas au retrait du contenu, **le filtrage ne peut pas être considéré comme un instrument pemettant de prévenir l'acte de mise à disposition de contenus illégaux** en ligne, mais il s'agit d'une solution technique possible pour prévenir les utilisateurs de commettre (accidentellement) un acte litigieux en accédant à un site web à caractère pédopornographique.

- Les **approches actuelles concernant le filtrage ne se préoccupent que des services web**. Les autres services ne sont pas inclus. Les difficultés pourraient ne pas résulter que des approches actuelles, mais également d'un accroissement de l'utilisation de services d'hébergement anonyme par l'intermédiaire de réseaux tels que TOR (« *The Onion Router* »). Si l'objectif du système de filtrage est de filtrer les délinquants chevronnés, ce système n'est pas suffisant et deviendra vraisemblablement, dans le futur, encore moins efficace.

- Le filtrage n'est pas la seule solution qui permette de réduire le laps de temps qui s'écoule entre l'identification d'un contenu illégal hébergé à l'étranger et le retrait de celui-ci de son serveur d'hébergement. Une autre approche, en vue de réduire ce laps de temps, pourrait consister en **l'amélioration des moyens alloués à la coopération internationale.**

- Le fait que les instruments de filtrage actuellement en discussion soient aisément contournables fait ressortir le caractère insuffisant de ces instruments, dans le cadre d'une approche destinée à empêcher les délinquants chevronnés d'avoir accès aux ressources illégales. Cette situation conduit à une conclusion principale, qui est que **le filtrage d'un contenu ne peut pas se substituer au retrait de ce même contenu** de son serveur d'hébergement, puisque seul ce retrait peut empêcher les délinquants chevronnés d'y avoir accès. En conséquence, la cible principale de ces technologies ne peut pas être ces derniers individus, mais les personnes qui sont moins expérimentées en matière de contournement de technologies de filtrage. L'un des objectifs vraisemblables de ces technologies est donc de **prévenir les accès accidentels** à de tels contenus.

- Dans le cadre des discussions relatives au filtrage ayant pour but de prévenir les accès non intentionnels, l'une des problématiques soulevées est que le fait que les contenus visés par la mesure **ne soient plus visibles pourrait dévoyer le débat politique**, puisqu'il pourrait donner l'impression que le problème de la pédopornographie en ligne a été résolu.

- Le fait de filtrer avec succès des ressources à caractère pédopornographique ne permet ni d'identifier les victimes figurant dans ces ressources, ni de retirer ces victimes de la situation abusive où elles se trouvent. Des investigations doivent se charger des images en cause afin d'assurer que ces deux étapes soient menées avec succès. Le filtrage réussi de telles images, lorsque ces dernières montrent des victimes qui ont déjà été identifiées et qui se trouvent sous soins ou sur le chemin de la récupération, pourrait prévenir une nouvelle victimisation de ces victimes.

- Outre les limites systémiques, mentionnées ci-dessus, des approches relatives au filtrage, des problématiques techniques et juridiques doivent être prises en considération.

4.8 Exemples de pays

Plusieurs pays européens tels que la Finlande, la Norvège[222], la Suède[223], la Suisse[224], le Royaume-Uni[225] et l'Italie[226], de même que des pays non européens tels que l'Australie[227], la Chine[228], l'Iran[229] et la Thaïlande[230], pratiquent le filtrage d'Internet. Les approches techniques, l'objectif du filtrage, de même que le degré de participation de l'industrie à l'opération, y sont variables.

En Australie, par exemple, une liste noire (« *block-list* ») générée par l'Autorité australienne des communications et des médias (ACMA) devra vraisemblablement être utilisée obligatoirement par tous les prestataires d'accès à Internet[231]. Actuellement, des tests sont en cours auprès de certains FAI. Telstra, le fournisseur d'accès à Internet le plus important d'Australie, a annoncé qu'il ne se joindrait pas aux essais de filtrage[232].

---

[222] « Telenor Norge: TelAuenor and KRIPOS introduce Internet child pornography Filter » (« Telenor Norvège : TelAuenor et KRIPOS introduisent le filtrage de la pédopornographie sur Internet », Telenor Press Release, 21 sept. 2004 ; Clayton, « Failures in a Hybrid Content Blocking System » (« Pannes dans un système hybride de filtrage des contenus »), in *Privacy Enhancing Technologies*, 2006, page 79 ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008, pages 46 et s. ; Comité de la Convention sur la cybercriminalité (T-CY), *Examples of how the private sector has blocked child pornographic sites (exemples des méthodes utilisées par le secteur privé pour bloquer des sites à caractère pédopornographique)*, T-CY (2006) 04, page 3.

[223] Les prestataires suédois utilisent un outil appelé « Netclean ». Voir Netclean Pro Active, disponible à l'adresse : http://www.netclean.com/documents/NetClean_ProActive_Information_Sheet_EN.pdf ; « Telenor and Swedish National Criminal Investigation Department to introduce Internet child porn filter » (« Telenor et le Département national suédois des enquêtes criminelles introduisent le filtrage de la pédopornographie »), Telenor Press Release, 17 mai 2005, disponible à l'adresse : http://press.telenor.com/PR/200505/994781_5.html ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, « Filteren van kinderporno op internet », 2008, pages 59 et s. ; Comité de la Convention sur la cybercriminalité (T-CY), *Examples of how the private sector has blocked child pornographic sites (exemples des méthodes utilisées par le secteur privé pour bloquer des sites à caractère pédopornographique)*, T-CY (2006) 04, page 3 ; Edwards et Griffith, « Internet Censorship and Mandatory Filtering » (« Censure d'Internet et filtrage imposé »), NSW Parliamentary Library Resarch Service, nov. 2008, page 6.

[224] Sieber et Nolde, « Sperrverfuegungen im Internet », 2008, page 55 ; Schwarzenegger, « Sperrverfuegungen gegen Access-Provider », in Arter et Joerg, *Internet-Recht und Electronic Commerce Law*, page 250.

[225] Edwards et Griffith, « Internet Censorship and Mandatory Filtering » (« Censure d'Internet et filtrage imposé »), NSW Parliamentary Library Resarch Service, nov. 2008, page 4 ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008, pages 64 et s. ; Comité de la Convention sur la cybercriminalité (T-CY), *Examples of how the private sector has blocked child pornographic sites (exemples des méthodes utilisées par le secteur privé pour bloquer des sites à caractère pédopornographique)*, T-CY (2006) 04, page 3 ; Eneman, « A Critical Study of ISP Filtering of Child Pornography » (« Une étude critique du filtrage de la pédopornographie opéré par les FAI »), 2006, disponible à l'adresse : http://is2.lse.ac.uk/asp/aspecis/20060154.pdf.

[226] Lonardo, « Italy: Service Provider's Duty to Block Content » (« Italie : le devoir des prestataires de services de filtrer les contenus »), Computer Law Review International, 2007, pages 89 et s. ; Edwards etGriffith, « Internet Censorship and Mandatory Filtering » (« Censure d'Internet et filtrage imposé »), NSW Parliamentary Library Resarch Service, nov. 2008, pages 6 et s. ; Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008, page 54.

[227] Concernant les approches relatives au filtrage, voir : *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety* (*Développements relatifs aux technologies de filtrage d'Internet et autres mesures pour promouvoir la sécurité sur Internet*), ACMA, 2008.

[228] Clayton, Murdoch et Watson, « Ignoring the Great Firewall of China » (« Passer outre le grand pare-feu de la Chine »), disponible à l'adresse : http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf ; Pfitzmann, Koepsell et Kriegelstein, « Sperrverfuegungen gegen Access-Provider », Technisches Gutachten, disponible à l'adresse : http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf ; Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008, page 53 ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008, page 73.

[229] Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008, page 53 ; Stol, Kaspersen, Kerstens, Leukfeldt et Lodder, *Filteren van kinderporno op internet*, 2008, page 73.

[230] Sieber et Nolde, *Sperrverfuegungen im Internet*, 2008, page 55.

[231] Concernant les approches relatives au filtrage, voir : *Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety* (*Développements relatifs aux technologies de filtrage d'Internet et autres mesures pour promouvoir la sécurité sur Internet*), ACMA, 2008.

[232] http://www.itu.int/osg/blog/2008/12/12/NetFirmsRebuffFilteringPlan.aspx.

Au royaume-Uni, la liste noire est générée par l'IWF (Internet Watch Foundation)[233]. La technologie utilisée est BT Cleanfeed[234]. Au Danemark, la liste noire est générée par le Centre national de lutte contre la criminalité liée aux nouvelles technologies (« *National High Tech Crime Centre* ») de la police nationale danoise, et par le service d'assistance « Save the Children Denmark » [235]. Les trois FAI les plus importants y participent. En Finlande, le filtrage était initialement basé sur une liste de domaines fournie par la police finlandaise. La plupart des FAI participent aujourd'hui à l'opération, sur la base d'un blocage DNS[236].

[233] Stol, Kaspersen, Kerstens, Leukfeldt et Lobber, « Governmental filtering of websites: The Dutch case » (« Le filtrage gouvernemental des sites web : le cas néerlandais »), Computer Law & Security Review 2009, page 251.

[234] Pfitzmann, Koepsell et Kriegelstein, « Sperrverfuegungen gegen Access-Provider », *Technisches Gutachten*, page 55, http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

[235] Concernant le filtrage au Danemark, voir : York, « Secret Censorship in Denmark » (« Censure secrète au Danemark »), 2008, disponible à l'adresse : http://opennet.net/blog/2008/12/secret-censorship-denmark.

[236] Ricknäs, « Europe makes moves towards Internet censorship » (« L'Europe en marche vers la censure d'Internet »), 2008, disponible à l'adresse : http://www.infoworld.com/d/security-central/europe-makes-moves-toward-internet-censorship-622.

Chapitre 5 LES ASPECTS TECHNIQUES DU FILTRAGE D'INTERNET

5.1 Introduction

Le développement et la mise en œuvre de différentes technologies de filtrage, sur Internet, sont loin d'être une nouveauté. Le spam, les virus et logiciels malveillants provenant d'Internet, à l'instar de nombreux autres contenus qui ne sont ni souhaités, ni sollicités par les utilisateurs finaux, sont devenus la cible des efforts de filtrage entrepris par l'industrie, pour des raisons de sécurité et d'utilisabilité, ou par l'Etat, dans le cadre de son rôle d'élaboration et de mise en application des lois et politiques.

Initialement, la pression en faveur du filtrage vint principalement des utilisateurs et de l'industrie. L'implication de l'Etat était, au départ, limitée aux affaires judiciaires concernant des cas de filtrage injustifié ou excessif. Un excellent exemple en est l'affaire Spamhaus contre e360, dans laquelle une société américaine a assigné Spamhaus devant la justice civile américaine, son objectif étant apparemment de déstabiliser Spamhaus dans la guerre qui opposait les deux parties sur le spam[237].

Ces dernières années, les Etats démocratiques ont promu l'usage de technologies de filtrage d'Internet dans différents domaines. Ils ont invoqué l'intérêt général pour requérir la mise en œuvre de certaines mesures de filtrage, en vue d'assurer le respect de divers aspects de leur politique publique, dans un contexte où les caractéristiques d'Internet rendaient l'application de la loi difficile (au niveau international). Les contenus visés sont variés et concernent tant la disponibilité d'objets nazis sur des sites de vente en ligne[238], que l'hébergement de sites de jeux d'argent dans des Etats dont les législations sont libérales sur la question[239]. De manière analogue, certains Etats, au régime moins ouvert sur l'information, utilisent le filtrage comme une ressource technique qui leur permet d'étendre leur pratique du contrôle de l'information aux médias électroniques.

---

[237] Voir « Spamhaus *[Une liste noire Internet destinée au filtrage du spam, ndlr]* fined $11.7 million; won't pay a dime » (« Spamhaus condamné à payer 11,7 millions de dollars : il ne payera pas un centime », Nate Anderson, Ars Technica, http://arstechnica.com/business/news/2006/09/7757.ars ; La décision de la Cour rendue par défaut est consultable à cette adresse : http://www.spamhaus.org/archive/legal/Kocoras_order_to_Spamhaus.pdf ; e360 Insight, le plaignant, a plus tard déposé le bilan et a invoqué d'énormes frais de justice comme ayant été un facteur contribuant.

[238] Affaire Yahoo (France), voir « Yahoo hits back at Nazi ruling » (« Yahoo riposte à la décision Nazi ») http://news.bbc.co.uk/2/hi/europe/1032605.stm et « Yahoo! loses! Nazi! lawsuit! » (« Yahoo! perd! le procès! nazi! »), http://www.theregister.co.uk/2006/01/13/nazi_yahoo_defeat/.

[239] *De Lotto* (le seul à être autorisé en droit néerlandais à opérer un site web de jeux d'argent en ligne) *c/ LadBrokes* (un site web britannique de paris en ligne). La Haute Cour de justice néerlandaise considéra qu'en permettant aux utilisateurs néerlandais de parier en ligne sur son site web basé au Royaume-Uni, LadBrokes était contrevenu aux dispositions de la loi néerlandaise sur les jeux de hasard. Elle lui a ordonné de bloquer l'accès des citoyens néerlandais à ce site. Voir (en néerlandais) la décision préliminaire de la haute Cour : http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AR4841&u_ljn=AR4841. Dans l'affaire principale qui est en cours entre les mêmes parties, la Haute Cour a posé des questions préjudicielles à la Cour de justice des communautés européennes (CJCE). Voir (en néerlandais) : http://www.rechtspraak.nl/Actualiteiten/Hoge+Raad+stelt+vragen+van+uitleg+aan+HvJEG+over+kansspelzaak+Ladbrokes.htm. Parmi les autres affaires de ce type, nous pouvons citer le procès diligenté contre Unibet, un autre site web de jeux d'argent basé au Royaume-Uni. Voir en anglais, sur l'affaire préliminaire : « Dutch Supreme Court rules on Ladbrokes appeal » (« Décision de la Cour suprême néerlandaise sur le procès en appel de Ladbrokes », à l'adresse : http://www.droit-technologie.org/actuality/details.asp?id=836.

La dernière étape de ces développements fut récemment franchie lorsqu'un certain nombre de pays occidentaux, démocratiques, commencèrent à tenter de limiter l'accessibilité de la pédopornographie en ligne. Parallèlement, les limitations de l'accès à l'information en ligne ont connu de nouveaux sommets dans de nombreux pays, dans le cadre de périodes d'agitation sociale (révolution Twitter des Moldaves) ou de révolution (révolution Internet iranienne) [240].

Tous ces développements s'articulent autour de la disponibilité de technologies de filtrage d'Internet. Ces technologies sont utilisables sur différents protocoles/services (méthodes de distribution de contenus) et peuvent être mises en œuvre à différents niveaux du réseau Internet, de même qu'au niveau des équipements de l'utilisateur final (c'est-à-dire au domicile ou au bureau). En fonction de leurs caractéristiques techniques, ces technologies peuvent s'avérer plus ou moins efficaces ou contournables. Le présent chapitre se propose de décrire les technologies de filtrage qui sont utilisées dans le cadre de la plupart des initiatives de filtrage, et d'engager une discussion sur l'implication de ces technologies, d'un point de vue démocratique.

Le présent chapitre se concentrera principalement sur les techniques qui permettent actuellement de filtrer les ressources à caractère pédopornographique, le principal sujet de ce rapport. Cependant, il est important de noter qu'un grand nombre de ces techniques peuvent être utilisées pour filtrer d'autres types de contenus ou d'activités, sans investissements supplémentaires significatifs. Ce chapitre explorera enfin les implications (démocratiques) de chacune des techniques disponibles, avant d'en arriver à un certain nombre de conclusions provisoires.

[240] Voir « The Moldovan Twitter revolution » (« La révolution Twitter moldave »), disponible à l'adresse : http://statismwatch.ca/2009/04/07/protests-in-moldova-explode-with-help-of-twitter/ et http://neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution. S'agissant des évènements qui ont suivi l'élection présidentielle iranienne de 2009, voir : http://english.aljazeera.net/programmes/rizkhan/2009/06/200962281940160238.html et http://cosmiclog.msnbc.msn.com/archive/2009/06/18/1970353.aspx.

5.2 Les stratégies techniques de filtrage

Il existe différentes stratégies de filtrage des contenus électroniques, qui autorisent chacune l'utilisation de plusieurs méthodes de filtrage, et qui connaissent chacune des degrés différents d'efficacité. La présente étude se concentrera sur le filtrage de la pédopornographie et proposera un panorama modérément détaillé des possibilités et des stratégies techniques qui permettent de filtrer les contenus à différents niveaux du réseau, à l'aide de diverses technologies.

5.2.1 L'identification du contenu

La mise en œuvre d'une décision de filtrage requiert la présence d'identificateurs de contenus. Certains de ces identificateurs étant très communs et abordés plus loin dans le présent chapitre, ils font chacun, ci-dessous, l'objet d'une description technique.

Les contenus sur lesquels se concentre le présent rapport sont généralement de nature visuelle. Autrement dit, ils contiennent soit des images, soit des séquences vidéo d'abus sexuels sur enfants.

5.2.1.1 Les adresses IP

L'adresse Internet Procotol, ou IP, est l'identificateur le plus basique d'une machine connectée à Internet. Tout ordinateur connecté directement au réseau, qu'il s'agisse d'un ordinateur individuel, d'une passerelle résidentielle (« *residential gateway* ») ou d'un serveur web utilisé pour afficher les sites web, est identifié grâce à son adresse IP. Dans la mesure où les adresses IP sont gérées et allouées de manière centralisée (sous la tutelle de l'ICANN), chaque adresse IP est unique (à l'exception de certaines plages d'adresses réservées à un usage privé).

Une adresse IP version 4 (IPv4) est constituée de 4 blocs de 4 octets chacun, [soit 32 bits, *ndlt*] et se présente comme suit : « x.x.x.x », où x est un nombre compris entre 0 et 255.

Une adresse IP version 6 (IPv6), plus longue (128 au lieu de 32 bits), est typiquement écrite avec le caractère « : » séparant chacun des huit nombres hexadécimaux qui la composent. Elle se présente de la façon suivante : `3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344`. Le système hexadécimal étant en base 16, 16 caractères allant de « 0 » à « 9 » puis de « a » à « f » sont utilisés pour représenter un chiffre. Ceci explique la présence de caractères alphabétiques dans une adresse IPv6.

Dans la mesure où l'IPv6 est encore relativement peu répandue, le présent rapport proposera principalement des exemples IPv4. D'un point de vue technique, il y a assez peu de différences entre le filtrage d'adresses IPv4 et le filtrage d'adresses IPv6.

Le vaste espace d'adressage offert par IPv6 résoudra probablement les problèmes de pénurie d'adresses. Le partage d'adresses IP sera dès lors moins fréquent (contrairement à ce qui se passe sous IPv4). Chaque adresse IPv6 conduira en conséquence à moins de contenu, ce qui devrait permettre en retour une meilleure précision du filtrage, lorsqu'il s'agira de le mettre en œuvre au niveau des adresses IP.

5.2.1.2 Les noms de domaine et les DNS

De façon à permettre un usage plus agréable et pratique d'Internet, les noms de domaine sont utilisés pour donner des noms signifiants aux contenus présents sur le réseau. Ils se présentent sous le format familier de « nomdedomaine.com » ou « siteweb.fr ».

Les noms de domaine sont utilisés pour identifier les ressources sur Internet, telles que les sites web ou les autres services (comme les serveurs de messagerie électronique ou de messagerie instantanée). Le système de noms de domaine (DNS) permet de résoudre ces

noms de domaine en adresses IP, [autrement dit d'établir une correspondance entre ces noms de domaine et les adresses IP qui leur sont associées, *ndlt*], ces dernières adresses étant utilisées par les ordinateurs pour communiquer.

Le premier niveau de la structure des noms de domaine consiste en des extensions de type « .com » ou « .fr ». Un nom de domaine de premier niveau (ou « domaine racine ») peut être de type générique, c'est-à-dire que son extension n'est liée à aucun pays ou région [tel que « .com », *ndlt*], ou de type géographique. Dans ce dernier cas, l'extension correspond à un code (ISO) de deux lettres (tel que .ie, .fr ou .nl) et permet d'identifier un pays.

Le deuxième niveau de la hiérarchie est généralement sélectionné et contrôlé par l'administrateur du domaine concerné. Le domaine aconite.ie, par exemple, est utilisé par Aconite Internet Solutions pour diriger les internautes sur son site web et pour ses services de messagerie électronique. Des identificateurs plus précis (les URL) pointent ensuite vers des contenus plus spécifiques du site web.

5.2.1.3 Les URL

Une URL, de l'anglais « Uniform Resource Locator », est l'adresse universelle qui permet de localiser un contenu sur Internet. L'URL est composée d'un nom de domaine (qui identifie la machine sur laquelle le contenu est disponible) et d'un certain nombre d'informations complémentaires permettant de localiser précisément le contenu sur la machine.

Une URL type de site web contient à la fois un chemin (les répertoires dans lesquels se trouve le contenu) et un nom de fichier cible (l'identificateur final du contenu sur le serveur). Un exemple d'URL type est : http://www.nomdedomaine.com/chemin/vers/fichier.html.

D'autres services tels que la messagerie électronique ou la messagerie instantanée peuvent également faire usage des URL et des noms de domaine pour identifier une partie de leur infrastructure.

5.2.1.4 Le nom et le contenu des fichiers

Dans de nombreux cas, la ressource (la photo ou la vidéo) est stockée dans un fichier. Chaque fichier a un nom différent, afin de permettre à l'utilisateur d'en identifier le contenu. Généralement, les utilisateurs choisissent des noms de fichiers assez parlants (par exemple « `ma_photo.jpg` »). Cependant, lorsqu'il s'agit d'un contenu illégal, celui-ci peut facilement être renommé de façon à passer inaperçu. En d'autres termes, le contenu d'un fichier est indépendant de son nom ou de son type.

5.2.1.5 Les mots-clefs

Une méthode d'identification des contenus est l'utilisation de filtres par mots-clefs. Les machines ont la possibilité d'identifier des mots-clefs à l'intérieur d'un document au format texte tel qu'un document Microsoft Word, ou dans le nom d'un fichier. Une liste de mots-clefs autorisés et interdits doit ensuite être maintenue, pour permettre les prises de décisions sur le filtrage. Cependant, de nombreux mots peuvent être utilisés dans un contexte parfaitement légal, et la simple apparence d'un mot ne cache pas toujours un contenu illégal (par exemple, les termes « adolescent » et « sexualité » peuvent très bien être employés dans un article scientifique). Il en résulte que, sans mots-clefs (ou noms de fichiers) très spécifiques et sans analyse précise du contexte, distinguer efficacement entre les contenus illégaux et ceux qui ne le sont pas est une tâche particulièrement compliquée pour un ordinateur.

5.2.1.6 La signature de contenu (valeur de hachage)

L'identification d'un contenu peut se faire d'après sa *signature*. Cette dernière permet de classifier les contenus qui ont été préalablement catégorisés comme illégaux. Il est possible

de créer une valeur unique qui identifie chacun de ces derniers, en utilisant un « *algorithme de hachage* » (tel que SHA1, SHA256 ou MD5).

Par exemple, une photo à caractère pédophile (contenue dans le fichier « `adolescent.jpg` ») a la valeur de hachage MD5 « `87e1a46d2529fe4f42a75789f0bae7a1` ». Cette valeur, qui est unique, ne permet pas de reproduire le contenu du fichier lui-même, car elle n'en constitue qu'une courte représentation, mais elle permet d'identifier ce contenu de manière certaine. Si une photo (dont le nom de fichier est « `inconnu.jpg` ») est découverte à plusieurs endroits, mais que sa valeur de hachage est identique à celle qui a été calculée pour l'image qui se trouvait dans le fichier « `adolescent.jpg` », cette circonstance démontre que les deux fichiers contiennent exactement la même image ou le même contenu. Il peut dès lors être démontré que l'image n'est pas innocente, et il pourrait être acceptable d'en empêcher l'accès.

5.2.2 L'efficacité du filtrage d'Internet

La présente sous-section se propose de mettre en lumière l'efficacité de chacun des mécanismes de filtrage. Cette efficacité va être évaluée en fonction de deux paramètres : la précision et l'impact réel sur l'accessibilité de la ressource ciblée.

Evaluer l'efficacité du filtrage en comparant la quantité de ressources qui se trouvent correctement bloquées à la quantité totale des ressources illégales disponibles (ce qui constituerait une méthode idéale de mesure de l'efficacité), s'avère une tâche extrêmement problématique car divers paramètres sont inconnus. Le volume total des contenus illégaux disponibles étant ignoré, le volume des requêtes (« *hits* ») dirigées vers les contenus filtrés par une liste noire ne peut donner qu'une vision très parcellaire de l'efficacité des différentes méthodologies de filtrage.

En outre, l'origine des requêtes étant souvent incertaine, les statistiques de volumétrie de ces requêtes, pour une liste noire donnée, constituent au mieux un indicateur très rudimentaire[241]. Les requêtes peuvent provenir d'utilisateurs qui tentent d'accéder au serveur web filtré, d'autres sites web qui référencent les contenus présents sur le serveur web filtré, ainsi que de moteurs de recherche et de logiciels appelés « robots », qui recherchent automatiquement les contenus présents sur Internet, sans intervention humaine. Par ailleurs, des logiciels malveillants comme des chevaux de Troie peuvent générer des accès vers un site web sans que le propriétaire de l'ordinateur accédant n'en soit conscient ou n'y ait consenti. Ces activités logicielles automatiques sont souvent prises en compte dans les statistiques des requêtes bloquées car il est difficile de les dissocier des activités humaines. Cette problématique devrait conduire à des investigations plus poussées, spécialement lorsque les statistiques présentent une relative stabilité sur une certaine période de temps, qui rend peu vraisemblable un accès aléatoire des utilisateurs.

Un autre paramètre permettant d'évaluer l'efficacité d'une mesure de filtrage est le potentiel de sur-blocage (ou filtrage excessif) et de sous-blocage (ou filtrage insuffisant) que cette mesure présente. L'efficacité des mesures actuellement utilisées, notamment sur les tentatives d'accès volontaires à des ressources illégales, ne peut donner lieu qu'à des estimations inexactes, notamment car aucun aperçu du volume total de la pédopornographie échangée sur Internet n'est disponible.

Un premier indicateur est **la facilité de contourner le filtrage**. S'il est facile de contourner ou de désactiver une mesure de filtrage, cette dernière n'a a priori pas d'effet sur la disponibilité de la ressource filtrée. Dès lors, l'efficacité peut être mesurée en fonction de l'impact du filtrage sur l'accessibilité de la ressource cible, lequel résulte lui même du nombre de tentatives d'accès réussies (accidentelles ou délibérées).

Par ailleurs, la **disponibilité de méthodes alternatives d'accès au même contenu** que celui qui est la cible du filtrage, quelles que soient ces méthodes, peut être considérée comme un élément de mesure de l'efficacité du filtrage en l'absence de données plus précises. En d'autres termes, un bon indicateur de l'impact du filtrage sur la disponibilité de la ressource, et donc du succès de la mesure de filtrage à cet égard, est de savoir s'il existe une possibilité aisée de publier le même contenu sur un canal différent de celui qui se trouve filtré, quand bien même la mesure de filtrage serait efficace sur ce dernier canal. Cette circonstance n'est pas nécessairement due aux propriétés d'une technologie de distribution donnée et des stratégies de filtrage qui lui sont applicables.

[241] Cf. Kaspersen 2009 p. 261 : Le nombre de hits publié ne distingue pas par type de visite (visite du robot d'exploration automatique de Google ou de l'utilisateur d'un fournisseur d'accès) ou par type de hit mesuré (un accès direct à une page d'avertissement ou le nombre de requêtes vers une liste noire, par exemple), ce qui rend difficile une comparaison efficace. La qualité, la taille et la nature des filtres employés ont également un impact sur le nombre de « hits » constatés par le système de filtrage.

Enfin, **la disponibilité d'autres méthodes de régulation**, qui seraient plus efficaces pour prévenir l'accès aux ressources concernées, est également à évaluer – spécialement si ces méthodes sont moins coûteuses, moins intrusives ou plus efficaces quant à la diminution de la disponibilité de la ressource.

5.2.3 Les caractéristiques des stratégies de filtrage

Les paragraphes qui suivent mettent en évidence les caractéristiques de plusieurs stratégies de filtrage, dont certains aspects sont communs et méritent d'être expliqués.

5.2.3.1 Liste blanche (« *allow-list* ») versus liste noire (« *block-list* »)

Une première caractéristique des stratégies de filtrage se révèle dans la manière dont le filtre opère. Les filtres qui sont configurés par défaut pour « autoriser » tout contenu à l'exception de ceux qui sont définis dans une liste spécifique sont communément considérés comme ayant recours à une « liste noire » (« *block-list* »). Les filtres qui sont configurés par défaut pour bloquer l'ensemble des contenus à l'exception de ceux qui sont spécifiquement définis dans une liste sont considérés comme ayant recours à une « liste blanche » (« *allow-list* »). Les immenses ressources qui sont nécessaires à l'analyse et à la classification de tous les contenus disponibles constituent un argument suffisant pour disqualifier l'utilisation large de listes blanches, y compris dans le cadre d'un usage public qui serait rendu obligatoire, dans une société démocratique et ouverte. Il n'est dès lors pas surprenant que la solution de la « liste noire » ait été adoptée par toutes les récentes initiatives occidentales de filtrage de la pédopornographie.

5.2.3.2 L'intervention humaine (filtrage dynamique ou manuel)

Une deuxième caractéristique de toutes les stratégies de filtrage est le nombre d'interventions humaines nécessaires pour réaliser le filtrage.

Typiquement, les filtrages mis en place pour lutter contre la pédopornographie se basent sur les signalements des utilisateurs et les investigations menées par les services en charge de l'application de la loi. Dans une telle situation, chacun des contenus présents dans le filtre est généralement sélectionné puis vérifié et confronté aux critères de la liste noire par l'administrateur de cette liste. Cette méthode est considérée comme correspondant à un filtrage manuel.

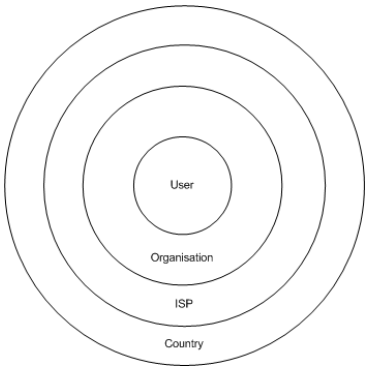
D'un autre côté, beaucoup de filtres, comme ceux des anti-spams et de certains antivirus, utilisent souvent des critères prédéfinis pour bloquer le contenu sans aucune intervention humaine. Ces critères peuvent être complexes et avoir des facettes multiples. Dans le cadre du filtrage du spam, des calculs statistiques complexes sont effectués pour distinguer les spams des messages qui n'en sont pas (filtrage bayésien). Ce type de filtrage est souvent considéré comme étant un filtrage de type dynamique[242].

Contrairement au filtrage du spam, des études ont démontré que le filtrage dynamique de la (pédo)pornographie était extrêmement inefficace. Etonnamment, toute tentative d'améliorer la précision de l'identification des contenus à filtrer conduit invariablement au sur-blocage de contenus conformes à la loi[243]. Le filtrage de la pédopornographie est donc condamné à recourir à de nombreuses variantes de listes noires, nécessitant maintenance régulière et intervention humaine intensive.

[242] Haselton B., « Report on accuracy rate of FortiGuard Filter » (« Rapport sur le taux de précision du filtre FortiGuard »), Bellevue, WA, Peacefire.org, 2007 ; Kaspersen 2009, p. 252.

[243] Kaspersen 2009 p. 253 ; Greenfield P, Rickwood R, Tran H., « Effectiveness of Internet filtering software products » (« Efficacité des produits logiciels de filtrage d'Internet »), CSIRO Mathematical and Information Sciences, 2001 ; Kranich N., « Why filters won't protect children or adults » (« Pourquoi les filtres ne protègeront ni les enfants ni les adultes »), Library Administration and Management, 2004, 8(1):14–8. ; Stark, Ph.B., Expert report of Philip B. (Rapport d'expert de Philip B.), Stark, Ph.D., « Civil Action no. 98-5591 (E.D. Pa) ACLU vs. Gonzales » (« Action civile n° 98-5591 (E.D. Pa), ACLU c/ Gonzales »), 8 mai 2006 ; Haselton B., « Report on accuracy rate of FortiGuard Filter » ("Rapport sur le taux de précision du filtre FortiGuard »), Bellevue, WA: Peacefire.org, 2007.

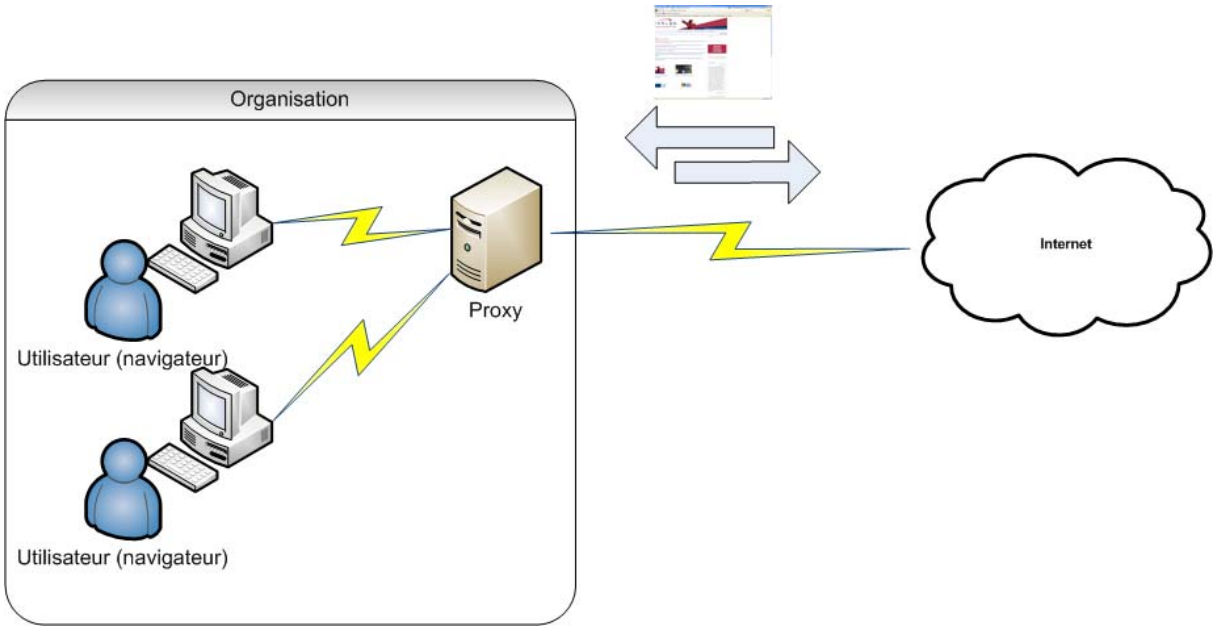
5.2.3.3 Point de filtrage



Les stratégies de filtrage peuvent être différenciées en fonction de l'endroit où elles sont mises en œuvre sur le réseau.

En premier lieu, les filtres pour postes clients, qui se trouvent placés au niveau de l'utilisateur, permettent aux parents et aux administrateurs de l'ordinateur de bloquer les contenus. Le contournement de ce type de filtres est généralement aisé pour l'administrateur de la machine. Les autres utilisateurs ne peuvent pas contourner facilement la mesure, tant qu'ils sont limités à l'utilisation de l'ordinateur concerné et du système d'exploitation sur lequel le filtre est installé[244]. L'efficacité des filtres pour postes clients sur les contenus à caractère (pédo)pornographique a fait l'objet de nombreux tests au début du siècle, aux Etats-Unis et en Australie. Les résultats se sont avérés, au mieux, médiocres[245].

Par ailleurs, d'autres techniques de filtrage sont utilisées à l'échelle d'une entreprise, d'un fournisseur d'accès à Internet (FAI), voire d'un pays. Typiquement, ces techniques requièrent que les flux soient envoyés en amont vers des machines centrales, chargées d'analyser le trafic. Ces machines sont au contact d'Internet et surveillent les requêtes effectuées par les utilisateurs. Elles vérifient généralement les adresses et les titres des contenus demandés et décident d'en bloquer ou non l'accès, en utilisant des filtres qui peuvent être dynamiques ou manuels.



Il est également possible d'utiliser les technologies de filtrage pour enregistrer et surveiller les requêtes vers Internet et les réponses qu'elles reçoivent, *sans* effectuer de filtrage. Ceci peut être utile pour surveiller les activités potentiellement criminelles ou terroristes qui utilisent les réseaux publics nationaux.

---

[244] Voir également ACMA, *Closed environment testing of ISP-level content filtering (test de filtrage en environnement fermé à l'échelle d'un FAI)*, juin 2008, p. 9, disponible à l'adresse :http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf.

[245] Voir : une étude effectuée en 2001 en Australie (en anglais) : http://www.acma.gov.au/webwr/aba/newspubs/documents/filtereffectiveness.pdf ; Le GAO des Etats-Unis sur l'efficacité du filtrage du P2P (en anglais) : http://www.freedom-to-tinker.com/doc/2005/gao_30jun.pdf ; une étude sur l'accès à Internet dans les établissements scolaires par l'EFF (en anglais) : http://w2.eff.org/Censorship/Censorware/net_block_report/net_block_report.pdf.

A l'échelle d'un pays, le coût d'une infrastructure centralisée de filtrage de l'ensemble du trafic Internet est extrêmement élevé. Les investissements nécessaires à l'implémentation d'une plateforme centrale capable de supporter les charges de trafic sont déjà significatifs à eux seuls.

5.2.3.4 Le niveau de détail ou de spécificité

Lorsque le contenu est vérifié manuellement avant d'être inséré dans une liste noire, il existe plusieurs méthodes pour empêcher les utilisateurs d'y accéder. La différence entre ces méthodes tient au niveau de détail avec lequel le contenu est identifié. Il est fréquent que plusieurs identificateurs soient utilisés, afin d'identifier le contenu à filtrer de différentes manières, plus ou moins détaillées :

Les adresses IP

Chaque identificateur a un niveau de granularité ou d'unicité différent, en termes de contenu filtré. Par exemple, bloquer une *adresse IP* implique que tous les autres services et utilisateurs qui partagent cette adresse IP seront également bloqués. Il convient de se rappeler que plusieurs sites web peuvent être identifiés sous des noms de domaine différents tout en partageant une seule et même adresse IP. Si l'accès à cette IP partagée est bloqué, tous les sites web et les services qui seront localisés à cette même adresse seront également rendus inaccessibles, quand bien même chacun d'entre eux serait géré par un propriétaire différent[246]. Lorsqu'un opérateur finlandais de transit Internet Tier 1 (opérateur de premier plan) bloqua une vaste plage d'adresses IP russes qui étaient régulièrement utilisées pour l'hébergement de sites web à caractère pédopornographique, cette initiative eut pour effet de bloquer un grand nombre d'utilisateurs russes innocents et de porter atteinte au commerce des prestataires russes de services Internet dont les adresses IP étaient concernées. L'objectif de cette tactique était d'exercer une pression sur certains prestataires russes de services Internet afin de les conduire à agir contre ces sites web proposant des ressources illégales.

Les noms de domaine

Le filtrage d'un nom de domaine bloquera ***la totalité*** du contenu résidant derrière ce nom de domaine. Bien que certains sites web puissent se focaliser sur un seul sujet ou type de contenus, tel que la pédopornographie, il reste possible qu'une partie du contenu résidant derrière un domaine ne soit pas relatif à la pédopornographie, mais qu'il soit impacté quand même par le filtrage. Dans certains pays, le pourcentage de ressources potentiellement illégales présentes sur un site web est calculé statistiquement par rapport aux ressources légales qui y sont également présentes. Si ce pourcentage dépasse un seuil prédéfini, le nom de domaine est ajouté à la liste noire. Cette approche accepte l'idée de dégâts collateraux et que certains contenus innocents/conformes à la loi seront bloqués. Par exemple, filtrer un nom de domaine (de premier niveau) tel que « `xs4all.nl` » (l'un des principaux FAI aux Pays Bas, dont les abonnés peuvent avoir des sites personnels hébergés sous ce nom de domaine, leur nom d'utilisateur servant d'identificateur pour leur répertoire sur le serveur) ne conduirait pas seulement au blocage de « `home.xs4all.nl/~malfaiteur` », mais aussi de « `home.xs4all.nl/~abonné_innocent` », ainsi que du site web principal du prestataire XS4all qui est accessible à l'adresse « `www.xs4all.nl` » (dans son ensemble, y compris tous ses domaines dits de second niveau qui contiennent divers sites web et services). [Le groupe France Télécom et sa marque Orange répondant aux mêmes caractéristiques, les exemples ci-dessus pourraient respectivement être remplacés par « `orange.fr` », « `pages.perso.orange.fr/malfaiteur` », « `pages.perso.orange.fr/abonné_innocent` » et « `www.orange.fr` », *ndlt*].

---

[246] Voir B. Edelman, « Web Sites Sharing IP Addresses: Prevalence and Significance » (« Le partage d'adresse IP par les Sites Web : Prédominance et Signification »), http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/, dont l'analyse montre que la majorité des sites web (87,3 %) identifiés par des noms de domaines sont hébergés derrière une adresse IP partagée.

Les URL (*Uniform Resource Locators*)

Pour obtenir de meilleurs résultats en termes de précision, il est donc préférable d'utiliser un filtrage *basé sur l'URL*. Cela implique que la liste noire permette de distinguer entre les différentes URL que sont *www.xs4all.nl/~malfaiteur/page_illégale.htm*, *www.xs4all.nl/~utilisateur_innocent*, ou *www.xs4all.nl/malfaiteur/page_légale.htm*. [Pour un exemple concernant France Télécom, il conviendrait de distinguer entre les URL www.orange.fr/malfaiteur/page_illégale.htm, www.orange.fr/utilisateur_innocent et www.orange.fr/malfaiteur/page_légale.htm, *ndlt*]. Pour cela, le système de filtrage doit lui aussi supporter ce niveau de détail. Or, un tel niveau de spécificité requiert un travail significatif et d'importantes ressources pour analyser l'immense quantité de contenus, aussi variés les uns que les autres, présents sur les sites webs et destinés à être intégrés à la liste noire. En outre, pour un propriétaire de site web, modifier une URL est un exercice trivial, qui peut être fait automatiquement à l'aide d'un logiciel pour chaque fichier sollicité par un utilisateur, dans le but de perturber les filtres. En raison de la facilité qu'il y a à contourner ce type de filtrage, le mettre en place peut conduire à un risque significatif de sous-blocage (ou filtrage insuffisant).

Les signatures de contenu

Les ressources Internet peuvent être classifiées et filtrées en utilisant les signatures de contenus qui ont été préalablement catégorisés comme étant illégaux. Voir supra, la sous-section 5.2.1.6 du présent rapport.

Ce type de filtrage requiert un accès étendu au contenu Internet qui est transféré entre l'utilisateur et Internet. Il implique également une connaissance préalable des contenus illégaux disponibles, puisqu'il requiert la création de signatures. De nouveaux contenus illégaux peuvent donc ne pas être identifiés par le système de filtrage. Par ailleurs, une modification de l'image, aussi infime soit-elle, peut conduire à la modification de sa signature, et dès lors à sa non reconnaissance par le système de filtrage, qui échouera à la bloquer. Cette situation ne peut être surmontée qu'au prix d'un investissement considérable dans l'analyse de nouveaux contenus par d'autres moyens, typiquement par des êtres humains, analystes de contenus. Le coût en serait probablement très élevé.

Le chiffrement du contenu concerné rendra également cette méthode de filtrage totalement inopérante, puisqu'un fichier chiffré ne peut pas être analysé facilement.

En conclusion, ce système présente un risque significatif de sous-blocage (ou filtrage insuffisant). Il est également très consommateur de ressources, en ce qu'une signature doit être calculée pour chaque contenu concerné par la mesure, afin de comparer cette signature à celles qui se trouvent dans une base de données.

Les mots-clefs

Une décision de filtrage peut être prise sur la base des mots-clefs trouvés dans le nom de fichier, dans l'URL ou dans le texte du contenu auquel un utilisateur souhaite accéder. Pour que cette méthode soit efficace, il est nécessaire de procéder à une analyse complexe des mots-clefs qui se trouvent ainsi reconnus, par rapport au contexte de leur utilisation. Un être humain peut identifier un contenu comme étant « potentiellement conforme à la loi » à la seule vue du contexte dans lequel apparaît un mot suspect. Une telle opération, pour un filtre dynamique, est loin d'être triviale lorsqu'il s'agit de décider de filtrer des contenus Internet.

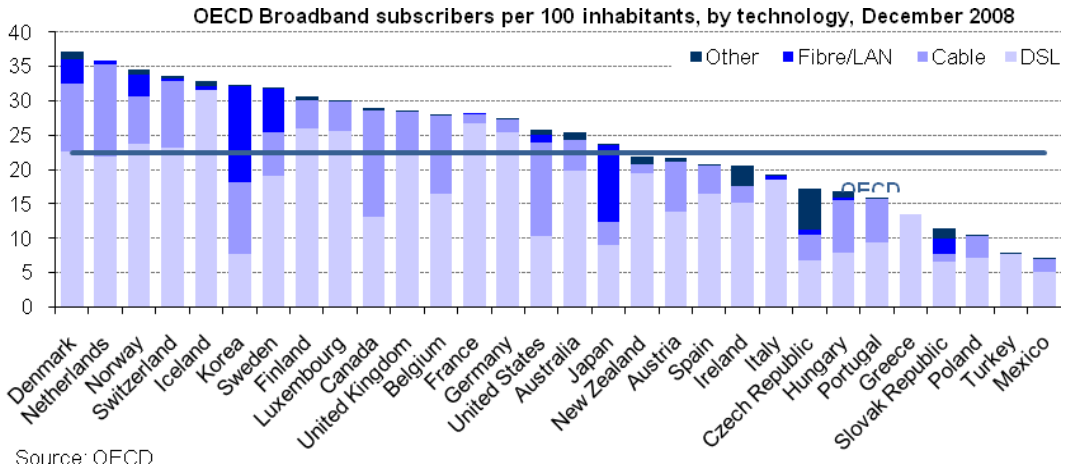
Par exemple, si l'on décidait de filtrer tout simplement l'ensemble des pages web contenant le mot « pédopornographie », les sites contenant les mots « recherches sur la pédopornographie » ou « législation sur la pédopornographie » seraient également filtrés, ce qui n'est clairement pas l'objectif du système de filtrage. Le présent rapport serait lui-même complètement filtré par de tels systèmes simplistes, qui y trouveraient ce mot-clef de nombreuses fois.

Un système utilisant les mots-clefs est encore facilement contournable en modifiant l'orthographe des mots importants. Le mot « pédopornographie » peut par exemple être transformé en celui de « pdopornographie » ou de « p9dopornographie ». L'utilisation de (mauvais) orthographes et d'acronymes plus complexes est encore un usage de plus en plus largement répandu parmi les utilisateurs de téléphones mobiles, dans le cadre de la rédaction des SMS, où l'expression « J'ai faim » s'écrit par exemple « G f1 ».

5.3 Les méthodes de distribution de ressources à caractère pédopornographique sur Internet

5.3.1 La pénétration d'Internet et la distribution de contenus illégaux

Les services haut-débit se sont développés à un rythme fulgurant au cours des dernières années. Le graphique n° 1 montre clairement que de nombreuses sociétés ouvertes, occidentales et démocratiques, sont leaders en la matière[247].



Graphique n°1 – Nombre d'abonnés haut débit pour 100 habitants selon le portail haut débit de l'OCDE[248]

Les ressources à caractère pédopornographique peuvent être distribuées sur Internet de diverses manières, grâce aux connexions Internet à haut-débit[249]. En plus de permettre la diffusion de contenus statiques (autrement dit de photos ou de vidéos), les connexions haut-débit servent également de tremplin pour des comportements tels que *la sollicitation d'enfants à des fins sexuelles* (« *grooming* ») ou *le cyber harcèlement ou cyber intimidation* (« *cyber bullying* »). L'usage croissant des réseaux sociaux a contribué de manière importante au développement de ces activités[250].

INHOPE, le réseau international de services d'assistance en ligne (« *hotlines* »), lesquels prennent en charge le traitement des signalements de certains types de contenus illégaux rencontrés sur Internet par le public, donne une indication des principaux moyens que le public a détectés comme étant actuellement utilisés pour diffuser des contenus illégaux de type statique[251]. Le graphique ci-dessous inclut les signalements concernant des contenus de

[247] A titre de comparaison (peu de pays en voie de développement sont membres de l'OCDE), les chiffres pour les pays non membres de l'OCDE en Afrique et en Europe de l'Est montrent des taux de pénétration bien moins élevés. Voir EBRD, *Comparative assessment of the telecommunications sector in the transition economies* (Eastern Europe) (*Etude comparative du secteur des télécommunications dans les économies en transition* - Europe de l'Est) : http://www.ebrd.com/country/sector/law/telecoms/assess/report.pdf. S'agissant de l'Afrique (accès bas débit inclus), voir (en anglais) : http://www.internetworldstats.com/stats1.htm.

[248] Chiffres pris à partir du Portail Haut-Débit de l'OCDE (en anglais) : http://www.oecd.org/sti/ict/broadband (2009).

[249] Voir (en anglais) http://is2.lse.ac.uk/asp/aspecis/20060154.pdf.

[250] Voir Kim-Kwang et Raymond Choo, Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offence (Comportements prédateurs en ligne à l'égard des enfants : une revue litteraire des mauvaises pratiques sur les réseaux sociaux pour solliciter les enfants à des buts de sévices sexuels), Australian Institute for Criminology (Institut australien de criminologie), disponible à cette adresse : http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf.

[251] Voir le Rapport d'Inhope 2007 Global Internet Trend Report (Rapport de 2007 sur les tendances de l'Internet au niveau mondial), disponible à l'adresse suivante : https://www.inhope.org/en/system/files/inhope_global_internet_trend_report_v1.0.pdf.

haine raciale ou des contenus d'une autre nature, mais dans la mesure où la pédopornographie représente plus de 50% des contenus potentiellement illégaux signalés, il donne malgré tout un assez bon éclairage sur les mécanismes de distribution tels qu'ils sont perçus par le grand public.

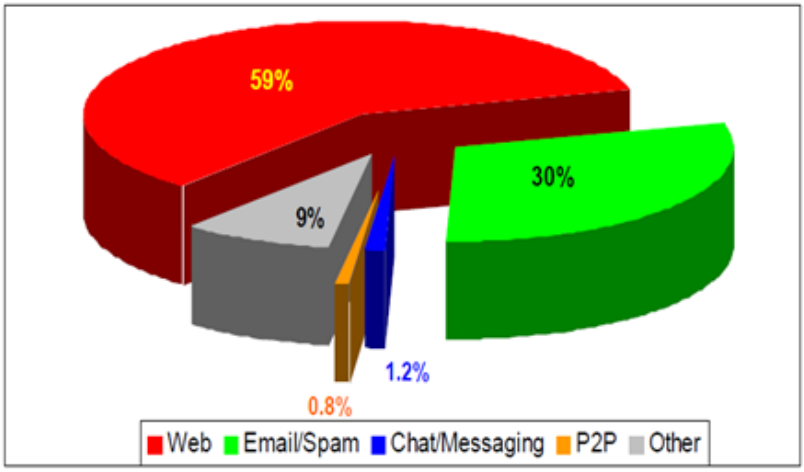
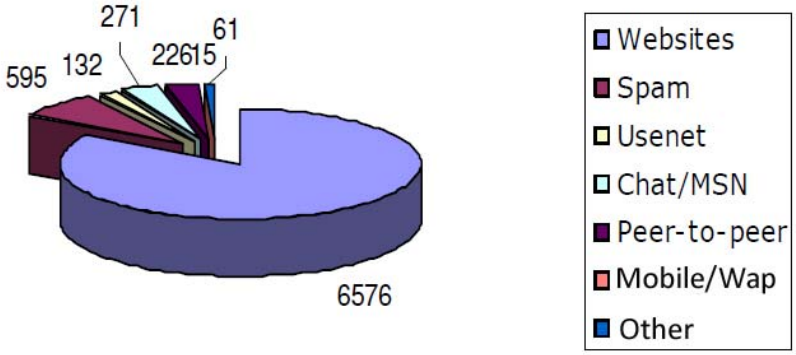


Diagramme des différents **services Internet** et de leur contribution dans le **nombre total des signalements reçus** (tendances moyennes pour le dernier trimestre 2006).

Graphique n°2
Moyens de distribution des contenus signalés comme étant illégaux selon INHOPE

De récentes statistiques du service néerlandais d'assistance en ligne contre la pédopornographie, qui indiquent également la répartition des signalements reçus par type de service concerné, confirment ces résultats. Elles montrent en effet que, selon la perception du public, les sites web représentent le moyen prédominant de distribution de ressources à caractère pédopornographique. Selon cette même perception, viennent ensuite les messages non sollicités (spams), les groupes de news du réseau Usenet, et enfin les réseaux de pair à pair (« *peer to peer* » - partage de fichiers)[252].



Graphique n°3
Moyens de distribution selon le service néerlandais d'assistance contre la pédopornographie

Il faut cependant noter que ces statistiques sont relatives à des signalements. Ces statistiques ne font donc état que d'allégations[253] de pédopornographie, émises par le public à l'occasion de ses signalements. Il est également important de remarquer que, bien que les sites web soient souvent accessibles publiquement et que le spam soit adressé de manière aveugle sans avoir de cibles précises, certains services (comme les réseaux de pair à pair - « *peer to peer* ») requièrent que l'utilisateur final procède à une sélection directe du contenu qu'il

[252] A comparer également : Kaspersen et al. 2008, p. 6, qui recense des chiffres historiques similaires depuis 2002.
[253] 20% des signalements correspondaient à des contenus illégaux ou préjudiciables et un pourcentage global de 10% correspondait à des contenus illégaux, incluant les ressources à caractère pédopornographique et les discours de haine (voir le *Global Internet Trend Report (Rapport sur les tendances de l'Internet au niveau mondial)* d'Inhope sur www.inhope.org).

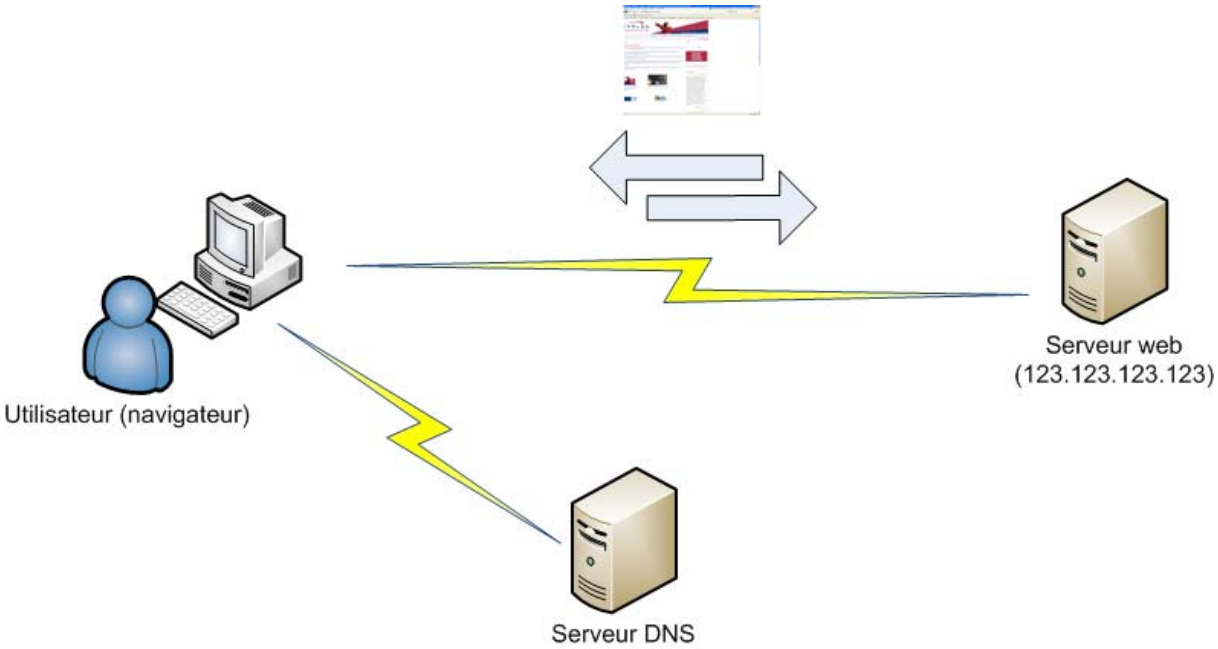
souhaite obtenir, parmi les contenus disponibles (par exemple en procédant à des recherches en ligne). Il en résulte qu'il est peu probable que les utilisateurs de ces derniers services « tombent par hasard » sur une information, et encore moins qu'ils en signalent le contenu répréhensible.

Il est enfin utile de préciser que malgré le fort taux de pénétration d'Internet aux Pays-Bas, la probabilité qu'un utilisateur néerlandais tombe accidentellement sur un contenu à caractère pédopornographique est relativement faible. Dans ce pays de 16 millions d'habitants, la plupart d'entre eux ayant un accès régulier à Internet, les 7 500 signalements[254] qui y ont été rapportés induisent une probabilité d'environ 0,05% que ceci arrive à un habitant au cours d'une année.

[254] Ce chiffre exclut les utilisateurs ayant découvert un contenu illégal mais ne l'ayant pas signalé à un service d'assistance en ligne.

5.3.2 Les sites web

Les sites web sont l'un des moyens les plus utilisés pour distribuer tous types de contenus sur Internet. Ils fonctionnent par l'intermédiaire de serveurs, lesquels sont tous identifiés par des noms de domaine et des adresses IP (Internet Protocol).



Le système de noms de domaine (DNS), à l'échelle mondiale, est utilisé pour traduire les noms de domaine des sites web en adresses IP, lesquelles permettent ensuite d'accéder aux contenus de ces sites.

Le système de communication, ou protocole, utilisé pour accèder à un site web, est appellé HTTP (HyperText Transport Protocol).

Afin de rendre le contenu disponible aux utilisateurs, un grand nombre de logiciels et d'équipements informatiques différents fonctionnent de concert. En premier lieu, il faut un serveur, qui est configuré pour recueillir le contenu du site web auquel l'accès est requis, afin de l'envoyer à l'utilisateur concerné, et pour maintenir une connexion avec le navigateur internet par lequel cet utilisateur a formulé sa requête d'accès. Cette machine est communément appelée *serveur web*. En général, une seule machine héberge le logiciel qui est utilisé pour délivrer le contenu à l'utilisateur. Toutefois, pour des sites web conséquents, il n'est pas inhabituel de répartir cette charge de travail sur plusieurs machines.

Il existe parfois également un serveur intermédiaire, appelé « serveur proxy », dont le rôle est de délivrer le contenu qu'il a préalablement récupéré de serveurs web à travers le monde. Les organisations utilisent souvent un serveur proxy pour accélérer l'accès aux contenus web qui sont fréquemment visités par les utilisateurs de leurs services.

Le logiciel utilisé pour délivrer le contenu des pages web est appelé logiciel d'hébergement web. La plupart du temps, il s'agit d'un logiciel open source, comme Apache, même s'il existe un grand nombre d'autres alternatives. Microsoft, ainsi que de nombreux autres éditeurs de logiciels, ont développé des logiciels de serveur web pour toutes sortes d'usages.

Habituellement, le contenu web est stocké sur le disque dur du serveur. Mais il est également possible que ce contenu soit récupéré ou créé dynamiquement, souvent au moyen d'une base de données qui contient les informations nécessaires à cette opération. Lorsque le contenu est produit dynamiquement en s'appuyant sur une base de données ou sur des programmes hébergés par le serveur web, le contenu est alors appelé « *contenu généré* ». Dans ce cas, le

contenu est le produit d'une opération programmée, et il n'en existe pas de copie statique sur le serveur web. Il en résulte que le contenu web renvoyé à l'utilisateur peut être différent selon l'adresse IP de la machine qui émet la requête, de l'heure, ou même de centaines d'autres critères définis sur le serveur web.

De nombreux langages de programmation ou de script peuvent être utilisés pour générer le contenu en fonction des interactions avec l'utilisateur. Les langages de script (ou de programmation web) les plus typiques sont le PHP (langage open source) et l'ASP (créé par Microsoft), bien que de nombreux autres langages soient utilisés sur Internet.

Dans un environnement multi-serveurs, le contenu peut résider sur plusieurs machines, ayant chacune un rôle différent. L'une d'entre elles peut très bien faire l'interface avec les utilisateurs finaux, alors que d'autres machines sont en charge de stocker les fichiers de contenus auxquels ces utilisateurs accèderont. Enfin, une dernière machine peut héberger la base de données qui produira les résultats de recherches que pourront explorer les utilisateurs. Dans ce type d'architectures multi-serveurs, il est possible d'utiliser des machines situées sur des réseaux géographiquement différents, et, grâce à Internet, de les faire travailler de concert dans un même environnement de travail.

Le contenu affiché par un serveur web est habituellement formaté en langage HTML (Hypertext Markup Language). Ce langage permet d'afficher des images, vidéos et d'autres types de contenus dans le navigateur web des utilisateurs (tel que Chrome, Firefox, Internet Explorer, Opera ou Safari).

Lorsqu'un utilisateur accède à un site web identifié par un nom de domaine, son navigateur Internet va généralement, en premier lieu, adresser une requête au serveur de noms de domaine (DNS) du FAI de cet utilisateur, pour obtenir l'adresse IP du serveur web à contacter pour ce domaine. Le système DNS, au niveau du FAI, sera alors sollicité pour suivre la structure hiérarchique du nom de domaine, successivement, jusqu'au serveur en charge d'apporter la réponse à la requête DNS de l'utilisateur.

Par exemple,

- Une première requête est envoyée au serveur DNS qui est en charge de répondre aux requêtes concernant le domaine de premier niveau (ou serveur racine du DNS) `.com` (opéré sous l'autorité de l'ICANN), qui est géré par la société VeriSign ;
- Ce serveur racine du DNS localise ensuite le serveur DNS (par exemple **`serveurdns.registrar.com`**) qui a autorité sur le nom de domaine concerné (comme **`nomdedomaine.com`**) ;
- Ce dernier serveur DNS est alors interrogé afin d'obtenir la localisation du serveur web. Cette information est ensuite envoyée à l'utilisateur.

Une fois cette information reçue, une connexion est établie entre l'ordinateur personnel de l'utilisateur et le serveur web qui contient ou génère le contenu du site web. Bien qu'un grand nombre de sites web opèrent à partir d'une adresse IP qui leur a été dédiée, il est possible que de nombreux noms de domaine pointent vers une même adresse IP. Cette pratique est assez répandue[255]. Il est également possible d'accéder à un site web sans utiliser son nom de domaine, en écrivant directement son adresse IP dans le navigateur.

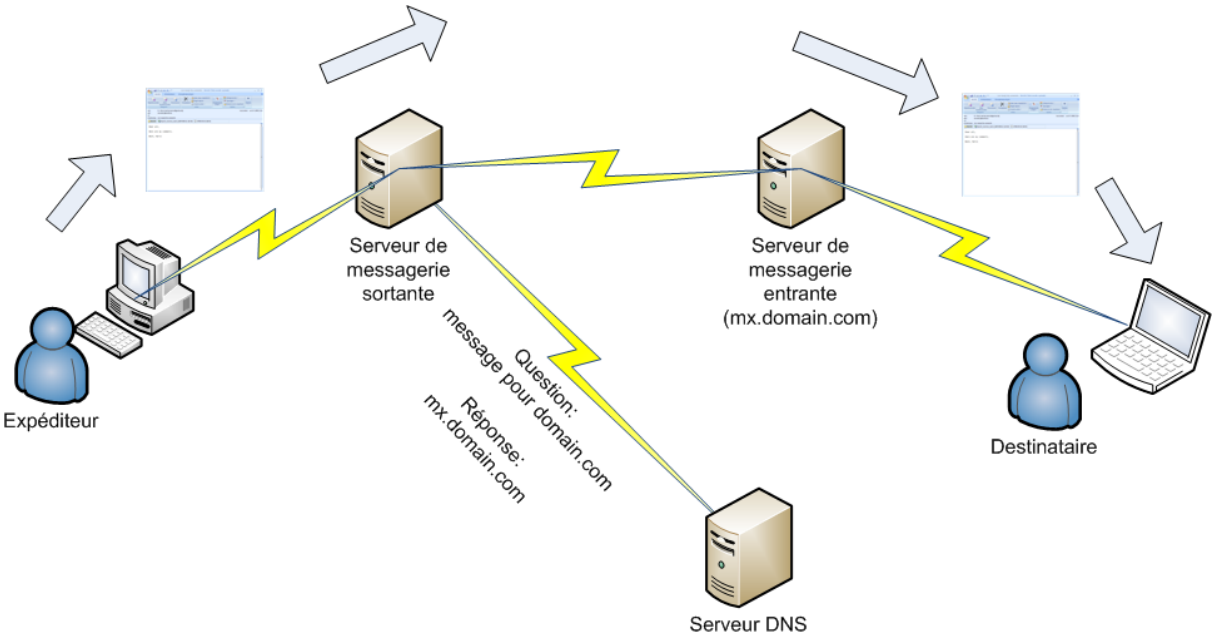
Il est fréquent que de nombreux sites web, gérés par des propriétaires différents, soient associés à une seule et même adresse IP. Dans une telle situation, le serveur web a alors besoin de connaître le nom de domaine qui correspond au site web qui fait l'objet de la

[255] B. Edelman, « Web Sites Sharing IP Addresses: Prevalence and Significance » (« Partage d'adresses IP par des sites web : prédominance et signification »), disponible à l'adresse : http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/.

requête (il doit autrement dit connaître l'URL ou le nom de domaine que l'utilisateur cherche à joindre à cette IP partagée), pour pouvoir afficher le site web qui est précisément demandé.

5.3.3 La messagerie électronique et le spam (messages non sollicités)

La messagerie électronique reste le service le plus utilisé sur Internet, bien plus encore que le web ou les réseaux sociaux. Ceci dit, la plupart des signalements relatifs à des ressources abusives concernent des messages électroniques faisant la promotion de sites web.



L'envoi d'un message se fait grâce à un client (comme Microsoft Outlook ou un système webmail comme MSN Live ou Gmail), via un serveur de messagerie (appelé aussi MTA : Mail Transfert Agent) prédéfini, qui est en charge de transmettre le message au destinataire.

Les serveurs de messagerie sortante sont généralement opérés par des fournisseurs d'accès à Internet ou des fournisseurs d'hébergement, lesquels n'autorisent l'envoi de messages qu'à leurs abonnés. Les serveurs de messagerie entrante, qui fonctionnent souvent sur les mêmes machines que ceux de messagerie sortante, ont pour fonction de recevoir les messages et de les stocker jusqu'à ce que les utilisateurs les récupèrent depuis un ordinateur personnel ou un terminal mobile.

Le système de noms de domaine (DNS) joue encore une fois un rôle important dans l'utilisation de la messagerie électronique. Il est utilisé pour localiser le point de destination du message. Une requête DNS permet de déterminer le serveur de messagerie compétent pour cette destination. Par exemple, une requête DNS concernant un destinataire final utilisant Google Gmail produira en réponse le nom DNS du serveur de messagerie entrante « `gmail-smtp-in.l.google.com` », ainsi que quatre autres adresses pouvant être utilisées en alternative si le serveur MTA principal ne fonctionne pas ou ne peut être joint.

Le transport des messages s'effectue entre les différents serveurs MTA, en utilisant le protocole SMTP (Simple Mail Transfer Protocol). Le SMTP est un protocole très ancien[256] et omniprésent, qui définit la manière dont les messages sont transmis d'un serveur à un autre. Le procotole est dit « *stateless* » (sans Etat) et « *open-by-design* » (ouvert par conception), ce qui signifie que le serveur MTA sortant (émetteur) ne conserve pas de trace de l'envoi du message (que ce soit un échec ou une réussite) et que, par défaut, n'importe quelle machine est susceptible de transmettre des messages à un serveur de messagerie entrante.

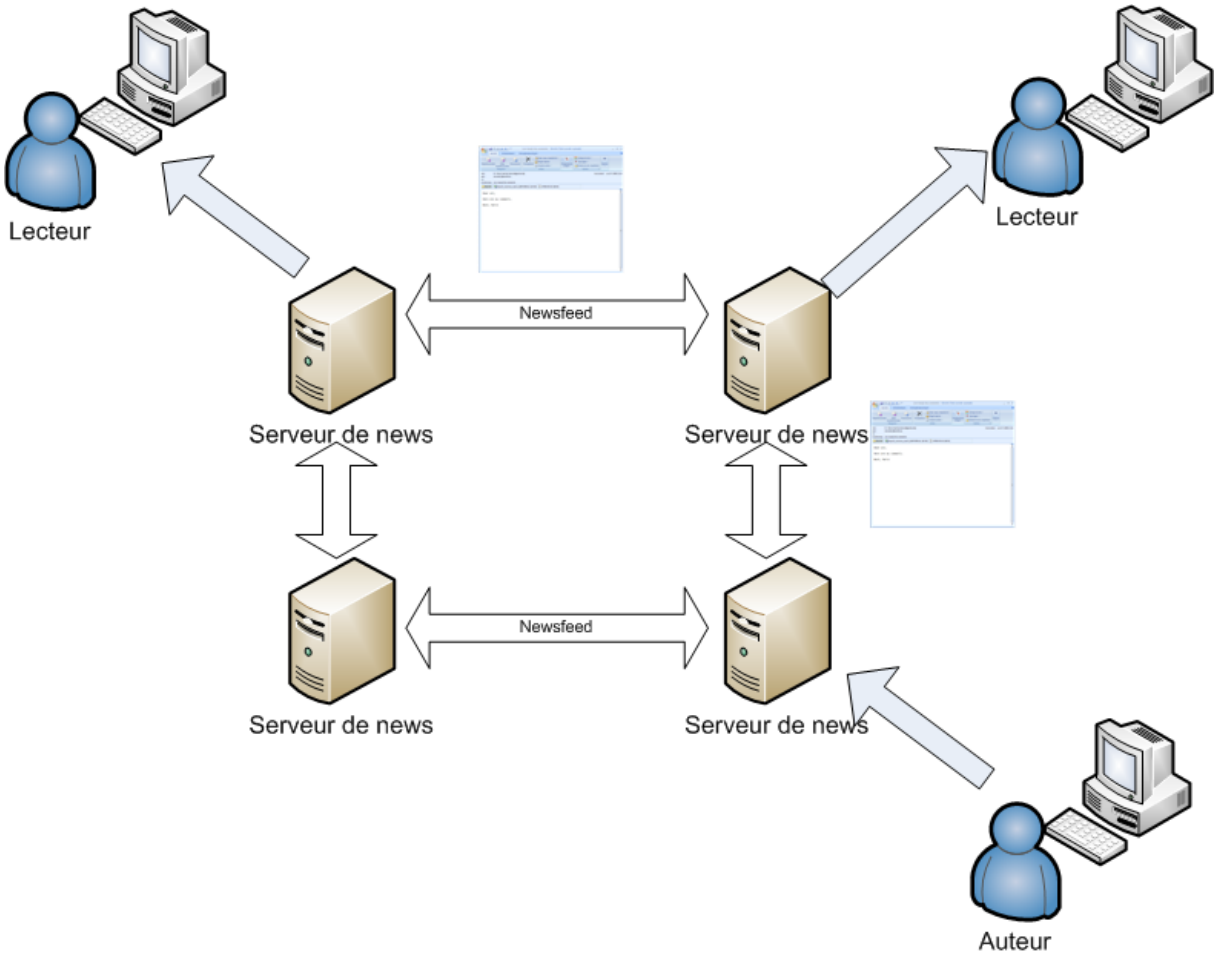
[256] Il fut defini en 1982. Voir ses spécifications techniques dans la RFC 822, disponible en anglais à l'adresse suivante : http://tools.ietf.org/html/rfc822, laquelle fut remplacée en 2001 par la RFC 2822, disponible en anglais à l'adresse suivante : http://tools.ietf.org/html/rfc2822.

Afin de pouvoir transporter des données (comme des photos ou des videos) à l'intérieur des messages textes qui transitent entre les serveurs MTA, celles-ci sont encodées et décodées en simples messages textes par le logiciel de messagerie de l'utilisateur final. C'est ainsi qu'un protocole initialement destiné à ne transporter que des messages textes peut transporter des fichiers de données (données binaires) en tant que pièces jointes, lesquelles se trouvent dans le corps du message texte.

5.3.4 Les groupes de news (« *newsgroups* ») du réseau Usenet

Usenet existe depuis des décennies[257], et servait initialement à diffuser du contenu texte entre ses différents serveurs publics. Depuis qu'Internet est utilisé à des fins commerciales, Usenet est devenu une plateforme très populaire de diffusion de toutes sortes de contenus illégaux, ces derniers allant des contenus protégés par des droits d'auteur aux contenus à caratère pédopornographique.

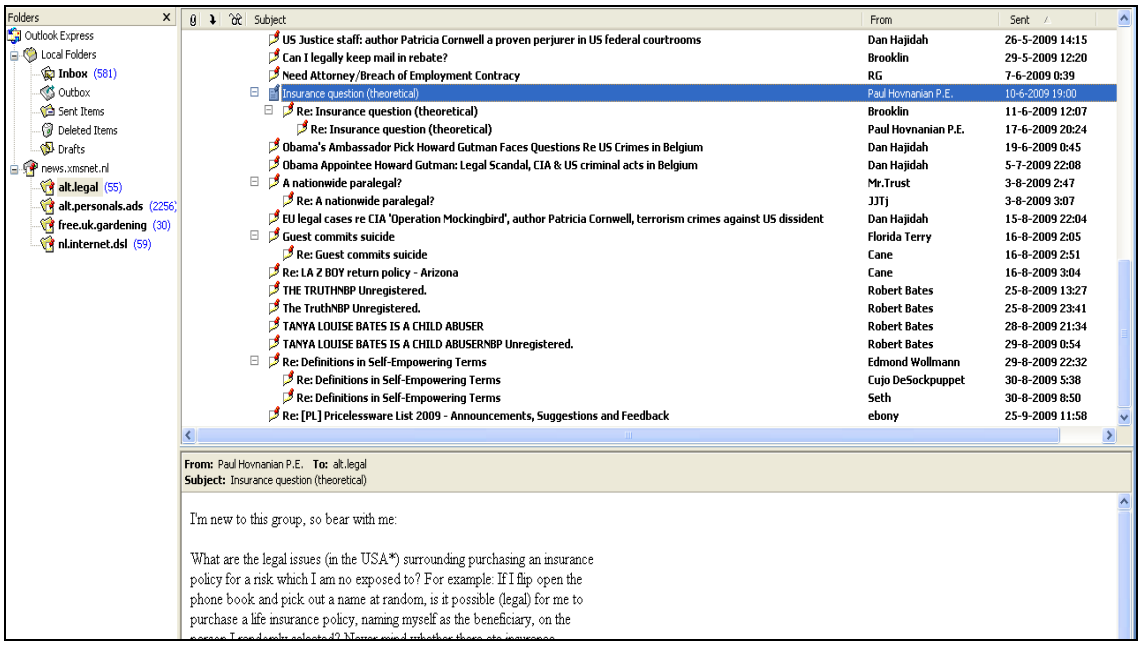
Les serveurs Usenet (ou serveurs de news), généralement opérés par les FAI, agissent de la même manière que les serveurs de messagerie, en ce sens qu'ils reçoivent des messages textes de la part des utilisateurs finaux, messages qu'ils transmettent ensuite aux autres serveurs de news. Les utilisateurs du réseau utilisent un programme logiciel appelé « lecteur de newsgroups », tel que Outlook Express ou des logiciels Usenet plus spécialisés (comme Grabit ou Newsleecher), pour télécharger et afficher le contenu des serveurs.



La différence majeure qui existe entre les groupes de news et la messagerie électronique est que les flux de messages qui circulent entre les serveurs Usenet (souvent appelés « newsfeeds », pour « distribution de nouvelles » ou « distribution d'articles Usenet »), sont organisés sous forme de groupes, dont le nom suggère le contenu des messages qui y sont échangés (par exemple « `alt.binaries.windows` »). Les serveurs affichent les messages, à l'attention du public utilisateur, de la même façon qu'un forum de discussion web ou un site de discussion en ligne (ou babillard, « *discussion board* »). Les listes de messages, groupe par groupe, sont maintenues par les serveurs et peuvent être récupérées grâce au protocole

[257] Usenet a été conçu par deux étudiants de l'Université de Duke, Tom Truscott et Jim Ellis, en 1979. Ils ont repris l'idée du service « Bulletin Board Services », très populaire à l'époque, auquel les utilisateurs pouvaient accéder par connexion téléphonique et en voir les contenus textes à partir de leur ordinateur.

NNTP (le protocole de Usenet). Les messages à l'intérieur d'un groupe sont organisés par sujet et sous-sujet et peuvent être affichés de manière hiérarchique par les lecteurs de newsgroups récents (voir capture d'écran).



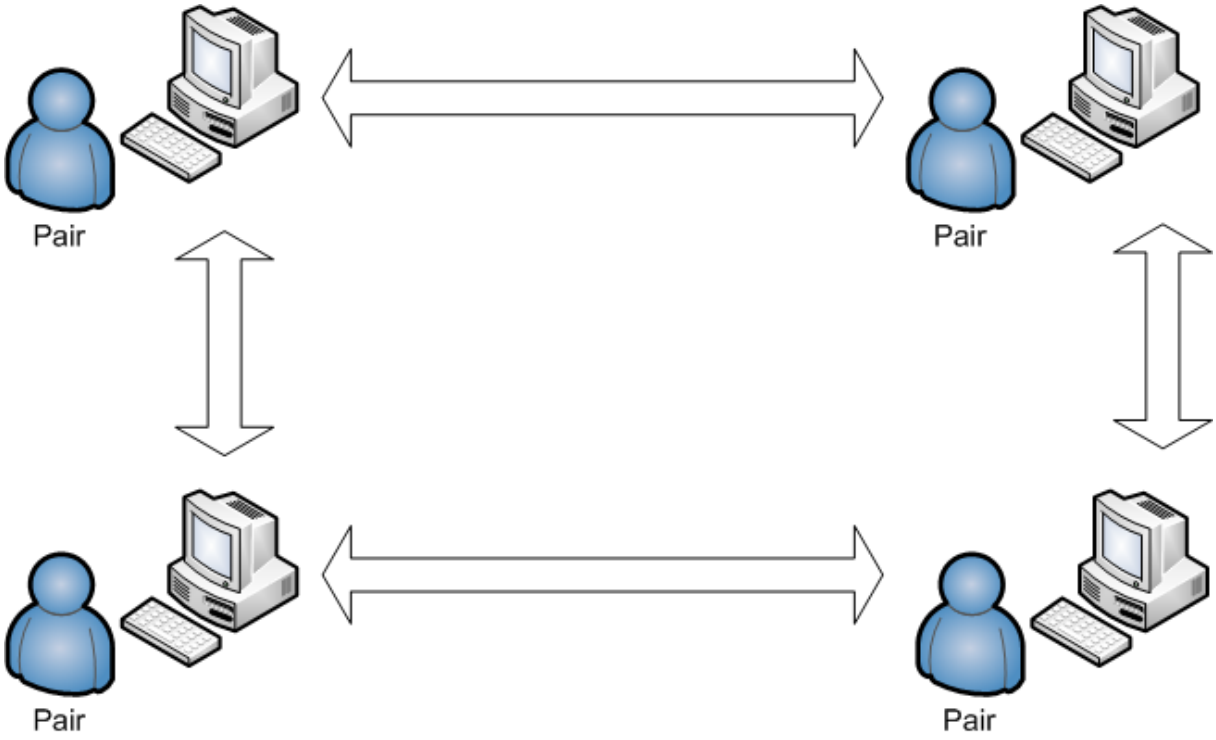
Usenet ne pouvant prendre en charge que du contenu texte, il est nécessaire d'utiliser un encodage pour pouvoir partager des fichiers de données, telles que des photos ou des videos. Comme la taille des messages est souvent limitée, des techniques complexes sont employées pour à la fois encoder et compresser les fichiers de données, puis les diffuser sous la forme de centaines voire de milliers de messages textes. Les messages sont alors téléchargés de manière séquentielle puis décodés.[258] Des moteurs de recherche tels que FTD ou des outils comme « nzb » sont ensuite fréquemment utilisés pour identifier ces messages et permettre à des logiciels spécialisés de les télécharger, de les réparer, et d'en décoder le contenu (il est fréquent que des messages soient perdus. Des mécanismes de réparation et de reconstitution de fichiers sont de fait utilisés pour diffuser de manière sécurisée des fichiers de grande taille sur Usenet).

Il est difficile de supprimer un contenu, sur le réseau Usenet, car les requêtes d'effacement (« *"cancel" requests* ») envoyées par un serveur à un autre sont souvent ignorées pour des raisons de sécurité. Bien que le protocole soit doté d'une option permettant d'effacer un message, aucun système ne permet de s'assurer que l'action a été prise en compte. Les messages (contenant les fichiers) binaires expirent généralement au bout d'un certain temps, qui oscille en principe entre 200 jours et un an. Après cette durée de conservation, ces messages font place aux nouveaux messages qu'envoit la communauté des utilisateurs. Pour cette raison, il est fréquent que des messages soient postés à nouveau après leur période de conservation initiale.

[258] Pour une description complète de ce processus, voir l'article de wikipedia, disponible en anglais à l'adresse suivante : http://en.wikipedia.org/wiki/Usenet#Binary_content.

5.3.5 Les réseaux de pair à pair (« *Peer-to-Peer* » ou P2P)

Depuis l'arrivée du système de partage de fichiers Napster en 1999, la technologie du partage de fichiers de « pair à pair » s'est développée très rapidement. Bien que cette technologie connaisse des usages légitimes, en particulier de la part des entreprises ayant besoin de transférer des fichiers de très grande taille, elle se prête très bien au partage sans droits de fichiers musicaux ou de films, générant ainsi des problèmatiques majeures pour les titulaires de droits d'auteur.



Le partage de fichiers de pair à pair est basé sur des échanges directs de fichiers entre les ordinateurs des utilisateurs finaux, sans passer par un serveur intermédiaire qui pourrait être susceptible d'introduire de la latence ou des erreurs de communication. Dans cet objectif, des logiciels ont été spécialement développés pour permettre l'indexation, la recherche et la récupération rapide des contenus disponibles sur le réseau P2P, lequel peut être constitué de dizaines de milliers, voire de millions d'utilisateurs simultanément connectés.

Au départ, des plateformes centralisées faisaient office d'intermédiaires pour la localisation et l'indexation des contenus. Cependant, ces dernières années (principalement à cause de la pression juridique excercée sur ces plateformes centralisées par les titulaires de droits d'auteur[259]), les progrès technologiques ont remédié à cette centralisation de la base de données, perçue comme un point de faiblesse, en permettant l'apparition de topologies de réseau décentralisé, distribué et permettant de rester complètement anonyme. Le terme « distribué » signifie que les fonctions de recherche de réseau et de recherche de contenus sont dispersées à travers une grande quantité d'ordinateurs personnels – appelés « pairs » (« *peers* »).

Les procotoles d'échange et de recherche de fichiers parmi l'ensemble des contenus disponibles ont des caractéristiques qui varient grandement de l'un à l'autre. Pour KaZaa (utilisant le protocole fasttrack) et eMule (utilisant le protocole gnutella), les requêtes réseau transitent par l'intermédiaire de connexions spécifiques entre certains clients. Tous les

[259] Voir, entre autres, à propos de Napster : (en anglais) http://en.wikipedia.org/wiki/Napster et http://news.findlaw.com/legalnews/lit/napster/ ; à propos de Kazaa : (en anglais) : http://en.wikipedia.org/wiki/Kazaa et http://news.bbc.co.uk/2/hi/technology/5220406.stm.

contenus sont publics, et il suffit d'être connecté au réseau pour observer un certain nombre des requêtes de connexion qui sont faites par d'autres pairs[260]. Chaque document ou fichier est découpé en un grand nombre de petits morceaux. Pour télécharger un fichier, il suffit alors d'envoyer de manière simultanée des requêtes de transfert pour chaque morceau à travers tout le réseau. Ceci permet d'accélérer les téléchargements tout en répartissant la charge sur l'ensemble des pairs connectés au réseau.

Pour d'autres protocoles comme BitTorrent, un traqueur (dont l'accès peut être limité à un groupe d'utilisateurs seulement, lorsque nécessaire) est utilisé de manière centralisée. Le traqueur a pour fonction de conserver l'état de disponibilité du contenu qui a été sollicité et de maintenir une liste des utilisateurs qui le proposent. Une source très connue de fichiers bittorents disponibles publiquement, qui référence ces traqueurs, est un site web appellé « The Pirate Bay ». Ce dernier fait actuellement l'objet d'une forte pression, exercée par les titulaires de droits d'auteur, car il répertorie un certain nombre de traqueurs qui conduisent à des ressources alléguées comme contrevenant à des droits d'auteur. Il a aussi récemment été impliqué dans plusieurs affaires de pédopornographie[261]. Beaucoup d'autres exemples de moteurs de recherche de traqueurs bitorrent opèrent aujourd'hui.

Dans Freenet, qui est un réseau de partage de fichiers très évolué, dont les connexions entre pairs sont chiffrées et anonymisées, la gestion de l'ensemble des contenus présents sur le réseau est répartie sur tous les pairs qui y sont connectés. Chaque pair maintient une copie, en local, d'une partie de cet ensemble. Le réseau fonctionne comme un système de fichiers indépendant, qui maintient, de manière automatique, un nombre suffisant de copies des contenus qui ont été publiés dans son enceinte. Cette circonstance, incidemment, rend la suppression de contenus encore plus difficile que dans le cadre des systèmes P2P classiques, en ce que les pairs eux-mêmes ne disposent d'aucune option simple qui leur permette d'effacer un contenu diffusé par l'intermédiaire de leur machine.

Au sommet de ce système de fichiers décentralisé et distribué, se greffe un mécanisme de chiffrement des communications entre les pairs, ainsi qu'un schéma d'adressage alternatif pour accéder au contenu du réseau. Un pair n'a donc aucune possibilité de savoir ce qui est stocké sur sa machine, ou qui utilise la bande passante de sa connexion internet et pour quelles raisons. En outre, les flux de partage de fichiers étant routés simultanément à travers plusieurs pairs pour assurer l'échange de fichiers qui est en cours (*routage par chemins multiples*), un très haut degré d'anonymat est garanti. Il est en pratique impossible de remonter au diffuseur initial d'un contenu.

Freenet a deux modes de fonctionnement, qui peuvent être utilisés, de manière optionnelle, simultanément. Dans le premier mode, le mode « *réseau ouvert* » (« *opennet* »), tous les pairs sont connectés les uns aux autres grâce à un mécanisme de découverte automatique. Cela signifie que n'importe quel pair peut se retrouver connecté à n'importe quel autre pair, en fonction du mécanisme de découverte. Dans le deuxième mode, le mode « *réseau fermé* » (« *darknet* »), la connexion se fait uniquement vers une liste prédéfinie d'amis, ce qui garantit encore encore plus d'anonymat. En tant que réseau à l'intérieur du réseau, Freenet est souvent considéré[262] comme étant le repère favori des extrémistes et des pédophiles. Il existe également d'autres systèmes similaires, tels que Entropy ou ANTsP2P.

---

[260] Voir par exemple Guillaume, Latapy et Le-Blond, « Statistical analysis of a P2P query graph based on degrees and their time-evolution » (« Analyse statistique d'un graphique des requêtes P2P, sur la base de leur nombre et de leur évolution dans le temps »), disponible en anglais à l'adresse suivante : http://hal.archives-ouvertes.fr/docs/00/05/45/86/PDF/guillaume04iwdc.pdf ; voir également le GAO des Etats-Unis, « The Use of Peer-to-Peer networks to access pornography » (« L'utilisation des réseaux de pair à pair pour accéder à des ressources pornographiques »), 2005, et « Peer-to-Peer Networks Provide Ready Access to Child Pornography » (« Les réseaux de pair à pair facilitent l'accès à la pédopornographie », 2003, respectivement disponibles en anglais aux adresses suivantes : http://www.gao.gov/new.items/d05634.pdf et http://www.gao.gov/new.items/d03351.pdf.

[261] Voir (en anglais) : http://www.theregister.co.uk/2007/09/03/another_pirate_bay_police_case/ ; M.J. Smith (ed.), *Child sexual abuse Issues and Challenges (Abus sexuel sur enfant problèmes et défis),* p.4.

Les dernières générations de logiciel de pair à pair optimisent la rapidité de réponse entre les hôtes. Pour ce faire, le réseau de pair à pair va donc favoriser les connexions entre utilisateurs proches et pouvant se trouver connectés sur le réseau d'un même FAI. Pour un filtrage efficace du trafic, il faudrait dès lors mettre en œuvre un filtrage local, y compris du trafic entre deux voisins, connectés au même équipement réseau (par exemple un switch ou un DSLAM). Ceci requerrait une infrastructure de filtrage décentralisée (ou, alternativement, impliquerait d'acheminer tout le trafic vers une plateforme de filtrage centrale) et aurait des impacts significatifs sur les réseaux des FAI et la façon dont ces réseaux sont architecturés.

Panorama du P2P

Logiciel	***Technologie (protocole)***	***Chiffrement***	***Anonymat***	***Distribué***	***Système de fichiers distribué***	***Partage privé***
Napster	Napster	Non	Faible	Non	Non	Non
KaZaa	Fasttrack	Non	Moyen	Oui	Non	Non
eMule	Gnutella	Non	Moyen	Oui	Non	Non
BitTorrent	BitTorrent	Non	Moyen	Oui	Non	Oui
Freenet	Freenet	Oui	Elevé	Oui	Oui	Oui

5.3.6 Les moteurs de recherche

Bien que les moteurs de recherche ne constituent pas principalement un moyen de distribution de contenus, il est important de reconnaître le rôle crucial qu'ils jouent dans le cadre des activités web quotidiennes. En indexant de manière automatique le contenu des sites web, ces services sont capables d'identifier les contenus pertinents grâce à des recherches par mots-clefs et à des algorithmes de recherche complexes. Google est l'un des moteurs de recherche les plus connus, notamment en raison de la forte part de marché qu'il a acquis dans le domaine.

Les mesures de filtrage d'Internet efficaces, qui utilisent des algorithmes d'analyse de mots-clefs aussi complexes, peuvent parfois être sujettes à des secrets industriels. En effet, elles emploient des méthodes très similaires à celles qui permettent de produire des résultats précis et pertinents dans le cadre des requêtes adressées aux moteurs de recherche ou dans le cadre des campagnes de publicité en ligne.

L'indexation des contenus par les moteurs de recherche passe par l'utilisation de technologies d'exploration du web, dites de « *web crawling* » (parmi d'autres méthodes). Le « web crawling » consiste en l'utilisation d'un logiciel, souvent appelé « robot », qui parcourt les serveurs DNS à la recherche de noms de domaine, puis les sites web associés à ces noms de domaine, en suivant chacun des liens qui y sont présents, afin d'indexer chaque page de contenus qu'il y trouve. L'index ainsi obtenu est ensuite utilisé pour répondre aux utilisateurs qui procèdent à la recherche de contenus spécifiques.

Ces techniques d'exploration du web peuvent créer des problèmes lorsque le moteur de recherche tente d'atteindre un contenu qui se trouve inclus dans une liste noire. Dans une telle situation, le système de filtrage redirige le robot d'indexation (le « *web-crawler* ») vers une page d'arrêt (« *stop page* ») avertissant de l'illégalité du contenu. Le robot d'indexation peut générer un grand nombre de requêtes de connexion (« *hits* ») sur cette page d'arrêt, alors même qu'aucun utilisateur réel n'a tenté d'y accéder.

5.3.7 La messagerie instantanée (« *IM* ») et autres outils

Un autre outil important à être utilisé dans le cadre d'échanges de ressources à caractère pédopornographique est la messagerie instantanée (IM).

Une étude suédoise datant de 2006 (Eneman 2006) montra que le réseau IRC, qui est une forme de messagerie instantanée qui repose sur un réseau de serveurs centraux, lesquels sont en charge de relayer les messages textes que s'échangent les utilisateurs, était la deuxième source de contenus véhiculant des abus sexuels sur enfants[263]. L'étude analysa 209 affaires judiciaires. Les mécanismes de partage de fichiers y étaient toutefois toujours combinés à des conversations textes, afin de permettre un échange efficace des contenus. Le canal de messagerie instantanée servait donc plus à la mise en relation et à la sécurisation de l'échange de ressources, tandis que ce dernier échange avait lieu directement par l'intermédiaire d'autres technologies.

Les systèmes IM récents tendent à permettre le partage de fichiers, en autorisant les utilisateurs à partager une partie de leur disque dur (cf. les dossiers partagés de MSN), voire en permettant à ces utilisateurs d'échanger des fichiers directement (les exemples sont encore MSN, AIM, Skype et beaucoup d'autres services). Les données qui seraient nécessaires à l'étude de l'utilisation de cette technologie à des fins de partage sont toutefois très rares.

Divers autres moyens numériques de transport et d'échange en ligne de contenus à caractère pédopornographique sont mentionnés dans les études qui concernent ce phénomène. Le plus important à relever, est que n'importe quel mécanisme de stockage de fichiers, tel que la sauvegarde en ligne (par exemple par le protocole FTP), les systèmes de disque dur en ligne (« *hard drive* »), ou même les comptes de messagerie web (où le système de messagerie est utilisé comme support de stockage plutôt que pour sa fonction messagerie), peut être utilisé pour transférer des fichiers entre deux personnes.

Les policiers enquêteurs confirment l'utilisation de ces systèmes dans des affaires de pédopornographie sur Internet[264]. L'incidence de ces transferts semble faible, à en juger par le nombre de plaintes et les résultats des enquêtes menées par la police. Cependant, ces statistiques peuvent être faussées par l'insuffisance des ressources investies dans les investigations liées à ce phénomène[265]. L'étude suédoise mentionnée plus haut semble également confirmer ce point.

Il est également possible d'utiliser des moyens de transmission directe (par exemple en utilisant des outils de webdiffusion - « *webcasts* » -, des cameras web - « *webcams* » -, ou des logiciels de messagerie instantanée permettant la communication vidéo), pour distribuer des ressources à caractère pédopornographique en temps réel[266].

---

[263] Voir Eneman, « A critical study of isp filtering of child pornography » (« Une étude critique du filtrage de la pédopornographie opéré par les FAI », 2006, p. 7, disponible à l'adresse suivante : http://is2.lse.ac.uk/asp/aspecis/20060154.pdf.

[264] Kaspersen, 2005, p. 7.

[265] Kaspersen, « Opsporing van kinderpornografie op internet een statusoverzicht » (« Investigations pénales relatives à la pédopornographie sur Internet, un état de la situation » -néerlandais), 2005, p. 7 ; Oosterink, Van Eijk, 2006, Ministère néerlandais de la Justice, La Haye.

[266] Wortly et Smallbone, « Child pornography on the internet » (« La pédopornographie sur Internet »), 2006, US DOJ COPS project (projet du Department of Justice des Etats-Unis, Office of Community Oriented Policing Services), disponible à l'adresse : http://www.cops.usdoj.gov/files/RIC/Publications/e04062000.pdf. Cet article mentionne une affaire de webdiffusion en temps réel, où les spectateurs pouvaient diriger l'acteur pour qu'il s'engage dans des relations sexuelles spécifiques avec un enfant, comme noté par Burke, A., S. Sowerbutts, B. Blundell, et M. Sherry dans leur article « Child Pornography and the Internet: Policing and Treatment Issues » (« La pédopornographie et Internet : problématiques de maintien de l'ordre et de soins »), 2002, in *Psychiatry, Psychology and Law* (*Psychiatrie, psychologie et droit*), 9(1):79–4.

5.4 Les stratégies de filtrage et leur efficacité

5.4.1 Introduction

La présente section analyse les stratégies de filtrage pour chaque média de diffusion. Bien que de nombreuses possibilités existent en la matière, l'analyse se concentrera sur les scénarios réalistes qui sont connus pour être déployés en pratique.

Remarque : cette analyse ne détaillera pas les logiciels de filtrage pour postes clients, utilisés par les internautes eux-mêmes. En effet, il est peu pertinent de discuter de l'impact de ce type de logiciels sur la démocratie ou sur l'ordre public (dans la mesure où c'est l'utilisateur lui-même qui choisit de limiter son propre comportement de navigation sur Internet). Par ailleurs, ces logiciels sont peu transparents (ce sont des logiciels propriétaires), et ils présentent peu d'aspects communs en termes de conception et d'objectifs.

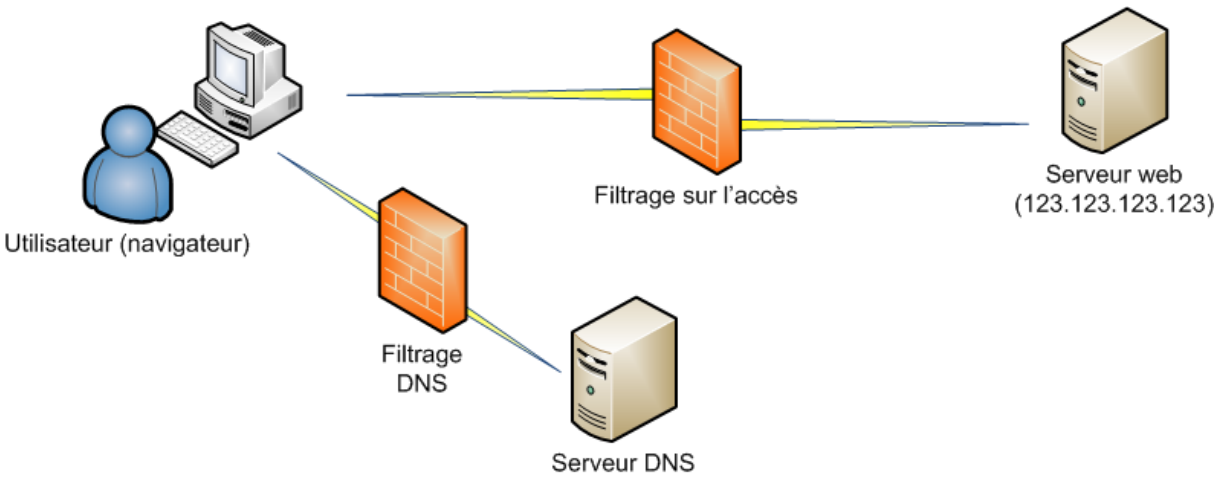
5.4.2 Le filtrage de sites web

Les sites web constituent généralement la première cible des tentatives de filtrage – particulièrement en ce qui concerne les ressources à caractère pédopornographique. Les sites web sont en effet un média très utilisé pour l'échange de ce type de contenus. Ils sont accessibles et sont souvent le terrain d'activité des pédophiles potentiels qui sont à la recherche de contenus à caractère pédopornographique.

Le filtrage dynamique n'est généralement pas envisagé, en raison de la nature visuelle de la plupart des ressources à caractère pédopornographique. Il est dès lors difficile, pour les systèmes de reconnaissance automatique, de les reconnaître efficacement. D'intenses recherches techniques sont menées dans le but de trouver une méthode de reconnaissance, par les machines, des contenus à caractère pédopornographique, mais ces méthodes sont encore insuffisamment fiables et efficaces pour qu'il soit utile de les commenter. D'un autre côté, la méthode consistant à analyser uniquement le texte des sites web à la recherche de mots-clefs est en proie à des techniques d'évasion faciles à mettre en œuvre (telles que le fait de ne pas employer les mots-clefs déclenchant le filtrage, tout en faisant la promotion du contenu concerné sur des canaux différents, ou de modifier l'orthographe de ces mots).

Il est donc généralement procédé au filtrage des sites web en utilisant l'un des deux identificateurs suivants :

- Premièrement, le serveur qui contient le contenu du site web pourrait être bloqué au niveau de son adresse IP, empêchant dès lors toute personne qui se verrait appliquer le filtre d'accéder à cette adresse. La liste noire ne contiendrait, dans cette situation, que les adresses IP de contenus identifiés comme étant illégaux.
- Deuxièmement, une mesure de filtrage peut être basée sur le nom de domaine, voire sur l'URL spécifique d'une page ou d'un fichier qui se trouve hébergé sur un site web. L'URL (remarque : un nom de domaine est une forme d'URL) est incluse dans chaque requête d'accès adressée à un serveur web. Dès lors, l'examen de chaque requête, généralement par l'intermédiaire de serveurs proxy, serait nécessaire pour identifier les URL concernées au sein du trafic web généré par les utilisateurs. Ces requêtes seraient alors comparées à la liste noire d'URL, et bloquées lorsqu'une correspondance serait trouvée.

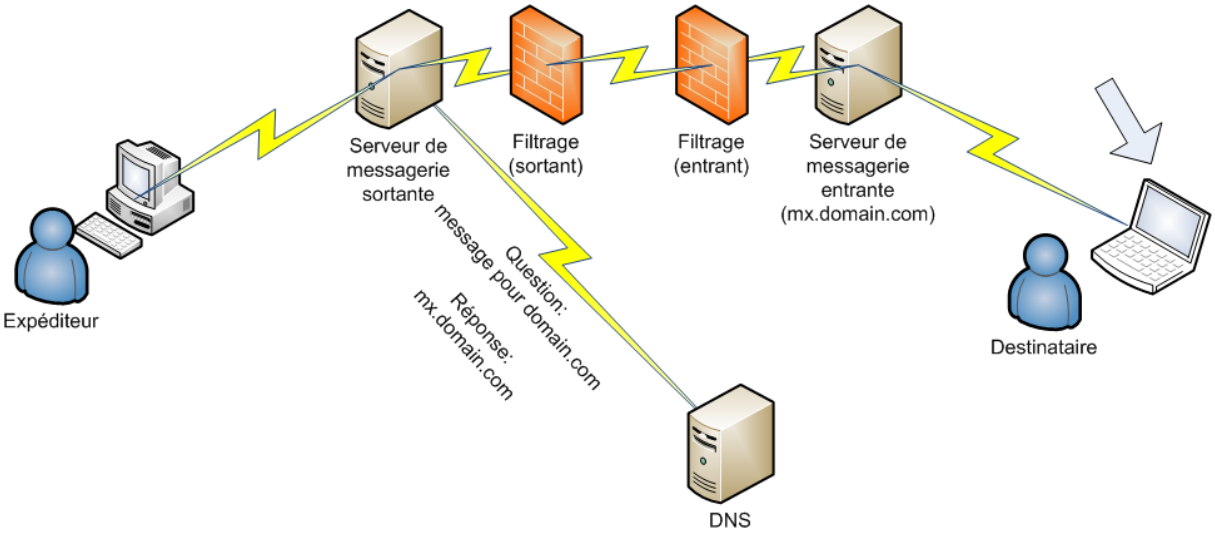


Il est important de noter que la tentative de filtrage peut être faite tant sur le chemin qui relie l'utilisateur au serveur distant (sur le réseau d'accès), que sur le chemin qui relie l'utilisateur au service DNS.

Dans le premier cas, si ce type de filtrage est mis en place au niveau du réseau d'accès et non pas sur l'ordinateur de l'utilisateur, ce dernier aura alors, toutes proportions gardées, plus de mal à le contourner, car il lui sera nécessaire d'avoir un minimum de connaissances sur le fonctionnement d'Internet. Lorsque le filtrage du trafic entrant ou sortant du serveur web distant est effectué sur le chemin qui conduit à ce dernier, l'utilisateur ne peut contourner la mesure que s'il trouve un moyen détourné d'accéder à ce site web distant.

5.4.3 Le filtrage de la messagerie électronique (« *Email Blocking* »)

Le filtrage de la messagerie électronique est une pratique répandue, en raison du volume important de spam qui traverse Internet. La plupart des filtres de messagerie électronique sont situés sur les serveurs de messagerie entrante, qui recoivent les messages électroniques à destination de leurs utilisateurs, ou sur des serveurs positionnés juste devant eux sur le réseau. Selon les configurations, la machine sur laquelle se trouve le serveur de messagerie ou une autre machine peut être en charge du filtrage. Ce type de filtrage est presque toujours mis en place avec le consentement explicite et préalable de l'utilisateur de la messagerie concernée, et est un service offert par le prestataire de service pour améliorer la qualité du service de messagerie électronique qu'il propose.



Souvent, les prestataires de services Internet mettent en œuvre un filtrage sur la messagerie sortante afin d'éviter que leurs serveurs ne soient utilisés pour diffuser du spam et autres sortes de messages non souhaités[267].

De manière générale, il existe deux manières de procéder à un filtrage de la messagerie électronique. En premier lieu, des filtres basés sur les connexions peuvent comparer l'adresse IP du serveur expéditeur des messages au contenu d'un certain nombre de listes noires. Ces listes sont généralement maintenues par des éditeurs d'anti-spam ou d'antivirus, ou par d'autres organisations qui s'attachent à collecter les adresses IP impliquées dans une activité de spam. En fonction de la configuration du filtre, soit les messages seront étiquetés (par exemple, une étiquette - « *tag* » - telle que « [SPAM] » sera ajoutée dans le sujet du message), soit les demandes de connexion provenant de serveurs dont l'adresse IP est contenue dans une liste noire seront ignorées.

En second lieu, des filtres peuvent identifier les messages non souhaités en s'attachant au contenu de ces derniers. Dans cet objectif, certaines listes noires répertorient les URL qui apparaissent dans le corps de certains spams. La présence d'une URL illégale connue dans un message peut alors conduire ce message à être filtré.

Alternativement, des mots-clefs ainsi que d'autres caractéristiques liées aux contenus peuvent être employés pour filtrer dynamiquement les messages. Le filtrage dynamique de la pédopornographie est toutefois difficile, lorsque le contenu du message ne comprend pas de mots-clefs explicites (comme « lolita » ou « preteen », ce dernier signifiant « préadolescent »), ou d'URL connue pour faire la promotion de ce type de contenus. Le filtrage des images est notamment très difficile et consommateur de ressources, lorsqu'il n'est

[267] ENISA spam study (étude de l'ENISA sur le spam), 2007 p. 6, disponible à l'adresse : http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf.

pas quasiment impossible, compte tenu de l'immense quantité de messages électroniques impliqués[268].

La stratégie ayant le plus de chances de succès semble dès lors être celle qui se base sur les URL contenues dans les messages. Elle doit toutefois être accompagnée d'efforts de qualification du contenu des sites web qui se voient ainsi promus dans le corps des messages électroniques. Dans la mesure où les listes d'URL utilisées en matière de filtrage de la messagerie électronique sont similaires aux listes noires utilisées dans le cadre du filtrage de sites web, ces dernières pourraient constituer une première base de travail pour la conception des premières, et éviter par là-même des duplications d'efforts. Ceci étant dit, il est tout à fait possible que des spammeurs transmettent des URL différentes, dans le cadre de leurs campagnes de spam. En conséquence, l'héritage d'une telle initiative pourrait être une surveillance de plus en plus généralisée des messages électroniques, en raison des fréquents changements de stratégie des spammeurs. La mesure n'atteindrait dès lors pas l'objectif qui a motivé sa mise en œuvre.

L'analyse des pièces jointes aux messages pourrait être effectuée en utilisant la signature des ressources à caractère pédopornographique qui sont déjà connues (les considérations juridiques faisant l'objet d'une analyse séparée au chapitre 6). Cette analyse pourrait permettre d'identifier les messages entrant à caractère pédopornographique, mais également de prévenir l'envoi de messages de cette même nature, si la technologie était appliquée au trafic de messagerie sortante. Plus particulièrement, le filtrage des messages sortants offre l'opportunité supplémentaire de permettre de procéder à l'identification des utilisateurs qui diffusent des contenus à caractère pédopornographique sur le réseau, voire de communiquer leurs coordonnées aux services en charge de l'application de la loi. Ceci dit, en raison de la grande incidence des logiciels malveillants, il est probable que cette méthode génère un grand nombre de faux-positifs, avec toutes les conséquences que cela peut impliquer[269]. Dans la mesure où les fournisseurs d'accès à Internet sont souvent considérés comme étant de « simples transporteurs », à l'instar des services postaux ou des opérateurs téléphoniques, et qu'ils ne sont soumis à aucune obligation de surveiller[270] le trafic sur leur réseau, s'engager dans une telle activité pourrait sembler contraire à leurs intérêts commerciaux et conduirait probablement à des demandes de rechercher, dans les messages électroniques des utilisateurs de leurs services, des contenus d'une autre nature, tels que des infractions aux droits d'auteur. En effet, il existe également des raisons juridiques qui expliquent la raison pour laquelle les prestataires de services Internet n'ont pas la permission de lire les messages électroniques, pas plus que l'on ne s'attend à ce que les services postaux lisent tous les courriers qui sont envoyés par leur intermédiaire.

Les infrastructures nécessaires au filtrage de la messagerie électronique sont, souvent, déjà en place, du fait du fort volume de spam et de l'important taux de pénétration des filtres anti-spam[271]. Le coût incrémental du filtrage des contenus à caractère pédopornographique présents dans les messages électroniques serait donc potentiellement plus faible que ne le serait celui du filtrage de ces mêmes contenus lorsqu'ils sont hébergés sur des sites web, puisqu'il suffirait d'implémenter des listes noires additionnelles dans les systèmes de filtrage déjà en place.

En termes d'efficacité, le filtrage des messages électroniques peut être considéré comme relativement efficace si sont utilisées des listes noires appropriées. Cependant, les recherches préalables à la présente étude n'ont apporté aucun élément de nature à démontrer l'efficacité

[268] Voir supra, sous-section 5.2.3.2.
[269] AOL est le seul prestataire de services, à la connaissance des auteurs de publications sur le sujet, à filtrer les pièces à caractère pédosexuel qui sont attachées aux messages électroniques, en utilisant une base de données de valeurs de hachage. Voir le témoignage de John D. Ryan de AOL devant le Sénat Américain en 2006, disponible en anglais à l'adresse suivante : http://archives.energycommerce.house.gov/reparchives/108/Hearings/06272006hearing1954/Ryan.pdf.
[270] Voir infra, la sous-section 6.8.2 de la présente étude.
[271] ENISA spam study (étude de l'ENISA sur le spam), 2007, disponible à l'adresse : http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf.

du filtrage des contenus à caractère pédopornographique par les filtres anti-spam actuellement en place. En conséquence, il est actuellement impossible d'estimer si les coûts de mise en œuvre d'un système permettant ce type de filtrage seraient proportionnés au problème, en prenant en compte, également, qu'un tel mécanisme pourrait être considéré comme consistant en une surveillance généralisée des communications privées, laquelle, à son tour, pourrait être considérée comme inacceptable, quelle que soit l'efficacité du mécanisme. Voir à ce sujet le chapitre 6 de la présente étude.

Une possibilité de sur-blocage existe, lorsque sont bloquées des adresses IP, voire lorsque sont bloqués des serveurs entiers de messagerie expéditeurs, en raison d'incidents liés à des contenus à caractère pédopornographique. De la même façon que pour le contenu web, le filtrage de l'ensemble des messages provenant d'un réseau ou d'une adresse IP peut conduire au filtrage d'autres services et usages, légitimes (ainsi, peuvent être bloqués d'autres utilisateurs du même serveur de messagerie à la même adresse, ou même l'ensemble des utilisateurs d'un nom de domaine, comme dans l'exemple mentionné plus haut). Une telle situation est déjà arrivée à plusieurs reprises, dans le cadre du filtrage du spam de manière plus générale [272].

Aucune initiative en matière de filtrage de la messagerie électronique n'a été observée dans les pays qui ont récemment entrepris de filtrer le web[273].

[272] A comparer, à titre d'exemple (en anglais) : http://www.wired.com/techbiz/media/news/2005/01/66226.
[273] Voir la section 4.4 de la présente étude.

5.4.4 Le filtrage des contenus sur le réseau Usenet

Les tentatives de filtrage de contenus sur Usenet sont traditionnellement opérées en bloquant l'accès à des sous-parties d'un groupe, ou en refusant d'héberger un groupe de news en particulier[274]. Généralement, les prestataires de services Internet qui opèrent des serveurs Usenet refusent d'héberger des groupes dont le nom est explicite, tel que « `alt.exemple.binaries.preteen` ». L'existence de sur-blocage (ou filtrage excessif) est souvent mentionnée en la matière, en ce que de nombreux prestataires de services semblent avoir fait l'objet de pressions telles que celles exercées par le Procureur Général de New York, M. Cuomo[275], qui décrit Usenet comme étant le moyen principal de diffusion de contenus à caractère pédosexuel, malgré des preuves suggérant que le problème n'est pas plus important sur ce média qu'il ne l'est sur les autres médias Internet.

A titre d'exemple, AT&T a arrêté son service Usenet après avoir eu affaire au Procureur Général de New York. Incapable de surveiller efficacement le contenu des groupes de news qu'il proposait aux utilisateurs de ses services, AT&T redirige à présent ses abonnés vers d'autres fournisseurs de news, qui, incidemment, permettent souvent un accès non filtré à bien plus de groupes, dont les durées de conservation sont plus longues[276]. Au final, il peut être dit que l'initiative a conduit à la disponibilité de plus nombreux contenus à caractère pédopornographique, pour de plus nombreux utilisateurs, et pour plus longtemps que ce n'était le cas initialement.

Contrairement au filtrage de la messagerie électronique, dont les messages sont limités en taille, le filtrage des messages postés sur les groupes de news est plus difficile car les fichiers binaires sont souvent découpés et éparpillés dans un grand nombre de messages en utilisant des techniques d'encodage. En pratique, cela signifie que seule la fermeture d'une partie de la hiérarchie Usenet sur leurs propres serveurs peut permettre aux prestataires de services Internet d'avoir une influence positive sur la diffusion de contenus à caractère pédosexuel sur Usenet.

Comme le montre cet exemple, le sur-blocage est une préoccupation majeure. La pratique du filtrage de groupes entiers, ou bien même d'arborescences de groupes, conduit à filtrer un grand nombre de discussions innocentes. Après que Verizon [l'un des principaux opérateurs de télécommunications américains, *ndlt*] ait arrêté de relayer l'arborescence alt.* (où * désigne tous les groupes hébergés sous l'arborescence « alt. »), un lecteur de Cnet a été cité comme ayant déclaré, à titre d'exemple, que « *ceci est ridicule. J'ai à vrai dire rencontré ma femme sur* `alt.personals` *il y a 14 ans… J'utilise toujours Usenet – Il y a énormément de discussions intéressantes et on peut y trouver des réponses à des questions concernant des sujets spécifiques très rapidement. C'est bien d'avoir un lieu de discussion décentralisé, dont la bonne gestion ne dépend pas d'un administrateur système comme dans un forum, un lieu sans images clignotantes et publicités en flash* »[277].

Bien que les fournisseurs d'accès à Internet ne communiquent généralement pas ouvertement sur le sujet, ils ont pu observer en interne que, lorsqu'ils sont privés d'accès à des arborescences suspectes, les utilisateurs ont tendance à déplacer leurs contenus illégaux vers

---

[274] Voir un exemple de sur-blocage lors duquel toute la hiérarchie alt.* a été filtrée par Verizon : « alt.blocked: Verizon blocks access to whole USENET hierarchy » (« alt. filtré : Verizon bloque l'accès à toute la hiérarchie USENET », disponible sur Ars Technica, à l'adresse : http://arstechnica.com/old/content/2008/06/alt-blocked-verizon-blocks-access-to-whole-usenet-hierarchy.ars.

[275] Voir EFF, Jennifer Granick, « More ISPs decide to Filter Usenet Newsgroups » (« De plus nombreux prestataires de services Internet décident de filtrer les groupes de news sur Usenet »), 2008, disponible à l'adresse : http://www.eff.org/deeplinks/2008/07/more-isps-decide-filter-usenet-newsgroups.

[276] Voir (en anglais) http://my.att.net/NewsGroup, commentaire parmi d'autres de l'article http://www.zeropaid.com/news/86599/att-quits-free-usenet-access-july-15th/. D'autres services payants semblables à Supernews, Giganews et Usenet.com pourraient apparaître.

[277] Traduit de l'anglais. Voir « Verizon offers details of Usenet deletion: alt.* groups, others gone » (« Verizon donne des détails sur les suppressions relatives à Usenet : les groupes alt.*, et d'autres disparus »), http://news.cnet.com/8301-13578_3-9967119-38.html.

des groupes dont le nom est moins explicite, ce qui conduit à un plus grand nombre d'incidents, en termes d'accès involontaire à des ressources illégales.

5.4.5 Le filtrage des résultats des moteurs de recherche

Afin d'empêcher les utilisateurs d'accéder à des contenus illégaux, il est possible de prévenir l'accès à des résultats de moteurs de recherche au niveau des prestataires de ces moteurs. Un fournisseur comme Google, par exemple, pourrait décider de filtrer toutes les requêtes pour un mot-clef tel que « pédopornographie ».

Une telle initiative conduirait immanquablement à du sur-blocage (ou filtrage excessif), car, d'un point de vue général, toutes les apparitions de ce mot-clef sur Internet ne sont pas illégales. Afin de juger si le filtrage des résultats doit ou non être mis en place, une étude plus détaillée du contexte, qu'il est difficile d'automatiser, serait nécessaire. Alternativement, il pourrait être procédé à une analyse humaine des contenus suspects, qui seraient identifiés dans le cadre de recherches par mots-clefs. Mais une telle entreprise aurait un coût très élévé, compte tenu des milliards de pages indexées qu'il s'agirait d'analyser manuellement.

Une autre question importante est celle de la visibilité qui est donnée aux initiatives de filtrage des résultats des moteurs de recherche. Certains prestataires informent clairement de l'existence d'un tel filtrage des résultats, tandis que d'autres ne le font pas[278].

Enfin, le contournement de ce type de filtrage est facile : il suffit d'accéder directement au contenu. Bien qu'un contenu non répertorié ne soit pas si facile à trouver pour un nouvel utilisateur, l'échange d'URL entre utilisateurs, de manière directe ou par l'intermédiaire de sites web ou de canaux dédiés de messagerie instantanée, permet d'arriver au même résultat : un contournement facile de la mesure de filtrage.

[278] Nous avons découvert que la version néerlandaise d'ask.com indiquait clairement qu'un filtrage sur les résultats était en place pour les requêtes de contenus à caractère pédopornographique. La version en langue anglaise (pour les Etat-Unis) ne comporte pas cette mention. Google n'indique pas non plus si le résultat des recherches a été filtré.

5.4.6 Le filtrage du pair à pair (« peer-to-peer » ou P2P) et de la messagerie instantanée

Tenter de filtrer le trafic pair à pair est une tâche difficile lorsque l'initiative n'est pas entreprise au niveau de l'utilisateur. Outre le fait qu'une partie du trafic est chiffrée, il peut être difficile de dissocier sur le réseau, d'un point de vue technique, le trafic P2P de celui de la messagerie instantanée. Beaucoup de protocoles P2P sont distribués – ce qui signifie que les fichiers y sont téléchargés par fragments provenant de plusieurs sources et qu'aucun des flux de données ne contient l'intégralité du fichier. Pour rendre les choses encore plus complexes, des mécanismes permettent de changer les ports réseau qui sont utilisés, ces ports servant normalement à différencier les catégories de trafic (tels que le trafic web, email ou des serveurs de news).

Les échanges de fichiers de pair à pair fonctionnent de manière indépendante des schémas d'adressage classiques d'Internet. Il n'y existe pas de conventions centralisées relatives à l'identification des contenus, à l'exception de l'utilisation des adresses IP et de ce qui concerne les fonctions de recherche et de téléchargement que comprennent les applications P2P qu'utilisent les internautes.

- La première option permettant le filtrage des contenus sur un réseau P2P, consiste à analyser ces contenus en se comportant comme un utilisateur du service. En émettant une requête pour certains fichiers, ou en surveillant les requêtes et les réponses qui leur sont apportées par d'autres utilisateurs, il est possible de trouver des utilisateurs ayant une partie d'un fichier donné sur leur disque dur. Bloquer l'accès à leur adresse IP ou déconnecter ces utilisateurs, toutefois, est le seul remède disponible. Dans la mesure où les contenus sont très largement répandus, de manière internationale et sur plusieurs réseaux, la disponibilité du contenu concerné n'en sera probablement pas affectée si de nombreux pays et prestataires de services Internet ne coopèrent pas dans le cadre d'une initiative concertée. En outre, récupérer ces fichiers en vue d'une analyse humaine ou pour comparer leur signature à celles, basées sur le hachage, d'une base de données, est très consommateur de ressources.

- La deuxième option permettant de filtrer les contenus sur ces réseaux, avec un maximum d'efficacité, consiste à utiliser une technologie apparentée à celles qui permettent l'analyse approfondie des paquets (« *Deep Packet Inspection* » ou DPI), [autrement dit du trafic réseau, *ndlt*], pour reconnaître les fichiers échangés pendant le temps de leur échange, voire identifier les paquets (trafic P2P) utilisés pour partager ces fichiers. Cette opération implique que le trafic soit entièrement routé vers un système central d'analyse (DPI), et nécessite des efforts importants pour reconstituer, afin de le classifier, le contenu qui arrive en différents morceaux des réseaux P2P distribués. Afin de réduire la charge de trafic sur le système d'analyse DPI, une alternative pourrait consister à calculer les signatures des morceaux constituant les fichiers [et à baser le filtrage sur les signatures de ces morceaux, *ndlt*]. Toutefois, cela conduirait à la constitution d'une liste noire bien plus importante, et à des processus de vérification des concordances très consommateurs de ressources (il s'agirait d'identifier les différentes parties d'un fichier, puis de les faire concorder, ce qui n'est pas aussi simple que de procéder au hachage d'un fichier entier).

  Compte tenu des connexions à haut débit actuelles, cette stratégie de filtrage impliquerait des investissements collossaux afin d'analyser le trafic sans trop impacter la qualité des connexions concernées par la mesure. Elle conduirait également à une intrusion majeure dans la confidentialité des communications des utilisateurs finaux, alors que seule une infime partie de l'ensemble du trafic analysé contiendrait le contenu illégal recherché.

  Mettre en œuvre un système DPI constitue un investissement important. Par ailleurs, procéder au filtrage des contenus P2P pour y trouver des fichiers spécifiques implique un

travail conséquent de classification de tout le contenu en ligne. En outre, le risque de sous-blocage (ou blocage insuffisant) semble omniprésent, compte tenu de l'immense quantité de données échangées sur les réseaux P2P de nos jours.

En raison de ces difficultés techniques, les fournisseurs d'accès à Internet et les organisations privées font l'objet d'une pression visant à ce qu'ils filtrent l'ensemble du trafic P2P. Il en résulterait un sur-blocage (ou filtrage excessif) significatif. Le contournement de ce type de technologies n'est pas simple, mais, encore une fois, l'usage de tunnels ou de proxys pourrait bien conduire au contournement efficace de la plupart des mesures de filtrage impliquant un système DPI[279]. Le chiffrement des échanges des fragments de fichiers est également un moyen efficace de contourner une stratégie de filtrage DPI. Des réseaux de pair à pair (« *peer to peer* ») tels que Freenet chiffrent déjà les transferts de fichiers, dans le cadre d'un système de distribution qui laisse une large place à la possibilité de nier plausiblement sa responsabilité, dans l'hypothèse où l'un des pairs serait accusé d'avoir été impliqué dans la diffusion de contenus illégaux.

Des problèmes similaires sont rencontrés dans le cadre des réseaux de messagerie instantanée. Même si les échanges de fichiers y sont plus faciles à identifier, puisqu'ils sont opérés par l'application de messagerie instantanée, dont l'architecture logicielle est généralement centralisée et non distribuée, router l'ensemble de ces échanges vers une infrastructure centrale représenterait un investissement conséquent. Souvent, dès lors, les programmes de messagerie instantanée vont autoriser l'échange direct de fichiers entre deux pairs du réseau de messagerie, ce qui contrarie tout scénario de filtrage centralisé (basé sur des signatures).

Compte tenu de ces défis techniques, les chances de filtrer efficacement les contenus à caractère pédopornographique sur les réseaux P2P et de messagerie instantanée, sans utiliser une technologie de type DPI, paraissent faibles. L'utilisation de cette technologie, en outre, pourrait conduire à une intrusion significative dans la confidentialité des communications de l'ensemble des utilisateurs d'Internet et nécessiterait des investissements colossaux.

[279] The Pirate bay (un site web de torrents très connu) a son propre service VPN ("Ipredator"). Voir l'article disponible en anglais à l'adresse : http://www.wired.com/threatlevel/2009/06/ipredator/.

5.4.7 Vue d'ensemble

Le tableau ci-dessous offre une vue d'ensemble des discussions précédentes. Il liste les caractéristiques de chacune des stratégies de filtrage qui ont été abordées dans leur cadre. Il montre les risques que présentent ces stratégies, selon nos estimations, en termes de sur-blocage (ou filtrage excessif) et de sous-blocage (ou filtrage insuffisant), et met en relief les ressources nécessaires à l'exécution de chaque stratégie de filtrage.

Il fait encore état des différents types de listes noires (« *block-list* ») et des efforts de maintenance qui sont nécessaires pour chacune de ces listes. Dans sa dernière colonne, il indique pour chaque stratégie si le contenu des communications doit être analysé de manière approfondie (avec une technologie DPI, autrement dit d'inspection approfondie des paquets, ou une technologie équivalente), pour que le filtrage soit efficace.

Média	**Filtrage**	**Efficacité**				**Liste noire (« *Blocklist* »)**		**DPI**
		SUR-blocage (ou filtrage EXCESSIF)	*SOUS-blocage (ou filtrage INSUFFISANT)*	*Ressources requises*	*Contournement*	*Effort de maintenance*	*Identificateur*	
Web	*DNS*	**TRÈS PROBABLE**	**PROBABLE**	**FAIBLES**	**FACILE**	**MOYEN**	Nom de domaine	-
	Domaine	**TRÈS PROBABLE**	**PROBABLE**	**MOYENNES**	**MOYEN**	**MOYEN**	Adresse IP du nom de domaine	-
	URL	**PEU PROBABLE**	**TRÈS PROBABLE**	**MOYENNES**	**MOYEN**	**ÉLEVÉ**	URL	+
	IP	**TRÈS PROBABLE**	**PROBABLE**	**FAIBLES**	**MOYEN**	**MOYEN**	Adresse IP	-
	Dynamique	**TRÈS PROBABLE**	**TRÈS PROBABLE**	**ÉLEVÉES**	**MOYEN**	**FAIBLE**	Mots-clefs, technologie de reconnaissance d'image et autres	+
	Signatures	**PEU PROBABLE**	**TRÈS PROBABLE**	**ÉLEVÉES**	**MOYEN**	**ÉLEVÉ**	Hachage	+
	Hybride (IP+signature /URL)	**PEU PROBABLE**	**TRÈS PROBABLE**	**MOYENNES**	**MOYEN**	**ÉLEVÉ**	IP et hachage ou URL	+
E-mail	*Dynamique*	**PROBABLE**	**PROBABLE**	**MOYENNES**	**DIFFICILE**	**FAIBLE**	Mots-clefs ou autres	-
	URL	**PROBABLE**	**PROBABLE**	**MOYENNES**	**DIFFICILE**	**ÉLEVÉ**	URL	-
	Adresse IP	**TRÈS PROBABLE**	**PROBABLE**	**MOYENNES**	**DIFFICILE**	**ÉLEVÉ**	Adresse IP	-
	Signatures	**PEU PROBABLE**	**PROBABLE**	**ÉLEVÉES**	**DIFFICILE**	**ÉLEVÉ**	Hachage	+
Usenet	*Par groupe*	**PROBABLE**	**PROBABLE**	**FAIBLES**	**FACILE**	**FAIBLE**	Nom du groupe	-
	Par hiérarchie	**TRÈS PROBABLE**	**PEU PROBABLE**	**FAIBLES**	**FACILE**	**FAIBLE**	Hiérarchie du groupe	-
Moteur de recherche	*Mot-clef*	**TRÈS PROBABLE**	**TRÈS PROBABLE**	**ÉLEVÉES**	**FACILE**	**MOYEN**	Mots-clefs	-
P2P	*Par protocole*	**TRÈS PROBABLE**	**PEU PROBABLE**	**MOYENNES**	**DIFFICILE**	**FAIBLE**	Reconnaissance de protocole	+
	Par fichier (signature)	**PEU PROBABLE**	**TRÈS PROBABLE**	**ÉLEVÉES**	**DIFFICILE**	**ÉLEVÉ**	Hachage	+
	Par fichier (dynamique)	**PROBABLE**	**TRÈS PROBABLE**	**TRÈS ÉLEVÉES**	**DIFFICILE**	**FAIBLE**	Algorithmes évolués	+

5.4.8 Conclusion

Bien que les méthodes de distribution de contenus qui ont été discutées dans le présent chapitre présentent des différences sensibles, il est important de noter que les contenus, ciblés par notre étude, qui sont diffusés par leur intermédiaire, demeurent les mêmes. Il s'agit de fichiers photos ou vidéos, qui sont les principales cibles du filtrage de contenus à caractère pédopornographique. Cela signifie qu'en pratique, même si ces méthodes de distribution peuvent varier, chacune d'entre elles peut se substituer aux autres. Indépendamment de l'efficacité du filtrage d'un contenu sur un média, toute faiblesse que rencontrerait une mesure de filtrage appliquée au même contenu sur un autre média conduirait probablement à un changement de la méthode de distribution de ce contenu.

La majorité des activités liées à la pédopornographie, sur Internet, fait aujourd'hui intervenir de multiples services et systèmes électroniques. Dans le cadre de plusieurs affaires ayant fait l'objet d'investigations, le contact entre un adulte et un enfant avait été initié dans des salons publics de discussion, puis s'était déplacé vers des salons privés de discussion, pour continuer sa progression par l'intermédiaire de messages électroniques et de textes SMS (« Short Messaging Service ») échangés sur les réseaux mobiles. Le rendez-vous physique final y avait été arrangé par la voie d'appels personnels sur téléphone mobile. Mener une enquête sur de telles activités est une réelle gageure et exige de la part des enquêteurs une connaissance très large de tous les aspects des technologies Internet et des télécommunications.

Ainsi, il est probable que les efforts mis en œuvre en vue de filtrer les médias publics tels que les sites web ou le spam conduiront à un départ des utilisateurs vers des plateformes plus à l'abri des regards tels que les réseaux privés virtuels (« *darknet* ») de partage de fichiers P2P, ou à des partages de fichiers en direct (dans les communautés IM dans lesquelles l'entrée doit être approuvée – « *vetted IM community* »). D'un point de vue technique, si les utilisateurs n'ont aucune inhibition (technique ou morale), les mêmes fonctionnalités de partage de fichiers peuvent être mises en œuvre dans ces communautés, vraisemblablement avec davantage de chiffrement et d'anonymisation du processus de partage. Il s'agit d'un aspect crucial qui doit entrer en considération, lors de l'évaluation de l'objectif et de la proportionnalité de toute initiative donnée de filtrage.

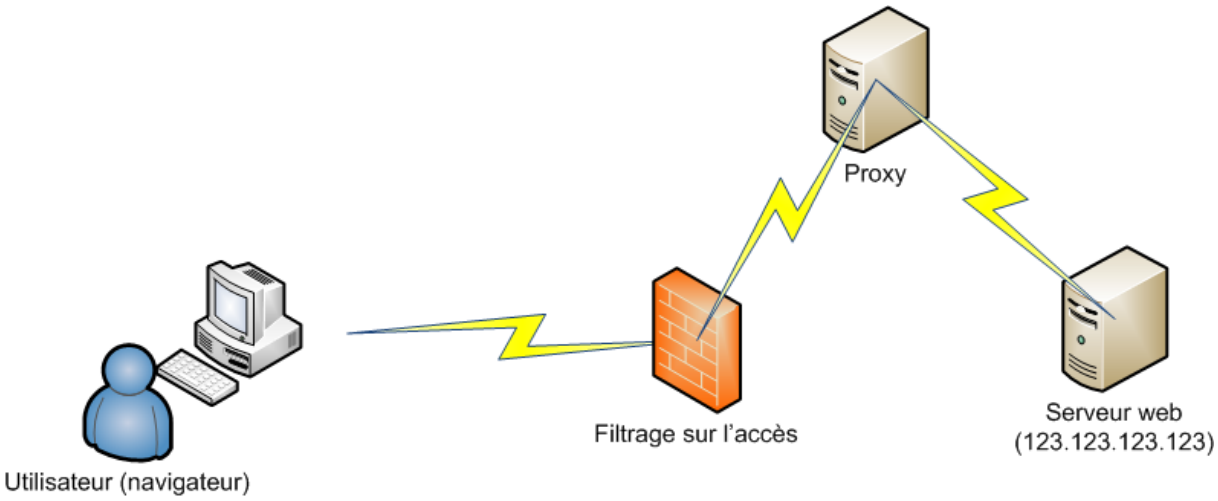
5.5 Contourner le filtrage d'Internet

5.5.1 Les serveurs proxy

Contourner une mesure de filtrage mise en place au niveau de serveurs proxy est assez simple si l'utilisateur peut utiliser les services d'un serveur proxy externe (c'est-à-dire d'une machine externe au réseau de son FAI ou de son entreprise, voire hors du pays). L'utilisation des serveurs proxy est très fréquente, et la plupart des fournisseurs d'accès à Internet en ont installés sur leur réseau.

Le but d'un serveur proxy est d'accepter les requêtes que formulent les utilisateurs pour accéder à des pages web, de collecter le contenu du site web distant concerné pour le transmettre à l'utilisateur qui l'a requis et, optionnellement, de conserver localement ce contenu dans un cache. Lorsqu'un autre utilisateur souhaitera accéder à ce même contenu, ce dernier sera alors disponible localement [et plus rapidement, *ndlt*]. Pour contourner directement une mesure de filtrage de l'accès, un utilisateur peut demander à un proxy externe d'accéder pour lui au contenu filtré. Il pourra ainsi accéder au site concerné en se libérant des contraintes du filtrage local, aussi longtemps que ce serveur proxy externe ne fera pas lui-même l'objet d'une mesure de filtrage.

La configuration d'un navigateur web pour utiliser un serveur proxy externe, afin d'obtenir le contenu souhaité, est très simple à réaliser et certains logiciels permettent même de le faire automatiquement.



Un grand nombre de serveurs proxy permettant de conserver son anonymat sont disponibles sur Internet – certains sont gratuits, d'autres payants. Un serveur proxy d'anonymisation ne donne aucune information au site distant sur l'auteur de la requête, protégeant ainsi l'anonymat de ce dernier. En situation réelle, cette stratégie de filtrage des sites web est donc, dans le meilleur des cas, d'une efficacité médiocre.

5.5.2 La tunnellisation (« *tunnelling* »)

Une autre technique permettant de contourner un filtre, laquelle requiert un peu plus de connaissances techniques, consiste à utiliser des protocoles de tunnellisation. Les logiciels de tunnellisation permettent aux utilisateurs de créer un « tunnel » chiffré vers une autre machine située sur Internet, laquelle empêche le système de filtrage de voir passer les requêtes web. Une fois que le tunnel est créé vers l'autre machine, toutes les requêtes Internet passent dans ce tunnel, puis à travers la machine qui est à l'autre bout du tunnel, laquelle sert de relais vers Internet.

Les protocoles de tunnellisation sont utilisés par les internautes pour accéder à un contenu à partir d'un endroit différent. Une personne peut utiliser un tunnel mis en place vers une autre machine pour se connecter à Internet à partir de cette autre machine, et contourner ainsi le filtre qui serait placé sur sa propre connexion à Internet. Cette technique de contournement fonctionne même lorsque l'ensemble du trafic web est redirigé vers un système de filtrage local. En effet, le tunnel est généralement sécurisé par un fort chiffrement de l'ensemble du trafic qui y circule. Il est donc impossible de reconnaître le trafic web à l'intérieur.

L'interdiction des technologies de tunnellisation à l'échelle d'un fournisseur d'accès à Internet est concrètement impossible. En effet, beaucoup d'entreprises utilisent ces technologies pour interconnecter leurs bureaux et sites à travers le monde. La mesure serait dès lors totalement disproportionnée, compte tenu de l'important volume des usages légaux de la tunnellisation. De manière analogue, les technologies de tunnellisation sont souvent utilisées pour sécuriser des systèmes de travail à distance, ainsi que des myriades de transactions avec des systèmes sensibles, ou pour sécuriser des environnements « nomades » (« *home office* »).

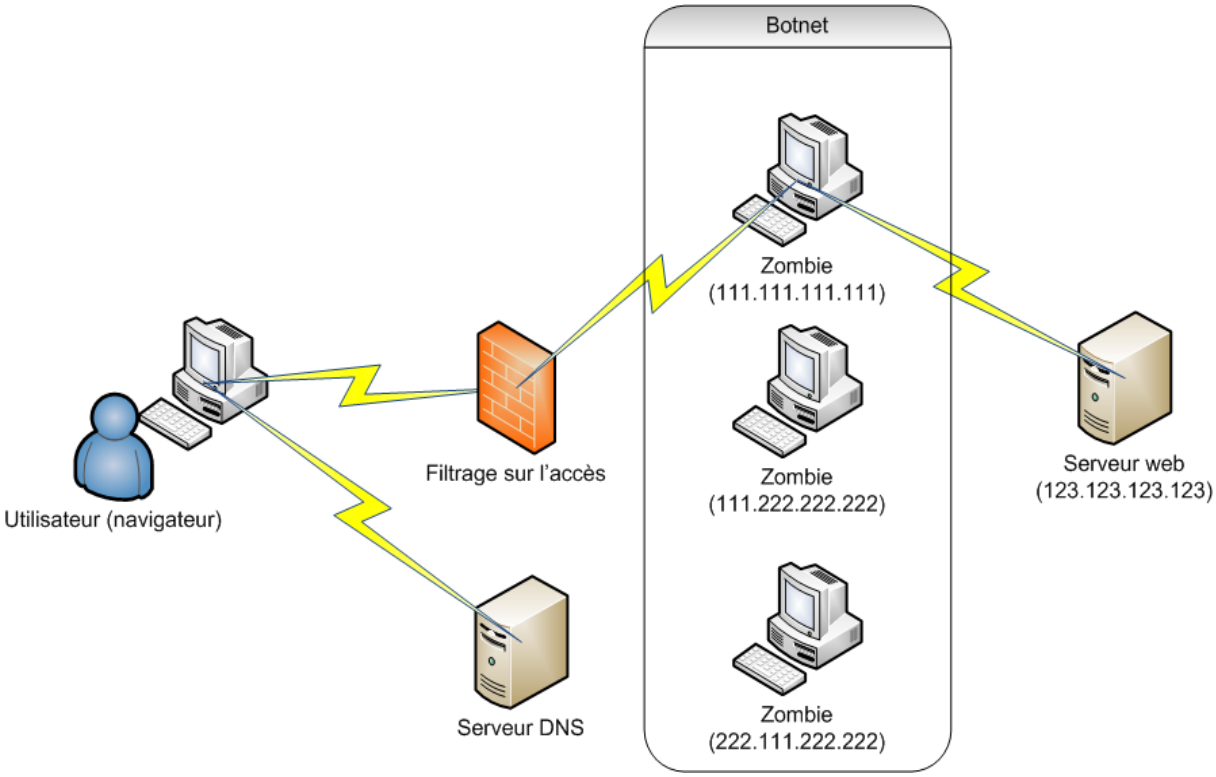
5.5.3 Le changement fréquent d'hébergement ou d'URL (« *hosting or URL rotation* »)

Pour une personne qui publie un contenu, modifier la configuration de son site web pour que ce dernier soit hébergé à une autre adresse (sous un autre nom de domaine, une autre URL ou même une autre adresse IP) est également très facile, et permet effectivement de contourner une mesure de filtrage qui aurait pour cible les adresses IP, les URL ou les noms de domaine.

Un changement fréquent de nom de domaine peut être une technique de contournement des filtrages basés sur les URL.

5.5.4 Les réseaux de zombies (« *botnets* »)

La technologie botnet est souvent utilisée à des fins de changements fréquents de nom de domaine (« *domain name rotation* ») ou de dissimulation d'adresse IP. Les machines compromises d'utilisateurs innocents y sont utilisées comme des portails (ou déflecteurs) sur le contenu d'un serveur web[280]. En quelque sorte, l'ordinateur de ces utilisateurs est transformé en un serveur proxy simple, c'est-à-dire sans cache. Il répond aux requêtes d'accès au dit contenu formulées par n'importe qui, et se charge d'aller chercher le contenu ailleurs, puis de le relayer au demandeur.



Au lieu de renseigner une adresse IP unique dans le DNS, le propriétaire du contenu peut de fait renseigner une liste de plusieurs adresses, qui correspondent à celles d'une succession rapide de machines compromises. Un utilisateur qui envoit au DNS une requête d'accès à ce contenu est alors redirigé vers l'adresse IP de l'un des zombies (« *bots* »). Ce dernier se connecte alors au système central où réside le contenu. Ce système central renvoie le contenu à la machine compromise, laquelle relaie à son tour le contenu à l'utilisateur requérant. Cette technique permet de contourner aisément des filtres basés sur l'adresse IP, à l'exception de ceux qui sont capables de supporter les coûts élevés de maintenance devant être engagés pour pister, tant le contenu concerné, que les machines compromises (les zombies) qui sont impliquées dans la mise à disposition de ce contenu.

Il est fréquent de voir des réseaux zombies (« *botnets* ») constitués de milliers de machines. Diffuser des contenus à caractère pédopornographique par ce biais permet donc, ici encore, de rester très anonyme, d'une part car l'adresse IP du serveur principal, sur lequel se trouve une copie du contenu et qui permettrait de faire facilement le lien avec l'éditeur, est cachée des utilisateurs, et d'autre part car l'adresse IP du portail ou des sites proxy (zombies) peut être modifiée à intervalles de temps très courts. Par ailleurs, aucune journalisation (« *logs* »)

[280] Il existe peu de statistiques sur les sites hébergés en fast-flux, mais un bon aperçu est disponible en langue anglaise sur le site du groupe de travail sur le fast-flux du GNSO de l'ICANN (« *ICANN GNSO fast-flux working group* ») : http://gnso.icann.org/files/gnso/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf. Quelques statistiques pour un seul nom de domaine sont disponible ici, en langue anglaise : http://www.honeynet.org/node/143.

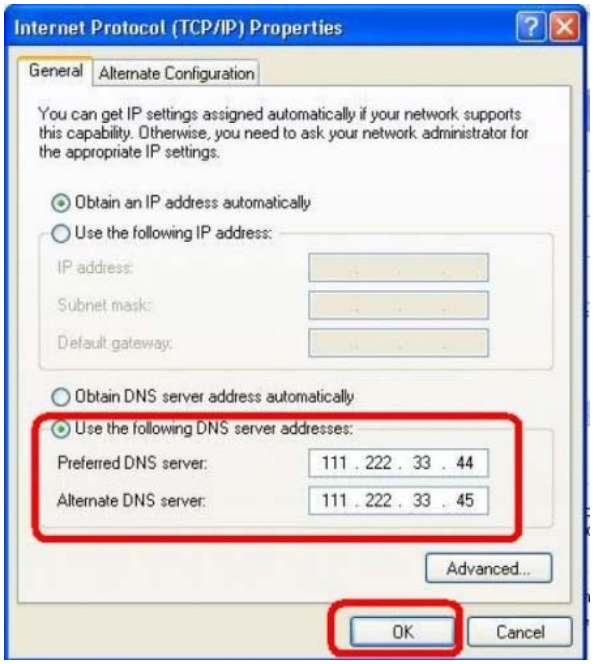
qui pourrait conduire à l'identification des visiteurs n'est conservée sur les machines compromises.

5.5.5 Le contournement du filtrage DNS

Le filtrage effectué au niveau des requêtes DNS est encore plus facile à contourner.

Il s'agit de la technologie de filtrage qui a été adoptée par la plupart des pays occidentaux dont les gouvernements ont imposé ou facilité le filtrage des contenus à caractère pédopornographique, en coopération avec les services en charge de l'application de la loi ou des acteurs privés[281]. Cette méthode de filtrage consiste habituellement à intercepter les requêtes vers un serveur DNS (qui est généralement celui qui est fourni par le FAI à ses abonnés) et à remplacer, dans le cadre des réponses qui sont apportées à ces requêtes, l'adresse IP du site qui héberge le contenu sollicité par une adresse IP différente. Ceci permet à l'opérateur de ce filtrage d'afficher un contenu alternatif, tel qu'une page avec un message d'alerte.

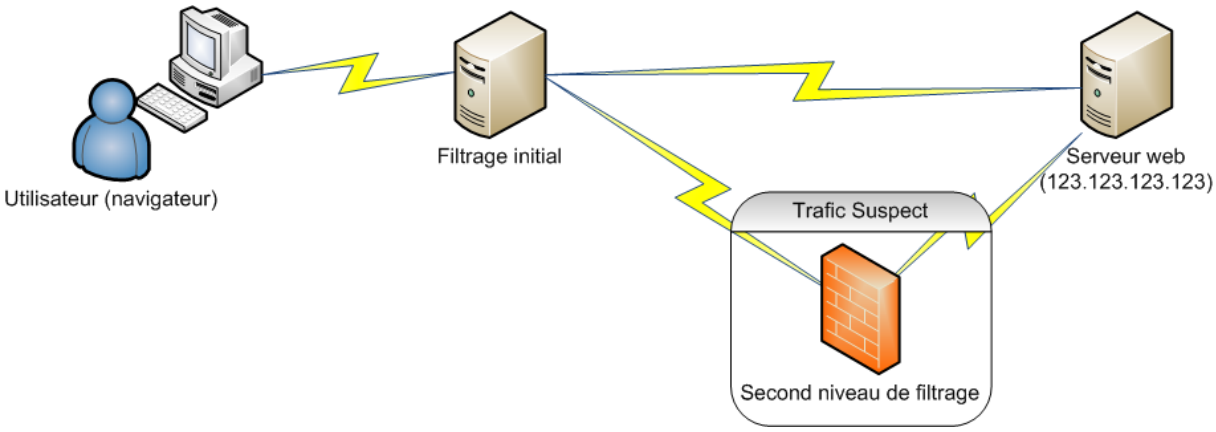
Il suffit simplement de changer la configuration de son ordinateur pour utiliser un autre serveur DNS que celui de son FAI (autrement dit un serveur n'incorporant pas le système de filtrage), pour contourner totalement cette méthode de filtrage. En outre, il existe sur Internet de nombreux serveurs DNS gratuits ou payants, qui peuvent fournir des réponses sans en filtrer les requêtes.



[281] Voir supra, le chapitre 3 du présent rapport.

5.5.6 Les autres systèmes de filtrage

A côté de ces stratégies de filtrage simples, des systèmes de filtrage plus évolués peuvent être utilisés pour surveiller ***la totalité*** du trafic circulant vers les sites web, en utilisant ***la signature de fichiers***. Cette opération implique généralement l'utilisation d'une technologie appelée ***inspection approfondie des paquets - « deep packet inspection » -*** (analyse du contenu de la totalité du trafic), ou bien l'utilisation d'un proxy, pour vérifier l'intégralité du contenu web téléchargé, à la lumière d'une liste de signatures de contenus illégaux connus. Dans la mesure où cette stratégie est très consommatrice de ressources, elle n'est généralement constatée qu'à l'échelle des organisations/entreprises, ces dernières supportant le coût du filtrage et acceptant l'impact de l'initiative sur les performances de leur réseau.



Une alternative pour surmonter ce fardeau à l'échelle d'un FAI ou même d'un pays est d'utiliser un système de filtrage hybride, qui combine plusieurs des éléments cités précédemment dans un même système de filtrage. Par exemple, British Telecom a conçu un système qui réduit les impacts sur les performances du réseau en utilisant une stratégie de filtrage combinée. Ce système hybride porte le nom de projet BT CleanFeed. Il fonctionne en isolant le trafic destiné à une adresse IP ou à une plage d'adresses IP suspectes, ce trafic étant ensuite analysé par un système de filtrage dont la granularité est plus fine (basé sur les URL)[282]. Le second niveau de filtrage prend alors ou non la décision de filtrer tout ou partie du contenu sollicité, ou simplement d'enregistrer les requêtes de connexion qui ont été dirigées vers ce dernier.

Bien que cette solution semble être plutôt efficace, il a également été prouvé qu'elle pouvait être vulnérable à une « ***attaque oracle*** », par laquelle les utilisateurs peuvent potentiellement utiliser le système pour identifier les sites web à caractère pédopornographique, en analysant attentivement les réponses que ce système apporte aux requêtes d'accès à des plages d'adresses IP suspectes (préalablement identifiées)[283]. Le système de filtrage devient alors une source d'information sur la localisation des contenus illégaux, se plaçant par là-même en totale contradiction avec son objectif initial.

Bien que, techniquement, des mesures puissent prévenir ce type d'attaques, il est important de noter que les stratégies de filtrage plus complexes peuvent tout à fait soulever des problématiques et avoir des impacts, en termes de fiabilité logicielle et de sécurité du réseau.

[282] Clayton, « Failures in a Hybrid Content Blocking System » (« Pannes dans un système hybride de filtrage des contenus »), 2005, disponible en anglais à l'adresse : http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf (visité pour la dernière fois le 1er oct. 2009).
[283] Clayton, 2005, précité, n° 4 et s.

5.5.7 Conclusion

En termes d'efficacité, toutes ces stratégies de filtrage souffrent de faiblesses similaires.

- En premier lieu, lorsque le filtrage est réalisé sur tout élément autre qu'une URL complète (laquelle correspond au chemin d'accès complet) ou qu'une signature de contenu, il existe un risque significatif de filtrer plus de contenu que souhaité. Les noms de domaine et les adresses IP ne sont pas suffisamment spécifiques pour pouvoir toujours filtrer avec la précision requise. Ces dommages collatéraux sont parfois considérés comme acceptables, car proportionnés au regard du type de contenu filtré. Cependant, ils ne peuvent pas être acceptables vis-à-vis de tous les types de contenus. Les questions juridiques et démocratiques soulevées au chapitre 6 devraient ici être prises en considération.

- En second lieu, un filtrage efficace du trafic web (autrement dit un filtrage de l'accès de l'utilisateur au contenu lui-même, et pas simplement une mesure utilisant un filtre DNS) requiert des investissements significatifs dans une infrastructure de proxy à inspection approfondie des paquets. Cela implique que la conception de l'architecture et l'infrastructure du réseau permettent de prendre en charge l'interception d'informations de trafic ET de contenu, à large échelle.

  A titre d'exemple, dans le cadre du projet de British Telecom, le coût de la configuration, de la conception et de la mise en œuvre de la solution a été estimé à près de 1 million de livres sterling.

Alors que les fournisseurs d'accès à Internet doivent actuellement avoir la capacité de répondre à un faible nombre de demandes judiciaires d'interception concernant des utilisateurs connus, un tel système implique de gérer tous les utilisateurs d'un fournisseur d'accès, ce qui constitue techniquement une réelle gageure et ne peut pas être mis en œuvre sans garanties minimales de succès.

Ce système peut également être particulièrement intrusif, en ce que la technologie rend possible un accès à l'ensemble du trafic et des contenus générés par les communications des internautes, l'ensemble des requêtes d'accès à des données formulées par tous les utilisateurs devant être analysées et comparées à une liste noire (« *blocking list* »). Une telle approche connaît des obstacles substantiels en termes juridiques et de démocratie, qui sont mis en lumière au chapitre 6 du présent rapport.

Toutes les stratégies de filtrage sont sujettes à contournement, par un moyen ou un autre. Les filtres DNS sont les plus faciles à contourner, bien qu'ils constituent l'option choisie dans de nombreux pays qui ont mis en place des systèmes de filtrage de la pédopornographie. Les filtres peuvent également avoir un effet inverse à celui qui est souhaité, lorsqu'ils sont eux-mêmes utilisés en tant qu'instrument permettant de localiser précisément des contenus illégaux – soit par le biais de l'utilisation des technologies décrites plus haut, soit en raison des divulgations quasi inévitables, de temps en temps, de la liste noire. Tous ces systèmes ne font que créer un « point individuel de défaillance » (« *single point of failure* »), dans une infrastructure Internet dont la plus grande force est essentiellement de ne connaître aucune centralisation, de par sa conception même.

Les filtres peuvent également procurer des informations utiles aux personnes qui opèrent des sites web à caractère pédopornographique. Si le site qu'elles opèrent a été intégré à une liste noire (« *blocking list* »), elles savent dès lors que leur site web a été identifié par les autorités et qu'il est donc hautement probable qu'elles fassent l'objet d'une enquête et d'une surveillance par les services en charge de l'application de la loi.

- Ces personnes peuvent prendre des mesures pour détruire toutes preuves conduisant à elles en qualité d'opérateurs de sites web ET pour relocaliser leurs services sous un

nouveau nom de domaine, sous une nouvelle adresse IP, dans un autre pays ou sur un autre service d'hébergement se trouvant n'importe où dans le monde. Elles peuvent également tester leurs technologies de dissimulation face au système de détection, pour identifier les techniques qui leur procurent la protection la plus longue contre la détection et le filtrage.

- Les activités de filtrage peuvent encore perturber l'activité des personnes qui accèdent à de tels sites web, en forcant les opérateurs de ces sites à relocaliser fréquemment leurs contenus. Ces mouvements peuvent également être suivis et dès lors fournir des renseignements utiles aux enquêteurs. Ils peuvent également être une source d'informations utiles, à des fins de recherche, sur la rapidité avec laquelle ces sites sont relocalisés, ou sur la fréquence avec laquelle ils changent d'adresse IP, de nom de domaine, de fournisseur d'hébergement ou de pays. L'ensemble de ces informations pourrait être très utile aux enquêteurs.

- Il est intéressant de noter que l'évasion constante des mesures de filtrage et le maintien parallèle d'un anonymat implique des ressources et des efforts qui ne devraient pas être sous-estimés. Il est probable que cette situation (outre le fait qu'elle augmente les coûts supportés par les délinquants ou criminels) conduise rapidement à la commission d'erreurs. Toutefois, les ressources et les efforts nécessaires à la création et à la maintenance d'un système de filtrage d'Internet sont tout aussi significatifs.

5.6 Implications dans une société démocratique

5.6.1 Introduction

La présente section a pour objectif d'analyser les dommages collatéraux que peut potentiellement causer une mesure de filtrage, tant en termes de sécurité que sur le terrain de la protection des droits de l'Homme. Elle se penche également sur la possibilité d'extension du filtrage d'Internet à des domaines qui dépassent la pédopornographie, d'un point de vue technique.

5.6.2 Les problématiques de sécurité

La sécurité de toute opération de filtrage constitue une préoccupation majeure. Par conception, l'infrastructure qui est requise pour exécuter une stratégie de filtrage peut interférer avec de nombreux éléments critiques de la connexion Internet des utilisateurs finaux. Il est important de se rappeler que l'un des critères de conception initiaux d'Internet était de mettre en place un système de communication transnational qui serait résistant au pannes, aux perturbations, aux altérations *et*, en conséquence, au filtrage.

Dès lors, garantir un fonctionnement adéquat et proportionné des systèmes de filtrage implique d'analyser minutieusement le niveau de sécurité technique et physique qu'ils présentent. L'implémentation d'une mesure de filtrage, dans toute infrastructure, implique d'introduire dans celle-ci des failles de sécurité et des points de faiblesse susceptibles de provoquer des pannes. Ces derniers doivent en fin de compte être mis en balance avec les effets positifs de l'initiative de filtrage.

En outre, le contenu des listes noires (non dynamiques) présente un intérêt particulier pour les pédophiles. Ces derniers sont particulièrement motivés pour utiliser ces listes dans un dessin opposé à celui qui a présidé à leur conception : les consulter en leur qualité de source de contenus (ou, selon les termes de Clayton (2005), d'oracle).

Ce problème peut être en partie surmonté en ne transmettant ou en ne stockant pas le contenu de la liste en format texte. Ce contenu est souvent encodé par des techniques de hachage cryptographique. La vérification de l'URL ou de l'adresse IP requise par un utilisateur est dès lors faite en calculant la valeur de hachage (ou empreinte) de cette URL ou de cette adresse IP, qui est ensuite comparée aux empreintes contenues dans une base de données. Bien qu'une telle opération soit source d'une certaine sécurité, elle ne s'avère pas suffisante lorsqu'elle est utilisée pour identifier des listes d'adresses IP bloquées. En effet, ces dernières sont limitées en nombre et il est tout à fait possible de calculer l'ensemble de leurs empreintes à l'avance[284], afin de les trouver dans la liste. Dès lors, des mesures additionnelles de sécurité sont nécessaires, afin de sécuriser les listes d'adresses IP au sein de chaque organisation qui les utilise.

Comme nous l'avons souligné plus haut, Richard Clayton (Clayton 2005) découvrit une méthode d'identification des contenus listés dans le système de filtrage hybride « CleanFeed » de British Telecom. Il montra qu'il était possible d'identifier les adresses IP filtrées par le système BT CleanFeed, car hébergeant des ressources à caractère pédopornographique, en analysant les réponses que ce système apportait à des requêtes formatées de manière spéciale, depuis une connexion Internet soumise à ce filtrage[285]. Bien que cette méthode implique d'avoir une certaine connaissance des adresses IP qui hébergent vraisemblablement ce type de contenus, l'exemple montre, d'un point de vue pratique, que toute méthodologie de filtrage peut soulever des préoccupations additionnelles de sécurité, lesquelles doivent être

[284] Résultant d'une base de données de toutes les adresses IP (4,2 milliards) et de leurs valeurs de hachage.

[285] En termes techniques, il définit une valeur de TTL très faible à l'intérieur d'un paquet SYN, utilisé pour envoyer une requête HTTP à destination d'une plage d'adresses IP connue comme étant « mauvaise ». Il découvrit alors que le proxy émulait le mécanisme d'établissement de connexion TCP/IP (« *handshake* ») en répondant par un SYN/ACK. Une adresse IP non filtrée n'aurait pas pu être atteinte à cause de la valeur de TTL trop faible et qui aurait engendré une réponse de rejet (RST).

prises en compte et mesurées aux bénéfices attendus. La complexité qu'il y a à mettre en œuvre des méthodes de filtrage efficaces ne devrait pas être sous-estimée.

Enfin, lorsque des mesures de sécurité sont requises afin de prévenir la divulgation du contenu d'une liste noire, la gestion des opérations de filtrage et de leur efficacité, en plus du maintien de leur proportionnalité, devient une vraie gageure. Cette situation est particulièrement problématique lorsque la liste noire est maintenue par un corps financé par le gouvernement, et pourrait générer des préoccupations relatives aux équilibres de pouvoirs (« *checks and balances* » - poids et contre-poids) qui sont nécessaires dans une société démocratique[286]. Un bon exemple en est la liste noire maintenue par l'Autorité australienne des communications et des médias (ACMA, une agence administrative indépendante), qui a été publiée de manière inappropriée sur Internet, et qui a été rapportée comme comprenant des entrées relatives à une pension canine située dans le Queens et un dentiste[287].

5.6.3 Sur-blocage (« *over-blocking* ») et sous-blocage (« *under-blocking* »)

L'une des problématiques principales que pose chacune de ces stratégies est celle du sur-blocage (ou filtrage excessif) et du sous-bocage (ou filtrage insuffisant). Bien qu'il ne soit pas possible de prévenir entièrement cette difficulté, le caractère inapproprié d'une mesure de filtrage peut être réduit de manière significative en mettant en place un important processus de qualification humaine des contenus filtrés, en utilisant des identificateurs très précis (tels que des URL entières ou des signatures obtenues par hachage), et en adoptant des technologies qui utilisent ce même niveau de détail dans le cadre de leur processus de décision sur le filtrage.

Dans tous les cas, il doit être noté qu'aucune des stratégies identifiées dans le présent rapport ne semble capable de prévenir complètement le sur-blocage. Cette situation constitue une préoccupation majeure, lorsqu'il s'agit de mettre en équilibre le besoin de limiter l'accès aux ressources à caractère pédopornographique, d'une part, et le besoin de préserver les droits de l'Homme et la liberté d'expression, d'autre part. Il semble inévitable que des contenus conformes à la loi soient bloqués, là où le filtrage est mis en œuvre.

Le sous-blocage est également un phénomène universel, particulièrement présent dans les stratégies de filtrage les plus précises et les plus proportionnées. Trouver l'ensemble des identificateurs de contenus illégaux puis en maintenir la liste requiert, de la part des opérateurs de listes noires (« *block list* »), d'importants efforts, une grande confiance en leur objectivité et une capacité à juger le contenu sur la base de critères juridiques.

Selon la stratégie choisie, le risque de décisions arbitraires de filtrage peut varier. La conclusion la plus importante, à ce point de notre analyse, est qu'aucune stratégie n'apparaît comme étant complètement en mesure d'éviter tant le sur-blocage que le sous-blocage. En conséquence, toute évaluation du besoin de filtrer les ressources à caractère pédopornographique devrait prendre en compte cette donnée, selon laquelle l'un et l'autre de ces phénomènes seront vraisemblablement maintenus de manière substantielle.

5.6.4 Les risques de dérives et la reterritorialisation

Il est important de noter la nature intrusive de nombre des stratégies de filtrage qui ont été discutées dans le présent chapitre. Ceci est particulièrement vrai des mécanismes les plus précis de filtrage de contenus (en premier lieu le filtrage basé sur les signatures par hachage ou les URL), qui requièrent une analyse du contenu de la ressource qui est échangée entre les utilisateurs. Cette situation est problématique tant en termes d'investissements (les investissements requis sont invariablement élevés, dans ce type de scénarios), que dans le cadre d'une approche plus large, sociétale.

---

[286] Cet aspect est discuté de manière détaillée au chapitre 6 de la présente étude.

[287] The Australian, 20 mars 2009, « Internet filter list of porn exposed » (« la liste de filtrage du porno sur Internet découverte »), http://www.theaustralian.news.com.au/story/0,25197,25213542-2702,00.html.

La technologie utilisée est comparable à plusieurs égards aux fonctionnalités de mise sur écoute qui sont utilisées par les services en charge de l'application de la loi sur des cibles particulières, dans un cadre juridique précis. La mise en œuvre d'une telle technologie sur un réseau public signifie qu'un volume significatif d'informations est ajouté aux logs des opérateurs de réseaux. Cette mise en œuvre entraîne par conséquent un risque réel de pressions en provenance d'autres sphères de discussion, qui pourraient profiter de la disponibilité de ces systèmes en vue de les utiliser à d'autres fins.

Les sujets de discussion pouvant vraisemblablement conduire à un tel risque de dérives vont de celui des droits d'auteur, en ce que les titulaires de droits vont rechercher des méthodes pour bloquer la diffusion illégale de ressources protégées par des droits d'auteur, à celui des jeux d'argent en ligne, puisque les gouvernements qui connaissent des régimes restrictifs en la matière ont pour objectif de limiter la disponibilité des services fournis par des opérateurs étrangers sur leur sol.

Il est important qu'un tel débat public prenne place. Toutefois, ce dernier devra tenir compte des différences fondamentales, d'ordre technique et juridique, que présentent les différents types de contenus, et de la proportionnalité de la mesure de filtrage par rapport à d'autres méthodes permettant de réduire les dommages, de prévenir les infractions, ou de procéder à des investigations en matière de cybercriminalité. Tous les types de filtrage sont différents, tous les types de contenus sont différents, et tous les types d'infractions sont différents.

Les systèmes de filtrage sont rarement conçus pour procéder à un filtrage à grande échelle d'une large variété de contenus, ainsi que la Chine et l'Arabie Saoudite ont pu s'en rendre compte.

5.7 Conclusions

Les initiatives de filtrage sont de meilleure qualité, lorsqu'elles impliquent une intervention humaine. Le filtrage dynamique est souvent observé comme étant incomplet ou arbitraire (en raison du sur-blocage – filtrage excessif –, ou du sous-blocage – filtrage insuffisant –, qu'il génère). Dans tous les cas, aucune stratégie de filtrage n'est en mesure de prévenir complètement le sur-blocage ou le sous-blocage.

Un défi supplémentaire est d'identifier les sites qui doivent être filtrés. Le fait que les adultes qui ont un intérêt sexuel pour les enfants utilisent souvent des canaux privés de communication au lieu de technologies Internet visibles et détectables comme des sites web ou des messages électroniques non ciblés, implique que le filtrage total de leurs activités est en pratique impossible.

Les contenus Internet peuvent également être échangés sur différents médias. En conséquence, la pratique de ne filtrer qu'un nombre limité de ces médias (telle que celle de ne filtrer que le trafic en direction des serveurs web) pourrait sans aucun doute conduire à l'utilisation d'une autre méthode de distribution de ces contenus. Ceux qui ont à l'esprit de distribuer des contenus illégaux sur Internet disposent d'une myriade d'options pour le faire, en dépit des mesures de filtrage mises en place. D'un point de vue technique, les initiatives de filtrage ne peuvent, en conséquence, qu'assurer la protection des personnes qui pourraient accéder aux contenus par inadvertance. Dès lors, le caractère proportionné d'une mesure de filtrage d'Internet ne peut être démontré qu'en montrant que cette situation représente un problème majeur. Il semble improbable que les stratégies de filtrage, ainsi que nous le montrons dans le présent document, soient en mesure de prévenir efficacement ou de manière substantielle les infractions ou la « revictimisation ».

En outre, la sécurité de la liste noire (« *blocking list* ») et du procédé de filtrage est une préoccupation majeure. Au lieu d'agir simplement comme une liste de contenus non souhaités, la liste noire sera utilisée par ceux qui ont un intérêt poussé pour les contenus qu'elle contient, dans l'objectif d'obtenir une liste de contenus illégaux.

Enfin, en raison de la nature générique des technologies qui sont requises dans le cadre de nombreux scénarios de filtrage, un risque de dérives est toujours présent, qu'il soit ou non intentionnel. Alors qu'elle peut être mise en œuvre dans un objectif particulier, une technologie de filtrage peut être utilisée dans d'autres objectifs – avec ou sans débat public. En effet, de telles technologies peuvent être utilisées aux fins de surveiller largement les activités Internet, sans utiliser les capacités de filtrage qui leur sont intrinsèques. Par exemple, elles peuvent autoriser la surveillance en direct de l'utilisation de sites web étrangers, sans avoir accès aux journaux d'enregistrement des évènements (« *records* ») de ces sites web.

Chapitre 6 LE FILTRAGE D'INTERNET ET LA LOI

6.1 Introduction

Les chapitres précédents ont montré que le filtrage d'Internet ne consiste pas en un retrait définitif des images, vidéos ou pages web concernées, lesquelles continuent d'être accessibles. En raison des inévitables possibilités de contournement de la mesure, des réalités du sous-blocage (ou filtrage insuffisant) et du sur-blocage (ou filtrage excessif), des risques de dérives et de conflits de lois, et du problème selon lequel le filtrage ne conduit pas à la suppression des contenus, la question qui se pose n'est pas simplement de celle savoir s'il faut « filtrer ou ne pas filtrer », mais plutôt celle de savoir quelles mesures de filtrage, proportionnées et acceptables dans une société démocratique, peuvent être introduites. En conséquence, il est crucial de passer en revue les enjeux juridiques et démocratiques que soulève la question du filtrage.

D'un point de vue juridique, le filtrage d'Internet est une mesure qui donnerait, à une personne ou à une entité, dans l'objectif de protéger un intérêt spécifique, le droit de filtrer, le droit de choisir les moyens technologiques destinés à réaliser cet objectif et le droit de choisir les contenus à bloquer, sachant que cette initiative aurait pour résultat de priver certaines autres personnes de leur droit d'accéder à certains contenus ou de leur droit de rendre disponibles certains contenus.

Le filtrage d'Internet est en conséquence une mesure qui, pour protéger certains droits ou libertés spécifiques, a un impact négatif, direct et immédiat, sur certains autres droits et libertés. Puisque les droits et libertés sont régis par la loi, l'analyse de la légitimité du filtrage requiert une analyse approfondie des éléments de droit qui autorisent ou peuvent entrer en conflit avec une telle mesure.

Le filtrage d'Internet est également une mesure qui est internationalement débattue. Pour cette raison, le présent chapitre se concentrera essentiellement sur les droits européen et international, pour ne donner que quelques exemples de leur application par certains systèmes juridiques nationaux.

Quelle loi?

Le terme de « loi » a plusieurs acceptions. La loi peut être définie comme « *toute norme ou système de normes d'ordre juridique ou extra-juridique* »(1). Cette définition inclut le ***droit naturel***, lequel correspond aux « *règles de conduite supposées inhérentes aux relations entre les êtres humains et découvrables par la raison* »(2), et le ***droit positif***, défini comme l' « *ensemble des règles de droit en vigueur dans un pays donné à un moment donné* »(3). Plus précisément, le terme de « loi » peut ne référer qu'aux « *texte(s) voté(s) par le Parlement ; (la) loi (est ici comprise) au sens organique et formel, par opposition à décret, règlement, ordonnance, arrêté, mais aussi à Constitution* »(4).

Le concept de loi, dans cette étude, sera compris comme renvoyant au droit positif, sauf indication contraire. Il inclura donc, au niveau d'un pays, les textes en vigueur votés par le Parlement, ainsi que les dispositions résultant de décrets et autres décisions et textes administratifs, les décisions de justice et, le cas échéant, les dispositions internationales et européennes que le système local reconnaît. La notion de droit européen renverra à l'ensemble des dispositions en vigueur émanant des institutions de l'Union européenne et à leur interprétation par la Cour européenne de justice. La notion de droit international sera comprise comme renvoyant à l'ensemble des dispositions dont l'objet vise des situations concernant plusieurs Etats, ou dont la source est internationale, émanant d'une institution ou d'une Cour se trouvant hors de la structure institutionnelle de l'Union européenne.

(1)(3)(4) Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique*, 7ème éd., Quadrige/PUF, juin 2005, respectivement pages 549, 682 et 549.
(2) Traduit de l'anglais : Webster's New World Dictionary, Third College Edition, 1988, page 903.

Au sein de ces systèmes juridiques, le filtrage d'Internet peut entrer en conflit avec des dispositions relevant de deux domaines du droit, que sont les droits de l'Homme et les libertés fondamentales d'une part, et les dispositions relatives aux communications électroniques d'autre part. Le filtrage peut inversement se révéler compatible avec certaines dispositions de l'un et l'autre de ces domaines, en fonction notamment de la proportionnalité de la mesure adoptée. L'enjeu est donc de déterminer la mesure dans laquelle une liberté peut être limitée dans l'objectif d'en préserver une autre. Le présent chapitre analysera de manière plus détaillée chacun de ces domaines juridiques, afin d'autoriser une conclusion sur les conditions dans lesquelles une mesure de filtrage pourrait être considérée comme juridiquement acceptable.

Sur cette base, la section 6.2 exposera brièvement les raisons pour lesquelles la question du filtrage d'Internet et celle du respect des libertés fondamentales doivent être considérées ensemble. La section 6.3 se concentrera sur les liens qui peuvent être constatés entre ces droits et libertés et la démocratie. La section 6.4 soulignera les différences qui existent entre les notions de droits de l'Homme, de libertés fondamentales et de libertés publiques. La section 6.5 rappellera la nature et la force juridique des textes qui consacrent ces droits et libertés. La section 6.6 présentera de manière détaillée les droits fondamentaux pouvant se trouver en conflit avec une mesure de filtrage d'Internet, tandis que la section 6.7 sera consacrée aux droits susceptibles de soutenir une telle mesure. La section 6.8 proposera une vue d'ensemble des dispositions relatives, d'une part, au commerce électronique dans le marché européen, et, d'autre part, à la responsabilité des prestataires d'accès à Internet, qui sont susceptibles de s'appliquer à une mesure de filtrage d'Internet.

Enfin, le chapitre 7 examinera la question de la mise en équilibre des droits fondamentaux en société, et la manière dont les conflits peuvent être appréhendés et arbitrés. Il évaluera l'ensemble des initiatives de filtrage d'Internet qui sont aujourd'hui à l'étude, et les comparera aux étapes de résolution des conflits qui seront décrites au sein de ce même chapitre et qui incluent l'utilisation du principe de proportionnalité. Ce chapitre fournira également quelques indications relatives aux contextes juridiques dans lesquels le filtrage d'Internet pourrait être acceptable dans une société démocratique.

Cet exposé sera particulièrement utile pour les pays qui débattent actuellement de la légitimité du filtrage d'Internet. Il leur permettra de savoir comment respecter les droits de l'Homme et les libertés fondamentales, ou d'autres dispositions plus spécifiques qui pourraient limiter la possibilité d'apposer des filtres sur le réseau Internet.

6.2 Le filtrage d'Internet et les libertés fondamentales

De nombreux systèmes juridiques nationaux, de même que les systèmes juridiques européen et international, aménagent une place très importante aux droits de l'Homme et aux libertés fondamentales, lesquels peuvent tour à tour être invoqués pour justifier une mesure de filtrage, ou affectés de manière inappropriée par une telle mesure. En effet, filtrer un contenu ou une communication électronique suppose, pour un individu ou une entité, d'avoir le droit de procéder à ce filtrage et d'avoir le droit de priver certaines personnes de leur droit d'accéder à un contenu électronique, d'utiliser un protocole de communication particulier, ou de communiquer un contenu donné à certains individus ou d'une certaine façon.

Ces droits et libertés n'ont pas toujours la même force juridique, selon leur source et les éventuels textes qui les intègrent en droit interne. Ceci accroît la confusion qui peut parfois être ressentie à l'abord de la notion de droits de l'Homme et de libertés fondamentales.

Il est inversement noté que certains pays peuvent avoir choisi de ne pas respecter les droits de l'Homme et les libertés fondamentales.

6.3 Le rôle de la démocratie

La préservation des droits de l'Homme, en particulier de ceux qui pourraient entrer en conflit avec une mesure de filtrage d'Internet, à savoir le droit à la vie privée et le droit à la liberté d'expression[288], est souvent considérée comme intrinsèque à toute démocratie[289]. Toutefois, définir la démocratie, et établir un lien clair entre un tel système politique et la préservation des libertés, n'est pas aussi aisé qu'il apparaît au premier abord.

Il existe plusieurs définitions de la démocratie[290], et « *les scientifiques et observateurs politiques* » eux-mêmes « *ne sont pas d'accord sur le nombre de démocraties qui existent dans le monde (et) ont des avis divergents sur la manière de classifier certains régimes particuliers, sur les conditions nécessaires à la naissance et à la consolidation d'une démocratie, et sur les conséquences de la démocratie sur la paix et le développement* »[291]. Ceci dit, il est possible de dire basiquement que la démocratie est au moins un « *gouvernement du peuple par lui-même* »[292], une forme de « *gouvernement dans lequel les personnes exercent le pouvoir, soit directement, soit par l'intermédiaire de représentants élus* »[293]. Dans ces circonstances, lorsque les « *dirigeants sont élus* »[294], la démocratie peut être définie comme « *un système permettant de choisir son gouvernement au terme d'une compétition électorale libre et juste, à des intervalles réguliers* »[295].

Ceci étant dit, les spécialistes de la démocratie admettent souvent que « *rien ne justifie que la démocratie électorale et la liberté doivent aller de concert* »[296]. Le professeur Larry Diamond explique quant-à-lui que le concept de liberté « *arriva avant la démocratie, tant en Angleterre que, à des degrés divers, dans les autres pays européens* », et que, de nos jours, « *il y a beaucoup de démocraties non libérales, qui connaissent des abus en matière de droits de l'Homme ainsi que des conflits civils* »[297].

6.3.1 La démocratie et les libertés fondamentales

Trois autres aspects de l'organisation politique permettent toutefois de déceler les relations[298] entre démocratie et libertés.

---

[288] Voir infra sous-sections 6.6.1 et 6.6.2.

[289] Voir par exemple « Democracy », Wikipedia, the free encyclopedia, disponible à l'adresse suivante : http://en.wikipedia.org/wiki/Democracy.

[290] Voir par exemple Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, page 31 : « *Un élément clef, dans tous ces débats, est le manque de consensus sur la signification de la notion de démocratie…* » (traduit de l'anglais).

[291] Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, page 31.

[292] Larousse encyclopédique en couleurs, France Loisirs, Librairie Larousse 1978, tome 6, page 2 660.

[293] Traduit de l'anglais. Webster's New World Dictionary, Third College Edition, 1988, page 366.

[294] Traduit de l'anglais. Adam Przeworski, « Minimalist Conception of Democracy: A Defense » (« La conception minimaliste de la démocratie : une défense »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, page 12.

[295] Traduit de l'anglais. Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, p. 29. Voir aussi Joseph Schumpeter, « Capitalism, Socialism, and Democracy » (Capitalisme, socialisme et démocratie), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, p. 9, « another theory of Democracy » (« une autre théorie de la démocratie ») : « *La méthode démocratique consiste en des accords institutionnels permettant d'arriver à des décisions politiques dans lesquelles les individus acquièrent le pouvoir de décider au terme d'une compétition pour obtenir le vote des électeurs* » (traduit de l'anglais).

[296] Traduit de l'anglais. Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, p. 30.

[297] Traduit de l'anglais. Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, page 30. L'auteur conclut : « *Ces deux faits ont ranimé l'intérêt intellectuel pour l'autocratie libérale, comme étant une forme meilleure de gouvernement, plus sûre et plus stable, pour nombre de sociétés en transition* » (traduit de l'anglais).

[298] Voir Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, page 30: « *la démocratie libérale procure, par définition, une relativement bonne protection pour les droits de l'Homme* » (traduit de l'anglais). Voir aussi Joseph Schumpeter, « Capitalism, Socialism, and Democracy » (« Capitalisme,

- Les élections
  Le premier de ces aspects est le principe selon lequel tous les citoyens ont le droit de participer à la vie politique. La possibilité (théorique) qu'a chacun « *de participer à la compétition pour la direction politique en se présentant lui-même devant les électeurs (…) signifiera dans la plupart des cas (…) une dose considérable de liberté de discussion pour tous* », ce qui assure normalement, « *en particulier* », *une « dose considérable de liberté de la presse »*[299].

- La séparation des pouvoirs
  Le second de ces aspects est la séparation des pouvoirs, notamment permise par l'organisation institutionnelle, puisque cette séparation « *(limite) l'arbitraire et (empêche) les abus liés à l'exercice de missions souveraines* »[300].

- Les droits fondamentaux
  Le troisième aspect, qui apparaît fondamental et qui est peut être une conséquence réelle de la démocratie, car résultant de la prise en compte de la volonté générale des citoyens à un moment donné, est le souhait et l'engagement pris par l'Etat de respecter les libertés, dans l'intérêt général des citoyens, ainsi que d'établir et de maintenir la paix nationale et/ou internationale.

Historiquement, de nombreux Etats ont choisi, au niveau national ou/et international, de proclamer légalement certains droits de l'Homme et libertés fondamentales – souvent après une guerre civile, une révolution ou des évènements nationaux d'une particulière violence. Ces déclarations sont destinées à agir comme un socle de droits sur lequel les gouvernements ne peuvent pas revenir aisément, quelles que soient les évolutions des craintes de la société civile ou des priorités politiques. Par ailleurs, la préservation et la promotion de ces droits fondamentaux sont considérées comme « *un idéal* » de la démocratie, laquelle est elle-même admise comme étant « *le meilleur moyen d'atteindre ces objectifs* », étant également « *le seul système politique apte à se corriger lui-même* »[301].

6.3.2 Les démocraties libérales

De nombreuses démocraties européennes choisirent cette approche, ainsi que le montrent les textes qui consacrent sur leur sol, actuellement, les droits de l'Homme et les libertés fondamentales, ce qui a conduit nombre de personnes à considérer la démocratie comme synonyme de protection des droits de l'Homme. Ces Etats européens ont généralement un « *gouvernement constitutionnel* », lequel, « *comme Locke, Montesquieu et les fédéralistes américains l'ont affirmé* », restreint et divise « *le pouvoir temporaire de la majorité* », et peut

---

socialisme et démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, p. 11: la « *méthode démocratique ne garantit pas nécessairement plus de libertés individuelles que ne le permettrait une autre méthode politique dans de mêmes circonstances (…) mais une relation persiste entre les deux* » (traduit de l'anglais).

[299] Joseph Schumpeter, « Capitalism, Socialism, and Democracy » (« Capitalisme, socialisme et démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, page 11: « *Si, au moins en principe, tout le monde est libre de participer à la compétition pour la direction politique en se présentant lui-même devant les électeurs, cela signifiera dans la plupart des cas, bien que non dans tous, une dose considérable de liberté de discussion pour tous. En particulier, cela signifiera normalement une dose considérable de liberté de la presse* ». Voir aussi Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, p. 32 : « *Les conceptions minimalistes de la démocratie électorale reconnaissent généralement, également, le besoin de degrés minimaux de liberté (d'expression, de la presse, d'organisation et d'assemblée) afin que la compétition et la participation aient un sens* » (traduit de l'anglais).

[300] Vie Publique, La Documentation Française, disponible à cette adresse : http://www.vie-publique.fr/decouverte-institutions/institutions/approfondissements/separation-pouvoirs.html, citant des théoriciens de la séparation des pouvoirs comme Locke ou Montesquieu.

[301] Voir par exemple la « Déclaration Universelle sur la démocratie » adoptée sans vote par le Conseil interparlementaire lors de sa 161ème session, http://www.ipu.org/cnl-f/161-dem.htm, article 3: « *En tant qu'idéal, la démocratie vise essentiellement à préserver et promouvoir la dignité et les droits fondamentaux de l'individu, à assurer la justice sociale, à favoriser le développement économique et social de la collectivité, à renforcer la cohésion de la société ainsi que la tranquillité nationale et à créer un climat propice à la paix internationale. En tant que forme de gouvernement, la démocratie est le meilleur moyen d'atteindre ces objectifs ; elle est aussi le seul système politique apte à se corriger lui-même* » (adoptée sans vote car, après l'adoption de la Déclaration, la délégation de la Chine a émis des réserves sur ce texte).

de ce fait « *protéger les libertés individuelles* ». Le Professeur Diamond considère que « *cette idée (et valeur) fondamentale donna naissance* » au « *concept (de) démocratie libérale* », qu'il définit comme « *un système politique dans lequel les libertés des individus et des groupes sont bien protégées et dans lequel existent des sphères autonomes de société civile et de vie privée, isolées du contrôle étatique…* »[302].

Faisant nôtre cette définition, nous pouvons dire que la préservation des libertés est un choix des démocraties libérales, et que les démocraties qui souhaitent être considérées comme libérales devraient préserver ces droits, y compris dans le cadre d'une mesure de filtrage.

Cette étude analysera en conséquence les droits qui pourraient être menacés par une mesure de filtrage, et les confrontera aux droits qui pourraient justifier une telle mesure. Cette analyse permettra à toute démocratie libérale de mesurer le contenu de chacun de ces droits et les conditions dans lesquelles le filtrage pourrait intervenir pour limiter certain d'entre eux. Avant de commencer une étude de cette ampleur, il semble important d'alimenter le débat public en expliquant la différence entre les droits de l'Homme, les libertés fondamentales et une autre notion fréquemment utilisée, celle de libertés publiques.

[302] Pour toutes ces citations, voir Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, page 29.

6.4 Droits de l'Homme, libertés publiques et libertés fondamentales

La différence entre les droits de l'homme, les libertés fondamentales et les libertés publiques réside principalement en la personne du *titulaire* de droits, lequel dépend lui-même du contenu du droit attribué, de la valeur juridique du texte qui consacre ce droit et de l'importance accordée à la protection de ce droit. Au delà, un droit particulier peut recevoir chacune des trois qualifications. Il en est ainsi, dans de nombreux pays, du droit à la protection de la vie privée et du droit à la liberté d'expression.

6.4.1 Les droits de l'Homme

Les droits de l'Homme ont été définis comme « *inhérents à l'être humain (homme ou femme)* », comme un « *ensemble de facultés et prérogatives considérées comme appartenant naturellement à tout être humain* »[303]. D'autres auteurs considèrent que la notion de droits de l'Homme « *renvoie aux sources du droit naturel et des premiers textes à les avoir proclamés »,* tant au niveau national « *(Bill of Rights de 1689, Déclaration de 1789)* » qu'au niveau international « *(Charte de San Francisco de 1945, Déclaration Universelle de 1948, Pactes de New York de 1966, Convention européenne des droits de l'homme (…)* » de 1950[304].

Au sein de la catégorie des « droits de l'Homme », certains auteurs distinguent les droits suivants :

- Les droits de l'Homme de première génération, « *d'inspiration libérale (individuels, civils et politiques)* » ;
- Les droits de l'Homme de deuxième génération, « *d'inspiration socialisante (économiques, sociaux et culturels (…), impliquant de l'Etat (…) des prestations positives)* » ;
- Les droits de l'Homme de troisième génération, « *d'inspiration tiers-mondiste (droits de l'homme et des peuples, collectifs, dits "de solidarité" : (droit au) développement, à la préservation du patrimoine commun de l'humanité) »*[305].

6.4.2 Les libertés publiques

Cette notion de droits de l'Homme est plus ancienne que celle de libertés publiques, elle-même considérée comme désignant « *une forme de consécration juridique des droits de l'homme* »[306]. La notion de libertés publiques apparut en France avec la Constitution du 14 janvier 1852 et est aujourd'hui mentionnée à l'article 34 de la Constitution française du 4 octobre 1958, ainsi que dans certains textes de droit français[307]. Des déclarations, conventions et autres textes internationaux font également des références de plus en plus fréquentes à cette notion[308].

Les libertés publiques constituent des limitations aux pouvoirs de l'autorité publique[309] à l'égard des citoyens, et incluent les « *libertés personnelles* » et les « *libertés collectives* »[310]. En ce qui concerne les libertés personnelles,

- Les Professeurs Robert et Duffar placent en première position « *la liberté individuelle ou "physique", c'est-à-dire la liberté de se déplacer librement, de n'être point arrêté*

[303] Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique*, 7ème éd., Quadrige/PUF, Juin 2005, p. 330.
[304] Dominique Turpin, *Les libertés publiques*, mémentos, Gualino éditeur, 5ème éd., 2000, page 11.
[305] Voir, pour la discussion et les citations, Dominique Turpin, Les libertés publiques, mémentos, Gualino éditeur, 5ème éd., 2000, page 11.
[306] Droit des libertés fondamentales, collectif, sous la coordination de Louis Favoreu, Dalloz, 3ème éd., 2005, n° 57.
[307] Dominique Turpin, *Les libertés publiques*, mémentos, Gualino éditeur, 5ème éd., 2000, page 11.
[308] François Terré, « Sur la notion de libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, sous la direction de Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, éd. Dalloz, 11ème éd., 2005, page 5, n° 10.
[309] Claude-Albert Colliard, *Libertés publiques*, Dalloz, 6ème éd., 1982, page 23.
[310] Jacques Robert et Jean Duffar, *Droits de l'homme et libertés fondamentales*, éd. Montchrestien, 7ème éd., 1999, page 27.

arbitrairement ou séquestré, d'être jugé avec toutes les garanties légales (…), de ne pas être atteint dans son intégrité physique, dans son intimité… »[311] ;

- En seconde position, ils placent les « *libertés de l'esprit* » que sont « *la liberté d'opinion, de religion, la liberté de la presse, la liberté d'enseignement* », ainsi que les « *libertés économiques* » que sont le « *droit au travail, (la) liberté du commerce et de l'industrie* ».

Aux côtés des libertés personnelles, ils mentionnent les libertés collectives, que sont notamment « *la liberté de réunion, la liberté d'association, la liberté syndicale, le droit de grève…* »[312].[313]

6.4.3 Les libertés fondamentales

Aux notions de droits de l'Homme et de libertés publiques, a été ajoutée la notion de « droits fondamentaux » ou de « libertés fondamentales ». Ces droits et libertés, qui bénéficient tant aux personnes physiques qu'aux personnes morales, peuvent être définis selon les termes du Professeur Louis Favoreu : « *Les droits et libertés fondamentaux sont,*

- *En premier lieu, protégés contre le pouvoir exécutif mais aussi contre le pouvoir législatif ; alors que les libertés publiques – au sens du droit français classique – sont essentiellement protégées contre le pouvoir exécutif…*
- *En deuxième lieu, les droits fondamentaux sont garantis en vertu non seulement de la loi mais surtout de la Constitution ou des textes internationaux ou supranationaux.*
- *En troisième lieu, la protection des droits fondamentaux nécessite, pour être assurée contre les pouvoirs exécutifs et législatifs, en application des textes constitutionnels (ou internationaux), qu'en soient chargés, non plus les juges ordinaires, mais aussi les juges constitutionnels et même les juges internationaux* »[314].

---

[311] Jacques Robert et Jean Duffar, *Droits de l'homme et libertés fondamentales*, éd. Montchrestien, 7ème éd., 1999, page 27.

[312] Jacques Robert et Jean Duffar, *Droits de l'homme et libertés fondamentales*, éd. Montchrestien, 7ème éd., 1999, page 27.

[313] François Terré donne aux libertés publiques un contenu analogue. Il distingue ces libertés publiques, prérogatives qui « *se manifestent avant tout dans les rapports de l'individu avec la puissance publique* », des « droits subjectifs », dont la notion sous-tend celle des droits de l'Homme, qui peuvent être vus comme des prolongements des libertés publiques et qui gouvernent principalement les « *relations entre les particuliers – individus ou groupements – soit dans leurs rapports entre eux, soit dans leurs rapports avec les biens* ». Les droits subjectifs, « *prérogatives individuelles qui existe sur la tête d'une personne* » (voir Gérard Cornu, Association Henri Capitant, *Vocabulaire juridique*, 7ème éd., Quadrige/PUF, juin 2005, page 874), « *sont dotés d'une structure et d'un contenu caractérisé : droit de créance, droit de propriété, d'usufruit, de servitude…* ». Pour les citations voir François Terré, « Sur la notion de libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, sous la direction de Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, éd. Dalloz, 11ème éd., 2005, page 5, n° 12, 13 et 15. Voir aussi François Terré, *Introduction générale au droit*, Précis Dalloz, 6ème éd., 2003, page 160.

[314] François Terré, « Sur la notion de libertés et droits fondamentaux », op. cit, page 7 ; voir aussi Serge Guinchard, « Le procès équitable : droit fondamental ? », AJDA, n° spécial du 20 juillet - 20 août 1998, page 191. Les deux auteurs citent notamment Louis Favoreu, « Universalité des droits fondamentaux et diversité culturelle », in *L'effectivité des droits fondamentaux dans les pays de la communauté francophone*, colloque international de l'île Maurice, 29 sept.-1er oct. 1993, AUPELF/UREF 1994, page 48. Pour d'autres analyses de la notion de droits fondamentaux, voir par exemple Véronique Champeil-Desplats, « La notion de droit "fondamental" et le droit constitutionnel français », D. 95, page 323. Pour une « esquisse d'une théorie des droits fondamentaux », voir aussi *Droit des libertés fondamentales*, collectif, sous la coordination de Louis Favoreu, Dalloz, 3ème éd., 2005, n° 70 et s.

6.5 Les instruments de protection des droits de l'Homme et des libertés fondamentales

Les premiers textes à avoir consacré les droits de l'Homme et les libertés fondamentales furent nationaux. Les textes internationaux furent adoptés après la seconde guerre mondiale et contribuèrent à modifier les systèmes juridiques locaux. Leur contenu fut ensuite reconnu par les institutions de l'Union Européenne. L'analyse de l'impact de ces textes est particulièrement importante pour les pays qui débattent de la mise en œuvre du filtrage d'Internet. En effet, les initiatives de filtrage d'Internet seront analysées plus loin à la lumière des principales libertés fondamentales qui semblent entrer en conflit avec elles – dont la liberté d'expression et le droit au respect de la vie privée et familiale – ou qui semblent inversement les soutenir, comme le droit des enfants à être protégés contre les violences et l'exploitation.

6.5.1 Les textes nationaux

Les premiers textes connus pour avoir proclamé les droits de l'Homme et les libertés fondamentales au niveau national sont principalement le Bill of Rights anglais de 1689, le Bill of Rights américain de 1787 et la Déclaration française des droits de l'Homme et du citoyen de 1789. Ces trois textes constituent ce que Moore appelle « *la route bourgeoise* » vers « *le monde moderne* », la route qui fit de l'Angleterre, des Etats-Unis et de la France des « *démocraties parlementaires occidentales* », à l'issue de « *différents modèles concrets de lutte des classes* »[315].

6.5.2 Les instruments internationaux

Les instruments internationaux relatifs aux droits de l'homme et aux libertés fondamentales furent adoptés dans le cadre des Nations Unies et du Conseil de l'Europe.

6.5.2.1 Les Nations Unies

A l'issue de la seconde guerre mondiale, le premier texte international à avoir consacré les droits de l'Homme et les libertés fondamentales fut la ***Charte des Nations Unies*** signée à San Francisco le 26 juin 1945 et entrée en vigueur le 24 octobre 1945. Notamment élaborée pour « *maintenir la paix et la sécurité internationales* », « *pour développer entre les nations des relations amicales fondées sur le respect du principe de l'égalité de droits des peuples et de leur droit à disposer d'eux-mêmes* » et pour « *être un centre où s'harmonisent les efforts des nations vers (les) fins communes* » décrites à l'article 1 de la Charte, les Nations Unies ont également pour objectif de « *réaliser la coopération internationale en résolvant les problèmes internationaux d'ordre économique, social, intellectuel ou humanitaire, en développant et en encourageant le respect des droits de l'homme et des libertés fondamentales pour tous, sans distinctions de race, de sexe, de langue ou de religion* »[316].

La Déclaration universelle des droits de l'Homme (DUDH)

Le second texte international à avoir consacré les droits et libertés fut la ***Déclaration universelle des droits de l'Homme (DUDH)***, adoptée à Paris par l'Assemblée générale des Nations Unies le 10 décembre 1948. Bien que cette Déclaration ne soit pas juridiquement contraignante, elle a été adoptée en tant qu' « *idéal commun à atteindre pour tous les peuples et toutes les nations* »[317] et se trouve être le texte le plus traduit et le plus diffusé,

---

[315] Theda Skocpol, « Social Revolutions in the Modern World » (« Révolutions sociales dans le monde moderne »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, Massachusetts Institute of Technology, 2003, pages 66 et 67.

[316] Voir l'article 1 de la Charte, disponible à l'adresse : http://www.un.org/fr/documents/charter/index.shtml.

[317] « Universal Declaration of Human Rights » (« Déclaration Universelle des droits de l'Homme »), « Introduction », sur le site web du Haut-Commissariat aux droits de l'Homme des Nations Unies : http://www.ohchr.org/EN/UDHR/Pages/Introduction.aspx.

« *360 traductions différentes* »[318] étant disponibles à partir du site web[319] du Haut-Commissariat aux droits de l'Homme (HCDH).

Cette Déclaration, qui souligne le principe d'universalité des droits de l'Homme[320] et qui « *énonce pour la première fois dans l'histoire de l'humanité les droits civils, politiques, économiques, sociaux et culturels fondamentaux dont tous les êtres humains devraient jouir* »[321], est « *généralement reconnue comme étant le fondement du droit international relatif aux droits de l'homme* », et « *a inspiré un corpus abondant de traités internationaux légalement contraignants relatifs aux droits de l'homme* »[322]. Avec le ***Pacte international relatif aux droits civils et politiques***, les deux protocoles facultatifs de celui-ci et le ***Pacte international relatif aux droits économiques, sociaux et culturels***, la DUDH forme la « *Charte internationale des droits de l'homme* »[323]. Avec sept autres instruments relatifs aux droits de l'Homme adoptés entre 1965 et 2006, il existe aujourd'hui neuf instruments internationaux principaux relatifs aux droits de l'Homme.[324] Les 192 Etats membres des Nations Unies ont chacun ratifié aux moins l'un de ces instruments, démontrant ainsi leur engagement en matière de protection des droits de l'Homme, tandis que 80% d'entre eux « *en ont ratifié quatre ou davantage* »[325].

Le Pacte international relatif aux droits civils et politiques

L'un des importants textes de ce corpus, qui doit être mentionné au regard des libertés qui devront être analysées dans le cadre d'une mesure de filtrage d'Internet, est le Pacte international relatif aux droits civils et politiques (PIDCP) adopté à New York par l'Assemblée générale des Nations Unies le 16 décembre 1966 et entré en vigueur le 23 mars 1976 (pour toutes ses dispositions à l'exception de celles de l'article 41, lesquelles sont entrées en vigueur le 28 mars 1979). 72 pays ont signé ce Pacte tandis que 164 pays en sont devenus parties, par ratification, adhésion ou succession[326], prenant de ce fait l'engagement de prendre les « *mesures d'ordre législatif ou autre, propres à donner effet aux droits reconnus dans le (…) Pacte qui ne seraient pas déjà en vigueur* »[327], comme le droit à la vie (article 6), le droit de ne pas être soumis à la torture ni à des peines ou traitements cruels, inhumains ou dégradants (article 7), le droit à la liberté et à la sécurité de sa personne (article 9), le droit de ne pas être l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille ou sa correspondance (article 17), le droit à la liberté de pensée, de conscience et de religion (article 18) ou le droit à la liberté d'expression (article 19). Le droit au respect de la vie privée et le droit à la liberté d'expression sont les deux libertés majeures susceptibles d'entrer en conflit avec une mesure de filtrage, ainsi que nous le verrons plus loin, et le nombre élevé d'Etats qui ont reconnu la nécessité de les préserver montre l'importance qui doit leur être accordée dans le cadre du débat sur le filtrage d'Internet.

---

[318] Traduit de l'anglais. « Universal Declaration of Human Rights » (« Déclaration universelle des droits de l'Homme »), « Introduction », sur le site web du Haut-Commissariat aux droits de l'Homme des Nations Unies : http://www.ohchr.org/EN/UDHR/Pages/Introduction.aspx.

[319] http://www.ohchr.org/.

[320] « Que sont les droits de l'homme », site web du Haut-Commissariat aux droits de l'Homme des Nations Unies : http://www.ohchr.org/FR/issues/Pages/WhatareHumanRights.aspx.

[321] « Le droit international relatif aux droits de l'homme », site web du Haut-Commissariat aux droits de l'Homme des Nations Unies : http://www.ohchr.org/FR/ProfessionalInterest/Pages/InternationalLaw.aspx.

[322] « Déclaration Universelle des droits de l'homme », site web des Nations Unies : http://www.un.org/fr/documents/udhr/law.shtml.

[323] « Le droit international relatif aux droits de l'homme », site web du Haut-Commissariat aux droits de l'Homme des Nations Unies : http://www.ohchr.org/FR/ProfessionalInterest/Pages/InternationalLaw.aspx.

[324] Ces traités, leurs protocoles optionnels et les organes qui en sont en charge sont listés sur le site du Haut-Commissariat aux droits de l'Homme des Nations Unies : http://www2.ohchr.org/french/law/.

[325] « Que sont les droits de l'homme », site web du Haut-Commissariat aux droits de l'Homme des Nations Unies : http://www.ohchr.org/FR/issues/Pages/WhatareHumanRights.aspx. Voir également « La Déclaration Universelle des droits de l'homme : fondement du droit international relatif aux droits de l'homme », site web des Nations Unies : http://www.un.org/fr/documents/udhr/law.shtml. La liste des Etats membres des Nations Unies est disponible à cette adresse : http://www.un.org/en/aboutun/.

[326] Les informations relatives au Pacte et la liste de ses signataires et parties sont disponibles sur le site web des Nations Unies à l'adresse : http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=fr&clang=_fr.

[327] Article 2 du Pacte.

La Convention relative aux droits de l'enfant

Un autre texte important est la Convention relative aux droits de l'enfant, adoptée et ouverte à la signature, ratification et adhésion par la résolution de l'Assemblée générale des Nations Unies n° 44/25 du 20 novembre 1989. Elle est entrée en vigueur le 2 septembre 1990[328] et comptabilise aujourd'hui 194 Etats parties[329].

Le préambule de cette Convention rappelle « *que la nécessité d'accorder une protection spéciale à l'enfant a été énoncée dans la Déclaration de Genève de 1924 sur les droits de l'enfant et dans la Déclaration des droits de l'enfant adoptée par l'Assemblée générale le 20 novembre 1959, et qu'elle a été reconnue dans la Déclaration universelle des droits de l'homme, dans le Pacte international relatif aux droits civils et politiques (en particulier aux articles 23 et 24), dans le Pacte international relatif aux droits économiques, sociaux et culturels (en particulier à l'article 10) et dans les statuts et instruments pertinents des institutions spécialisées et des organisations internationales qui se préoccupent du bien-être de l'enfant* ». Son article 1 ajoute qu'au sens de la Convention, « *un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable* ».

La Convention fait basiquement bénéficier les enfants de quatre catégories de droits qui pourraient être en discussion dans le cadre d'une mesure de filtrage d'Internet.

- Le droit d'être protégés contre toute forme de violence et d'exploitation[330] ;
- Le droit au développement, spécialement au travers de l'accès à l'information[331] et en étant préparés « *à assumer les responsabilités de la vie dans une société libre* »[332] ;
- Le droit de voir leurs meilleurs intérêts considérés en priorité : « *Dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale* » ;
- Le droit, pour « *les enfants mentalement ou physiquement handicapés* », de « *mener une vie pleine et décente, dans des conditions qui garantissent leur dignité, favorisent leur autonomie et facilitent leur participation active à la vie de la collectivité* »[333].

L'article 34 impose l'obligation spécifique, aux Etats parties à cette Convention contraignante, de prendre « *toutes les mesures appropriées sur les plans national, bilatéral et multilatéral pour empêcher (…) que des enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique* ». Si nous nous remémorons les déclarations de certains ministres gouvernementaux[334] relatives au manque apparent de coopération internationale, il semble que des efforts soient encore nécessaires pour assurer le respect de cette obligation contraignante.

Un protocole facultatif à la Convention relative aux droits de l'enfant, concernant spécifiquement la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, a été adopté le 25 mai 2000 et est entré en vigueur le 18 janvier 2002.

---

[328] Cette convention est accessible à l'adresse suivante : http://www2.ohchr.org/french/law/crc.htm.
[329] Voir la page relative à la Convention, sur le site web des Nations Unies : http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=fr.
[330] Voir les articles 19, 32, 34, 36, et 39 de la Convention.
[331] Article 17 de la Convention
[332] Article 29d de la Convention
[333] Respectivement, articles 2 et 23.1 de la Convention.
[334] Le Ministre australien Stephen Conroy déclara, lors d'une interview télévisuelle, que « *s'agissant des sites web étrangers, pour le moment, la seule chose que l'ACMA* [Autorité australienne des communications et des médias, *ndlt*] *peut faire, lorsqu'ils sont identifiés, est d'écrire au serveur étranger pour lui demander de ne pas le faire – ce qui se résume à rien, en pratique* » (traduit de l'anglais). Voir http://news.sbs.com.au/insight/episode/index/id/59#watchonline (visité pour la dernière fois le 3 septembre 2009).

La Convention relative aux droits des personnes handicapées

La Convention des Nations Unies relative aux droits des personnes handicapées du 13 décembre 2006[335] énonce spécifiquement les droits des personnes handicapées. Ce texte a pour objectif « *de promouvoir, protéger et assurer la pleine et égale jouissance de tous les droits de l'homme et de toutes les libertés fondamentales par les personnes handicapées et de promouvoir le respect de leur dignité intrinsèque* »[336], reconnaissant entre autres « *qu'il importe que les personnes handicapées aient pleinement accès aux équipements physiques, sociaux, économiques et culturels, à la santé et à l'éducation ainsi qu'à l'information et à la communication pour jouir pleinement de tous les droits de l'homme et de toutes les libertés fondamentales* »[337]. Son article 4.1(f) prévoit que « *les Etats Parties s'engagent à garantir et à promouvoir le plein exercice de tous les droits de l'homme et de toutes les libertés fondamentales de toutes les personnes handicapées sans discrimination d'aucune sorte fondée sur le handicap* », notamment en entreprenant ou encourageant « *la recherche et le développement de biens, services, équipements et installations de conception universelle, selon la définition qui en est donnée à l'article 2 de la présente Convention, qui devraient nécessiter le minimum possible d'adaptation et de frais pour répondre aux besoins spécifiques des personnes handicapées, (en encourageant) l'offre et l'utilisation de ces biens, services, équipements et installations et (en encourageant) l'incorporation de la conception universelle dans le développement des normes et directives* ». Dans le cadre de ce même engagement, les Etats doivent encore « *g) entreprendre ou encourager la recherche et le développement et encourager l'offre et l'utilisation de nouvelles technologies - y compris les technologies de l'information et de la communication, les aides à la mobilité, les appareils et accessoires et les technologies d'assistance - qui soient adaptées aux personnes handicapées, en privilégiant les technologies d'un coût abordable* ».

La Convention internationale sur l'élimination de toutes les formes de discrimination raciale

Une autre convention des Nations Unies qui se trouve être importante dans le cadre de la discussion sur le filtrage est la Convention internationale sur l'élimination de toutes les formes de discrimination raciale[338], signée par 173 Etats[339]. Cette Convention vise à protéger les personnes contre « *toute distinction, exclusion, restriction ou préférence fondée sur la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, qui a pour but ou pour effet de détruire ou de compromettre la reconnaissance, la jouissance ou l'exercice, dans des conditions d'égalité, des droits de l'homme et des libertés fondamentales dans les domaines politique, économique, social et culturel ou dans tout autre domaine de la vie publique* »[340].

L'ensemble de ces droits est encore protégé, d'une manière substantiellement analogue, à l'échelle du Conseil de l'Europe. La Convention de sauvegarde des droits de l'Homme et des libertés fondamentales du Conseil de l'Europe protège notamment tous les droits du PIDCP que nous avons précédemment énumérés[341].

6.5.2.2 Le Conseil de l'Europe

Le Conseil de l'Europe a été créé le 5 mai 1949 par 10 Etats et compte aujourd'hui 47 pays membres[342]. Son premier objectif est « *de créer sur tout le continent européen un espace*

---

[335] Cette Convention est disponible à l'adresse : http://www2.ohchr.org/french/law/disabilities-convention.htm.
[336] Article 1 de la Convention.
[337] Préambule de la Convention, v.
[338] Adoptée et ouverte à la signature et à la ratification par la résolution de l'Assemblée générale n° 2106 (XX) du 21 décembre 1965, entrée en vigueur le 4 janvier 1969, disponible à l'adresse suivante : http://www2.ohchr.org/french/law/cerd.htm.
[339] Voir le site web du Comité pour l'élimination de la discrimination raciale, disponible à l'adresse suivante :: http://www2.ohchr.org/french/bodies/cerd/index.htm.
[340] Article 1 de la Convention.
[341] Respectivement articles 2, 3, 5, 8, 9 et 10.
[342] « Qui sommes-nous? » in « Le Conseil de l'Europe en bref », site web du Conseil de l'Europe, http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=fr.

démocratique et juridique commun, en veillant au respect de valeurs fondamentales : les droits de l'homme, la démocratie et la prééminence du droit »[343].

La Convention européenne des droits de l'Homme (CEDH)

La création de cet espace juridique et démocratique se fonde principalement sur les principes établis par la ***Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (Convention européenne des droits de l'Homme ou CEDH)*** signée à Rome le 4 novembre 1950 et entrée en vigueur le 3 septembre 1953, qui est considérée comme « *faisant de plus en plus figure de Charte constitutionnelle européenne et d'axe privilégié de la construction d'une Europe unie et démocratique* » [344].

L'innovation la plus importante de cette Convention est le « *mécanisme institutionnel* » qu'elle crée afin de contrôler le respect des droits et libertés qu'elle consacre. Initialement composé de trois organes de décision (la Commission pour les investigations et les conciliations, la Cour pour les décisions judiciaires et le Comité des ministres pour les décisions politiques), ce mécanisme de contrôle consiste aujourd'hui uniquement en la Cour européenne des droits de l'Homme, substituée aux trois organes de décision précédents par le protocole n° 11 adopté le 11 mai 1994 et entré en vigueur le 1er novembre 1998[345]. En conséquence, l'ensemble des violations alléguées des droits de l'Homme sont soumises directement à la Cour[346].

La manière dont la Convention européenne des droits de l'Homme est transposée dans les droits internes varie selon les pays. Généralement, l'obligation faite aux Etats de respecter les traités relatifs aux droits de l'Homme[347], sans que ces Etats ne puissent invoquer le principe de réciprocité[348], est remplie par l'adoption d'une loi, mais les pays restent libres d'utiliser les moyens qu'ils considèrent appropriés pour atteindre cet objectif[349], conformément à leur

---

[343] « Nos objectifs » in « Le Conseil de l'Europe en bref », site web du Conseil de l'Europe, http://www.coe.int/aboutCoe/index.asp?page=nosObjectifs&l=fr.

[344] Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, sous la direction de Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, éd. Dalloz, 11ème éd., 2005, page 35, n° 61. Voir aussi Pär Hallström, « The European Union – From Reciprocity to Loyalty » (« L'Union européenne – de la réciprocité à la loyauté »), Scandinavian Studies in Law, vol. 39, 2000, pages 79-88, disponible à l'adresse : http://www.cenneth.com/sisl/pdf/39-5.pdf, page 82 : « *La Convention est censée fonctionner comme une "super Constitution" européenne, qui garantit à chacun, indépendamment de sa nationalité, ses droits inclusifs* » (traduit de l'anglais).

[345] Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, sous la direction de Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, éd. Dalloz, 11ème éd., 2005, page 35, n° 61.

[346] Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, Résumé du traité, site web du Conseil de l'Europe : http://conventions.coe.int/Treaty/fr/Summaries/Html/005.htm.

[347] Voir Claudia Sciotti-Lam, L'applicabilité des traits internationaux relatifs aux droits de l'homme en droit interne, thèse, Bruylant Bruxelles, 2004, pages 35 et s.

[348] Voir Jeremy McBride, « Proportionality and the European Convention on Human Rights » (« La proportionnalité et la Convention européenne des droits de l'Homme »), in *The principle of Proportionality in the Laws of Europe* (*Le principe de proportionnalité dans les lois d'Europe*), édité par Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et s., notamment p. 28: « *La Convention est considérée, depuis ses premiers jours, comme organisant un ordre public européen qui n'est pas, de fait, sujet au principe de réciprocité, lequel prend plus généralement place dans l'application de leurs obligations internationales par les Etats* » (traduit de l'anglais), se référant à l'arrêt *Autriche c/ Italie*, 4 YBECHR 112 (1961). Voir également Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, sous la direction de Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, éd. Dalloz, 11ème éd., 2005, page 37, n° 65 ; Pär Hallström, « The European Union – From Reciprocity to Loyalty » (« L'union européenne – de la réciprocité à la loyauté »), Scandinavian Studies in Law, vol. 39, 2000, pages 79-88, notamment page 82, disponible à l'adresse : http://www.cenneth.com/sisl/pdf/39-5.pdf ; Claudia Sciotti-Lam, *L'applicabilité des traités internationaux relatifs aux droits de l'homme en droit interne*, thèse, Bruylant Bruxelles, 2004, page 297 et s. Le principe de réciprocité permet à un Etat de ne pas exécuter l'un de ses engagements lorsqu'une autre partie au Traité n'exécute pas les siennes.

[349] Voir Claudia Sciotti-Lam, *L'applicabilité des traités internationaux relatifs aux droits de l'homme en droit interne*, thèse, Bruylant Bruxelles, 2004, page 65 *et s*. Voir aussi Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, Résumé du traité, site web du Conseil de l'Europe : http://conventions.coe.int/Treaty/fr/Summaries/Html/005.htm : « *Les Parties s'engagent à reconnaître ces droits et libertés à toute personne relevant de leur juridiction* ».

Constitution[350]. En conséquence, la place de la Convention dans la hiérarchie des normes n'est pas la même dans tous les pays qui respectent le texte international.

Par exemple, la Convention a été directement intégrée en droit interne par la Constitution aux Pays-Bas, en Belgique, en Espagne et en Bulgarie, et a été intégrée par la loi à Malte, en Finlande, au Danemark, en Islande, en Norvège, au Royaume-Uni et en Suède. En ce qui concerne la place de la Convention dans la hiérarchie des normes, elle connaît une force supra-constitutionnelle aux Pays-Bas, une force constitutionnelle en Autriche, une force infra-constitutionnelle mais supra-légale en Belgique, en Grèce, en Suisse et en Espagne, et une simple force de loi en Allemagne, en Turquie et en Finlande[351]. En France, la Convention est directement intégrée en droit interne par la Constitution, dont l'article 55 énonce que « *les traités ou accords régulièrement ratifiés ou approuvés ont, dès leur publication, une autorité supérieure à celle des lois, sous réserve, pour chaque accord ou traité, de son application par l'autre partie* »[352]. La Convention a en conséquence une force infra-constitutionnelle mais supra-légale, même si la loi nationale lui est postérieure[353].

La Convention européenne des droits de l'Homme est considérée comme étant l'un des textes fondamentaux assurant la protection du droit des enfants, puisqu'elle s'applique à tout être humain[354]. Il en est de même de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains[355]. Parmi les autres instruments du Conseil de l'Europe qui protègent les enfants nous pouvons également mentionner la Convention sur la protection des enfants contre l'exploitation et les abus sexuels[356], laquelle n'est toutefois pas encore entrée en vigueur en raison d'une pénurie de ratifications[357].

La Convention sur la cybercriminalité

La Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001[358] organise également la protection des mineurs, lesquels sont ici encore définis comme « *toute personne âgée de moins de 18 ans* »[359], en demandant aux Etats membres de criminaliser la pornographie mettant en scène des enfants. Cette Convention, qu'ont ratifiée ou à laquelle ont adhéré 26 pays[360], ne consacre pas en elle-même le droit des enfants à ne pas être victimes d'une production d'images à caractère pédopornographique. Il est pour cette raison difficile de considérer un tel droit comme un droit fondamental autonome. Ceci dit, il est possible de voir la Convention sur la cybercriminalité comme proposant des mécanismes propres à assurer la protection de droits par ailleurs consacrés par d'autres textes internationaux, comme le droit d'être protégé contre la violence et le droit au développement,

---

[350] Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, sous la direction de Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, éd. Dalloz, 11ème éd., 2005, page 39, n° 68.

[351] Frédéric Sudre, op. cit., page 39, n° 68.

[352] Frédéric Sudre, op. cit., page 39, n° 68. La seconde partie de l'article ne reçoit pas application puisque le principe de réciprocité ne s'applique pas à la CEDH.

[353] Frédéric Sudre, op. cit., page 39, n° 69.

[354] Voir le site web du Conseil de l'Europe, « Construire une Europe pour et avec les enfants », Textes fondamentaux relatifs à l'enfance, disponible à l'adresse suivante : http://www.coe.int/t/transversalprojects/children/keyLegalTexts/Default_fr.asp.

[355] Convention sur la lutte contre la traite des êtres humains, STCE n° 197, ouverte à la signature le 16 mai 2005, entrée en vigueur le 1er février 2008 (16 signatures non suivies de ratifications et 25 ratifications/adhésions à la date du 19 août 2009), disponible à l'adresse suivante : http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=197&CM=8&CL=FRE.

[356] Convention sur la protection des enfants contre l'exploitation et les abus sexuels, STCE n° 201, ouverte à la signature le 25 octobre 2007. La Convention est disponible à l'adresse suivante : http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=7&DF=14/01/2010&CL=FRE.

[357] Le 19 août 2009, 35 pays avaient signé la Convention sans l'avoir ratifiée et 2 pays l'avaient ratifiée ou y avaient adhéré, tandis que 5 ratifications incluant au moins trois Etats membres du Conseil de l'Europe sont nécessaires pour permettre à la Convention d'entrer en vigueur. Voir la page y afférente sur le site web du Conseil de l'Europe, disponible à l'adresse suivante : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=7&DF=14/01/2010&CL=FRE.

[358] Cette Convention est disponible à l'adresse : http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm.

[359] Article 9, 3 de la Convention.

[360] Voir la page y afférente sur le site web du Conseil de l'Europe, disponible à l'adresse suivante : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=7&DF=14/01/2010&CL=FRE.

affirmés par la Convention des Nations Unies relative aux droits de l'enfant[361] (notons par ailleurs que l'utilisation, le recrutement ou l'offre d'un enfant pour la production de matériel pornographique sont également prohibés par la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants de 1999 - Convention numéro 182 -, qui a été ratifiée par 171 pays).

La Convention européenne des droits de l'Homme bénéficie aussi aux personnes qui souffrent d'un handicap. Toutefois, le Conseil de l'Europe entend protéger ces personnes par le biais d'autres initiatives. Peut notamment être citée la Recommandation Rec(2006)5 du Comité des ministres aux Etats membres « *sur le Plan d'action du Conseil de l'Europe pour la promotion des droits et de la pleine participation des personnes handicapées à la société : améliorer la qualité de vie des personnes handicapées en Europe 2006-2015* »[362]. Ce document prévoit notamment dans sa section 1.2.1 que « *les Etats membres continueront d'œuvrer dans le cadre des droits de l'homme et de la lutte contre la discrimination afin d'accroître l'autonomie, la liberté de choix et la qualité de vie des personnes handicapées, et de provoquer une prise de conscience du handicap comme faisant partie de la diversité humaine* ». Il ajoute que « *le Plan tient dûment compte des instruments, traités et programmes européens et internationaux pertinents, et notamment des travaux en cours sur le projet de convention internationale des Nations Unies sur les droits des personnes handicapées* ».

S'agissant des libertés qui pourraient être concernées dans le cadre d'une discussion sur le filtrage d'Internet, il est enfin important de mentionner le protocole n°12 à la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, qui prévoit en son article 1 une « *interdiction générale de la discrimination* ».

La protection des personnes contre la discrimination est également assurée au niveau de l'Union européenne.

6.5.2.3 L'Union européenne

L'Union européenne compte aujourd'hui 27 pays, qui sont tous membres du Conseil de l'Europe[363]. Même si l'Union européenne n'a pas pour l'heure adhéré à la Convention européenne des droits de l'Homme, essentiellement car les traités doivent être modifiés à cette fin[364], l'Union européenne a reconnu la nécessité de préserver les libertés fondamentales et de respecter la CEDH.

Le Traité sur l'Union européenne énonce par exemple en son article 6 que « *l'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et des libertés fondamentales, ainsi que de l'État de droit, principes qui sont communs aux États membres* » et que « *l'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles*

---

[361] La Convention sur la cybercriminalité fait par exemple référence à la Convention des Nations Unies relative aux droits de l'enfant, dans son préambule, § 12.

[362] Cette recommandation a été adoptée par le Comité des ministres le 5 avril 2006 lors de la 961ème réunion des délégués des ministres. Elle est disponible à l'adresse suivante : https://wcd.coe.int/ViewDoc.jsp?id=986837&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

[363] « Ne pas confondre » in « Le Conseil de l'Europe en bref », site web du Conseil de l'Europe, http://www.coe.int/aboutCoe/index.asp?l=fr&page=nepasconfondre.

[364] Voir l'Avis 2/94 de la Cour de justice du 28 mars 1996, Adhésion de la Communauté à la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, disponible à l'adresse suivante : http://www.pravo.hr/_download/repository/Opinion_2_1994.pdf (sommaire en français disponible à l'adresse : http://www.ena.lu/avis_2-94_cour_justice_28_mars_1996-010003222.html). Voir également « Adhésion de l'Union européenne à la Convention européenne des Droits de l'Homme », Audition organisée par la Commission des questions juridiques et des droits de l'homme, à Paris, le 11 septembre 2007, Intervention de Florence Benoît-Rohmer, Professeur à l'Université Robert Schuman (Strasbourg), Projet - 10.09.2007, disponible sur le site web du Parlement à cette adresse: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/background_document_rohmer_/background_document_rohmer_fr.pdf: « *Après avoir longtemps fait l'objet de fortes réserves de plusieurs Etats membres de l'Union, l'adhésion de l'Union à la CEDH est aujourd'hui unanimement soutenue* ».

communes aux États membres, en tant que principes généraux du droit communautaire »[365]. L'article 7 du Traité organise une procédure qui permet au Conseil de « *constater l'existence d'une violation grave et persistante par un État membre* » de ces principes, après avoir recueilli l'« *avis conforme du Parlement européen* », et de « *décider de suspendre certains des droits découlant de l'application du présent traité à l'État membre en question, y compris les droits de vote du représentant du gouvernement de cet État membre au sein du Conseil* ».

La Cour européenne de justice, le 28 mars 1996, a également considéré que « *le respect des droits de l'Homme est (…) une condition de la légalité des actes communautaires* »[366]. La Charte des droits fondamentaux de l'Union européenne, qui fut incluse dans la Constitution européenne que la France et les Pays-Bas rejetèrent, est elle-même « *le premier document formel de l'Union européenne à associer et déclarer l'ensemble des valeurs et droits fondamentaux (économiques et sociaux de même que civils et politiques) dont les citoyens européens devraient bénéficier* », rassemblant « *les droits existants qui étaient auparavant dispersés au sein de nombreuses sources internationales* », dans l'objectif de « *rendre ces droits plus visibles* »[367]. Par ailleurs, la nécessité de respecter les libertés fondamentales est généralement précisée au sein des directives européennes[368].

En conséquence, appartenir à l'Union européenne implique de respecter les droits de l'Homme et les libertés fondamentales, particulièrement ceux et celles qui se trouvent protégés par la Convention européenne des droits de l'Homme.

L'Union européenne met l'accent sur certaines catégories de droits, à l'instar des textes internationaux que nous avons précédemment analysés, tels que les droits de l'enfant, les droits des personnes handicapées ou le droit de ne pas subir de discriminations.

- En premier lieu, l'Union européenne a adopté de nombreux textes et instruments relatifs à la protection des droits de l'enfant[369]. Parmi ces derniers, figure la Décision-cadre 2004/68/JAI du Conseil, en date du 22 décembre 2003, relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie[370], laquelle est actuellement en cours de révision.
- En deuxième lieu, le plan d'action de l'Union européenne en faveur des personnes handicapées 2003-2010 a pour objectif « *de faire de l'égalité des chances une réalité pour les personnes handicapées* »[371]. Il entend notamment « *permettre aux personnes handicapées de disposer des mêmes choix personnels et du même degré de contrôle de leur quotidien que les autres personnes* » [372].
- En troisième lieu, parce que l'Union européenne avait besoin de combattre « *la discrimination fondée sur des motifs autres que le sexe* », le Traité d'Amsterdam introduisit « *l'article 13 qui habilite la Communauté à agir pour lutter contre la*

---

[365] Union européenne, versions consolidées du traité sur l'Union européenne et du traité instituant la communauté européenne, Journal Officiel de l'Union européenne, 29 décembre 2006, C 321 E/1 à 331, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:321E:0001:0331:FR:pdf.

[366] Avis 2/94 de la Cour de justice du 28 mars 1996, Adhésion de la Communauté à la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, disponible à l'adresse suivante : http://www.pravo.hr/_download/repository/Opinion_2_1994.pdf (sommaire en français disponible à l'adresse : http://www.ena.lu/avis_2-94_cour_justice_28_mars_1996-010003222.html), n° 34.

[367] Traduit de l'anglais. Site web de la Charte des droits fondamentaux de l'Union européenne, « introduction », disponible à l'adresse suivante : http://www.eucharter.org/.

[368] Voir par exemple la Directive 95/46/CE, § 1: « Considérant que les objectifs de la Communauté, énoncés dans le traité, tel que modifié par le traité sur l'Union européenne, consistent (…) à préserver et conforter la paix et la liberté, et à promouvoir la démocratie en se fondant sur les droits fondamentaux reconnus dans les constitutions et les lois des États membres, ainsi que dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ».

[369] La liste complète peut être trouvée sur le site web de l'Union européenne à cette adresse : http://eur-lex.europa.eu/fr/dossier/dossier_30.htm.

[370] J.O.C.E. du 20 janvier 2004, L 013, pp. 0044-0048, disponible à cette adresse : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:FR:HTML.

[371] Voir le site web de la Commission européenne, « emploi, affaires sociales et égalité des chances », « Le plan d'action de l'UE en faveur des personnes handicapées », disponible à cette adresse : http://ec.europa.eu/social/main.jsp?catId=430&langId=fr.

[372] Voir le site web de la Commission européenne, « emploi, affaires sociales et égalité des chances », « personnes handicapées », disponible à cette adresse : http://ec.europa.eu/social/main.jsp?catId=429&langId=fr.

discrimination fondée sur une série de nouveaux motifs, à savoir la race ou l'origine ethnique, la religion ou les convictions, l'âge, un handicap et l'orientation sexuelle »[373]. Sur cette base, le Conseil de l'Union européenne adopta la Directive sur l'égalité raciale du 29 juin 2000, qui interdit notamment « *toute discrimination basée sur la race ou l'origine ethnique* »[374].

Ces dispositions particulières peuvent être vues soit comme des déclarations de droits fondamentaux, soit, a minima, comme des indications sur les moyens à mettre en place pour assurer le respect de certains droits ou libertés fondamentaux consacrés dans la CEDH et ses protocoles additionnels, ainsi que dans d'autres instruments internationaux.

Parmi l'ensemble des droits et libertés que nous avons analysés, certains peuvent apparaître en opposition avec une mesure de filtrage d'Internet, tandis que d'autres pourraient être invoqués pour justifier cette même mesure.

[373] Voir le site web de l'UE, « Synthèse de la législation de l'UE », « Egalité et non-discrimination dans l'Union européenne élargie », disponible à l'adresse suivante : http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/l14157_fr.htm.

[374] Voir le site web de l'UE, « Synthèse de la législation de l'UE », « Egalité de traitement sans distinction de race ou d'origine ethnique », disponible à l'adresse suivante : http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33114_fr.htm.

6.6 Les libertés fondamentales susceptibles d'entrer en conflit avec le filtrage

Certains droits de l'Homme et libertés fondamentales pourraient se trouver en conflit avec une mesure de filtrage, tandis que la mise en place d'une telle mesure technique pourrait être justifiée par la nécessité de protéger d'autres droits.

Un équilibre doit donc être fait entre ces différents droits et libertés (ainsi que nous l'expliquerons dans la section 7.6), à la lumière de la clause d'ordre public que nous décrirons en détail au chapitre 7.

Le filtrage d'Internet peut en effet avoir un impact sur certains droits de l'Homme et libertés fondamentales qui représentent une part importante des valeurs que la communauté internationale et l'Union européenne se sont engagées à respecter.

- En premier lieu, une mesure de filtrage d'Internet peut constituer une ingérence dans le droit au respect de la vie privée, lorsqu'elle permet ou requiert la conservation de données électroniques protégées par la confidentialité, ou lorsqu'elle empêche les individus de s'adonner à certains usages d'Internet, les privant par là-même de la possibilité de nouer certaines relations ou de faire certains choix de connexion. Dans ce dernier cas, les limitations sont portées au droit à la liberté de la vie privée. Ce type de limitations est particulièrement présent dans les situations inévitables de sur-blocage (ou filtrage excessif), lequel impacte des sites web totalement innocents.
- En deuxième lieu, une mesure de filtrage peut constituer une ingérence dans le droit à la liberté d'expression, lorsqu'il empêche les personnes d'accéder à certaines informations en ligne ou de rendre disponibles ces mêmes informations. Le filtrage a de fait un impact négatif sur la diffusion de l'information, sa communication et sa réception.
- En troisième lieu, une mesure de filtrage d'Internet peut constituer une ingérence dans les droits spécifiques dont bénéficient certaines catégories de personnes, tels que le droit des personnes handicapées d'accéder aux communications électroniques.
- En quatrième lieu, le filtrage peut être vu comme une alternative au respect de l'obligation, posée par la Convention sur les droits de l'enfant, de prendre toutes les mesures internationales appropriées en vue de prévenir l'exploitation des enfants à des fins pornographiques. Ceci est illustré par les commentaires du Ministre australien (mentionnés plus haut), qui déclara que la transmission de signalements n'aboutissait à « rien ».

6.6.1 Le droit au respect de la vie privée et familiale

6.6.1.1 Les textes principaux

Le droit au respect de la vie privée et familiale est consacré à l'article 12 de la Déclaration universelle des droits de l'Homme, à l'article 17 du Pacte international sur les droits civils et politiques, à l'article 8 de la Convention européenne des droits de l'Homme et à l'article 7 de la Charte des droits fondamentaux de l'Union européenne, laquelle a la même signification et la même portée que la Convention européenne des droits de l'Homme[375]. Ce droit est en conséquence un droit de l'Homme et une liberté fondamentale[376], et, de fait, dans de nombreux Etats, une liberté publique. Il bénéficie directement aux adultes comme aux enfants, même si la Convention des Nations Unies relative aux droits de l'enfant le complète en consacrant spécifiquement le droit des enfants au respect de leur vie privée en son article 16.

Tous ces textes protègent les individus des immixtions arbitraires dans leur vie privée et familiale, leur domicile ou leurs correspondances, et des atteintes à leur honneur ou à leur réputation (seule la CEDH n'est pas explicite sur cet aspect – mais la Cour européenne des droits de l'Homme protège la réputation des individus sous le visa de l'article 8[377]). La DUDH précise que « *toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». Le PIDCP apporte la même précision, et ajoute que **les immixtions doivent être légales**, ce qui permet de s'interroger sur certaines initiatives de filtrage conduites par l'Industrie, qui n'ont aucune base légale. La Convention européenne des droits de l'Homme permet quant-à-elle certaines immixtions lorsque ces dernières répondent aux conditions décrites dans la dite « clause d'ordre public », laquelle sera décrite au chapitre 7 et qui inclut, elle-aussi, le principe de légalité.

Le droit au respect de la vie privée est encore protégé, au niveau national, par différentes Constitutions. Ce droit est par exemple protégé, selon le Conseil constitutionnel français, « *par les articles 2 et 4[378] de la Déclaration de 1789* »[379], cette dernière appartenant au dit « bloc de constitutionnalité » français. Le Conseil constitutionnel français protège également certains aspects du droit au respect à la vie privée sous le visa de la liberté individuelle[380], dont les règles doivent être fixées par le Parlement, conformément à l'article 34 de la

---

[375] Site web de la Charte des droits fondamentaux de l'Union européenne, « Art 7. Respect for private and family life » (Article 7 – Respect de la vie privée et familiale), disponible à cette adresse : http://www.eucharter.org/home.php?page_id=14.

[376] Voir également Emmanuel Dreyer, « Le respect de la vie privée, objet d'un droit fondamental », Comm., com. élec. n° 5, mai 2005, Etudes, 18.

[377] Voir par ex. *Fayed c/ Royaume-Uni,* arrêt du 21 septembre 1994, séries A, n° 294 B, pp. 50-51, § 67; *Chauvy et autres c/France*, n° 64915/01, § 70, CEDH 2004, VI ; *Gunnarsson c/ Islande*, n° 4591/04, 20 octobre 2005. Pour toutes ces références, voir « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », Cour européenne des droits de l'Homme, 24 janv. 2007, disponible à cette adresse : http://www.echr.coe.int/NR/rdonlyres/49779DCC-6DBA-49BA-B1F1-4B554D860E56/0/COURT_n1968041_v2_Pointscl%C3%A9s_de_jurisprudence__Les_notions_de__Vie_priv%C3%A9e__et_de__Vie_familiale__.pdf.

[378] Article 2 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression »; Article 4: « La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société, la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi ». La Déclaration est disponible sur le site web du Conseil constitutionnel à cette adresse : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/la-constitution/la-constitution-du-4-octobre-1958/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789.5076.html .

[379] Voir par ex. la décision n° 2004-492 DC, 2 mars 2004, J.O. 10 mars 2004, page 4 637, considérant n° 4.

[380] Les autres éléments de la liberté individuelle sont, en droit français, la liberté d'aller et venir, le droit de ne pas être arbitrairement arrêté ou séquestré, le droit d'être jugé avec toutes les garanties légales et le principe d'inviolabilité du domicile. Voir Jacques Robert et Jean Duffar, *Droits de l'homme et libertés fondamentales*, éd. Montchrestien, 7ème éd., 1999, p. 27 ; l'article 136 du Code de procédure pénale ; Estelle De Marco, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », 4 juin 2009, Juriscom.net, page 3, disponible à cette adresse : http://www.juriscom.net/uni/visu.php?ID=1133.

Constitution[381]. Enfin, le droit à la vie privée et familiale est protégé par le juge civil français, et certains de ses aspects bénéficient d'une protection pénale, tels que le droit au respect des correspondances[382].

6.6.1.2 La vie privée et le filtrage d'Internet

Le contenu précis du droit au respect à la vie privée varie selon les époques et selon les pays, et est principalement défini par les juges et la doctrine, en ce que les textes n'en déclarent généralement que le principe, sans autres précisions. En 1965, la Cour suprême des Etats-Unis définit ce droit comme étant celui, pour tout individu, « *de prendre seul les décisions dans la sphère de sa vie privée* ». Précédemment, deux juristes américains avaient défini ce même droit comme « *le droit d'être laissé tranquille* »[383]. En France, l'analyse des décisions de justice permet au Professeur François Terré de voir la vie privée comme un ensemble composé de différents cercles. Au centre, se trouve la « *vie personnelle* », laquelle comprend « *les données tenant à l'identité, à l'origine raciale, à la santé physique ou mentale, au caractère ou aux mœurs* »[384]. Les informations génétiques compteraient également parmi les informations inhérentes à la vie privée, même si leur statut n'est pas tranché. Un cercle plus large comprend ensuite les données relatives à la « *vie sentimentale, conjugale, extraconjugale (et) familiale* », aux « *relations amicales* », et à la « *participation à une réunion de caractère privé* »[385]. Enfin, le domicile[386] et la correspondance privée[387] sont également protégés sous le visa du respect de la vie privée.

La Cour européenne des droits de l'Homme est considérée comme ayant une conception plus extensive de la vie privée que plusieurs pays[388], même si elle « *ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de "vie privée"* »[389], qui est

---

[381] Le Conseil constitutionnel considère que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle : décision n° 94-352 DC, 18 janv. 1995, J.O. du 21 janvier 1995, page 1154 et JCP 1995, II, 22 525, note Frédérique Lafay. Le Conseil a également analysé la mise en place de dispositifs techniques de captation, fixation, transmission et enregistrement de paroles ou d'images sans le consentement des intéressés à lumière de la liberté individuelle : décision n° 2004-492 DC, 2 mars 2004, J.O.R.F. du 10 mars 2004, p. 4 637. Le Conseil étend encore la notion à certains fichiers de données nominatives : décision n° 2004-492 DC, 2 mars 2004, J.O.R.F. du 10 mars 2004, p. 4 637, § n° 64. Sur tous ces éléments, voir Estelle De Marco, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », op. cit., et Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 20. La Constitution française est disponible sur le site web du Conseil Constitutionnel à cette adresse : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/la-constitution/la-constitution-du-4-octobre-1958/la-constitution-du-4-octobre-1958.5071.html.

[382] Voir par exemple l'article 226-15 du Code pénal français : « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende ». « Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions ».

[383] Pour la discussion et les deux citations, voir Pierre Tabatoni, « Avant-propos », in *La protection de la vie privée dans la société d'information*, sous la dir. de Pierre Tabatoni, tome 1, Cahier des sciences morales et politique, PUF, 1ère éd., janv. 2002, page 4.

[384] François Terré, « La vie privée », in *La protection de la vie privée dans la société d'information*, sous la dir. de Pierre Tabatoni, tomes 3, 4 et 5, Cahier des sciences morales et politique, PUF, 1ère éd., janv. 2002, page 138. Voir aussi Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 41 et s.

[385] François Terré, « La vie privée », op. cit., page 139. Estelle De Marco, *L'anonymat sur Internet et le droit*, op. cit., n° 41.

[386] Voir par ex. Cass. Civ. 3ème, 25 fév. 2004, Bull. civ. III, n° 41, p. 38.

[387] Voir par exemple l'arrêt dit « Nikon », Cass. soc., 2 oct. 2001, Bull. civ. V, n° 291, page 233.

[388] Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3ème éd., 1995, page 27 et s. Pour une définition de la vie privée sur le critère de la légitimité des tiers à connaître de la vie privée d'autres personnes, en remplacement des critères de la conception extensive ou restrictive de la vie privée, voir Estelle de Marco, *L'anonymat sur Internet et le droit*, op. cit., n° 109 et s.

[389] *Niemietz c/ Allemagne,* arrêt du 16 décembre 1992, séries A, n° 251 B, p. 33, § 29, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700220&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

une « *notion large* »[390]. La Cour considère toutefois qu'il serait « *trop restrictif de la limiter à un "cercle intime" où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle* »[391]. Sous le visa de l'article 8, la Cour offre protection à « *quatre domaines de l'autonomie de la personne* » (la vie privée, la vie de famille, le domicile et la correspondance), qui ne sont pas « *mutuellement exclusifs* », ce qui signifie par exemple qu'une « *mesure peut constituer une ingérence à la fois dans la vie privée et dans la vie de famille* »[392].

La seule distinction que nous pouvons retrouver dans chacune de ces définitions apparaît être une distinction entre le ***secret de la vie privée***, qui est « *l'opacité pour autrui de la vie personnelle et familiale* », et la ***liberté de la vie privée***, qui est « *le pouvoir pour une personne de prendre les partis qui lui paraissent les meilleurs pour cette part de vie* »[393]. Nous verrons que le filtrage peut se trouver en conflit avec chacun de ces aspects.

6.6.1.3 Le secret de la vie privée et le filtrage d'Internet

S'agissant du secret de la vie privée et des autres éléments de vie qui se trouvent protégés sous le visa de l'article 8 de la CEDH, la Cour européenne des droits de l'Homme protège en premier lieu l'inviolabilité du domicile[394], cette protection s'étendant aux locaux professionnels[395]. Elle protège également certains « *aspects de l'identité physique et sociale d'un individu* »[396], ainsi que l'inviolabilité des correspondances[397], ces dernières incluant les lettres[398], les conversations téléphoniques[399], les messages par bipeur[400], les correspondances

---

[390] Voir par exemple *Peck c/ Royaume-Uni*, n° 44647/98, § 57, CEDH 2003-I, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=703325&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[391] *Niemietz c/ Allemagne*, arrêt du 16 décembre 1992, séries A, n° 251 B, p. 33, § 29, disponible à cette adresse: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700220&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. Voir « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », Cour européenne des droits de l'Homme, 24 janv. 2007, disponible à cette adresse : http://www.echr.coe.int/NR/rdonlyres/49779DCC-6DBA-49BA-B1F1-4B554D860E56/0/COURT_n1968041_v2_Pointscl%C3%A9s_de_jurisprudence_Les_notions_de_Vie_priv%C3%A9e_et_de_Vie_familiale_.pdf.

[392] Voir par exemple *Menteş et autres c/ Turquie*, arrêt du 28 novembre 1997, Recueil 1997, VIII, p. 2711, § 73 ; *Stjerna c/ Finlande*, arrêt du 25 novembre 1994, séries A, n° 299 B, p. 60, § 37 ; *López Ostra c/ Espagne*, arrêt du 9 décembre 1994, séries A, n° 303 C, p. 54, § 51 ; *Burghartz c/ Suisse*, arrêt du 22 février 1994, séries A, n° 280 B, p. 53, § 24 ; *Płoski c/ Pologne*, n° 26761/95, § 32, 12 novembre 2002. Sur la discussion, ces arrêts et pour chaque citation, voir « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », Cour européenne des droits de l'Homme, 24 janv. 2007, disponible à cette adresse : http://www.echr.coe.int/NR/rdonlyres/49779DCC-6DBA-49BA-B1F1-4B554D860E56/0/COURT_n1968041_v2_Pointscl%C3%A9s_de_jurisprudence_Les_notions_de_Vie_priv%C3%A9e_et_de_Vie_familiale_.pdf.

[393] Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3ème éd., 1995, page 12. Voir aussi Estelle De Marco, *L'anonymat sur Internet et le droit*, op. cit., pages 99 et s.

[394] Arrêt *Chappell*, 30 mars 1989, Court publications, n° 152, série A ; Niemietz c/ Allemagne, 16 décembre 1992, volume n° 251B, série A ; Voir Pierre Kayser, op. cit., pages 43 et 44 et note n° 158.

[395] Pierre Kayser, op. cit., page 44, se référant à l'arrêt *Niemietz c/ Allemagne*, op. cit.

[396] *Mikulić c/ Croatie*, n° 53176/99, § 53, CEDH 2002 II, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=702462&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. Voir aussi « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », Cour européenne des droits de l'Homme, op. cit.

[397] Voir par exemple *B.C. c/ Suisse*, n° 21353/93, décision de la Commission du 27 février 1995 ; *Silver et autres c/ Royaume-Uni*, arrêt du 25 mars 1983, séries A, n° 61, p. 32, § 84.

[398] Voir par exemple *Silver et autres c/ Royaume-Uni*, arrêt du 25 mars 1983, séries A, n° 61, p. 32, § 84.

[399] Voir par exemple *Malone c/ Royaume-Uni*, arrêt du 2 août 1984, séries A, n° 28, p. 21, § 41.

[400] *Taylor-Sabori c/ Royaume-Uni*, n° 47114/99, 22 octobre 2002. Sur cette question et les deux précédentes, voir « Points-clés de jurisprudence, les notions de "domicile" et de "correspondance" », Cour européenne des droits de l'Homme, 31/01/2007, disponible à l'adresse suivante : http://www.echr.coe.int/NR/rdonlyres/BEFD4F63-0B4A-4A36-A7C7-59FBF487A4BE/0/COURT_n1968047_v2_Pointscl%C3%A9s_de_jurisprudence_Les_notions_de_Domicile_et_de_Correspondance_a.pdf.

professionnelles[401], les correspondances téléphoniques en provenance et à destination de locaux professionnels[402] et les communications électroniques[403].

Le principe d'inviolabilité des correspondances, sur le fondement duquel la Cour européenne des droits de l'Homme protège « *le caractère confidentiel des communications privées* »[404], est l'une des libertés fondamentales qui pourraient se trouver directement heurtées par une mesure de filtrage d'Internet. La notion de correspondance a été définie par la doctrine comme « *une communication personnelle et temporelle, susceptible d'interactivité, adressée à des personnes déterminées et individualisées* »[405]. Cette définition est généralement considérée comme s'appliquant aux correspondances protégées par le Code pénal français. Elle se trouve de fait très stricte et pourrait correspondre à la définition des correspondances de plusieurs pays. Le contenu de cette définition qualifie tant le support de l'information que l'information elle-même, pendant le temps de sa transmission. En conséquence, tout moyen de communication permettant l'interactivité peut devenir le support d'une correspondance, comme l'email, le FTP ou le pair à pair (« *peer to peer* »)[406]. Le web peut lui-même être utilisé à des fins de correspondance, par exemple lorsque l'expéditeur et le destinataire utilisent un espace web privé pour échanger des informations, espace qui peut être un forum privé de discussion ou l'espace *ad hoc* d'une boite aux lettres électronique privée, sur lequel chacun d'entre eux est en mesure de se connecter pour discuter.

En fonction de l'objet à filtrer (contenu d'un certain type, protocole de communication), des moyens utilisés pour mettre en place ce filtrage et des règles additionnelles qui sont potentiellement ajoutées pour atteindre l'objectif particulier du mécanisme global (journalisation (« *logs* »), enregistrements, etc.), une mesure de filtrage peut parfois conduire à la conservation du contenu d'un message, ou de certains éléments de ce contenu, en relation avec une personne spécifique, sans le consentement de cette dernière. Une telle situation peut être considérée comme constituant une ingérence dans l'exercice du droit protégé sous le visa de l'article 8 de la CEDH. La Cour européenne des droits de l'Homme a en effet spécifiquement précisé que « *la collecte et la conservation, à l'insu de la requérante, de données à caractère personnel se rapportant à l'usage qu'elle faisait du téléphone, du courrier électronique et de l'Internet ont constitué une ingérence dans l'exercice du droit de l'intéressée au respect de sa vie privée et de sa correspondance, au sens de l'article 8* »[407].

La définition des correspondances

Il pourrait être dit que, prenant acte de la définition restrictive que nous avons retenue de la notion de « correspondance », les communications d'une autre nature entre les personnes pourraient être sujettes à de plus importantes restrictions, sans que ces dernières ne puissent

[401] Pierre Kayser, op. cit., page 44, se référant à l'arrêt *Niemietz c/ Allemagne*, op. cit.

[402] *Kopp c/ Suisse*, arrêt du 25 mars 1998, Recueil 1998, II, p. 539, § 50 ; *Halford c/ Royaume-Uni*, arrêt du 25 juin 1997, Recueil 1997, III, p. 1016, §§ 44-46 ; cités par « Points-clés de jurisprudence, les notions de "domicile" et de "correspondance" », op cit.

[403] Voir *Copland c/ Royaume-Uni*, n° 62617/00, 3 avril 2007, § 41 : « Selon la jurisprudence de la Cour, les appels téléphoniques émanant de locaux professionnels sont *a priori* compris dans les notions de "vie privée" et de "correspondance" au sens de l'article 8 § 1 (*Halford* précité, § 44, et *Amann c. Suisse* [GC], n° 27798/95, § 43, CEDH 2000-II). Il s'ensuit logiquement que les messages électroniques envoyés depuis le lieu de travail doivent jouir de la même protection au titre de l'article 8, tout comme les éléments recueillis au moyen d'une surveillance de l'usage qu'une personne fait de l'Internet ». L'arrêt est disponible à l'adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=815062&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[404] « Points-clés de jurisprudence, les notions de "domicile" et de "correspondance" », op. cit., se référant à l'arrêt *B.C. c/ Suisse*, n° 21353/93, décision de la Commission du 27 février 1995.

[405] Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 637. Voir aussi Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille, 1999.

[406] S'agissant de la protection de certaines formes de communications électroniques, voir le paragraphe suivant ou le premier paragraphe de la présente section.

[407] *Copland c/ Royaume-Uni*, n° 62617/00, 3 avril 2007, § 44, disponible à l'adresse suivante : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=815062&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

être considérées comme des ingérences dans l'exercice du droit au secret de la vie privée. Une telle conclusion devrait être reconsidérée avec attention.

- **Le caractère personnel et temporel des correspondances**
  En premier lieu, la définition de correspondance dépend en partie du caractère personnel et temporel du contenu du message. Une communication est personnelle lorsque le contenu du message informe le destinataire de manière adaptée à sa situation, et ne peut répondre à la situation de tous. En conséquence, une publicité commerciale n'est pas personnelle, sauf si l'offre est adaptée au destinataire et à ses choix précis de consommation[408]. Une communication est temporelle lorsqu'elle appartient à une époque déterminée ; elle ne peut « *appartenir à toutes les époques : passées, présentes et futures* » [409].

  En conséquence, déterminer qu'une communication *n'est pas* une correspondance implique pour l'analyste d'en lire le contenu, lecture qui n'est pas permise s'il s'agit en réalité d'une correspondance. Les communications entre les personnes bénéficient dès lors d'une présomption de fait de correspondance, qui interdit leur violation, quel que soit leur contenu. Cette conclusion rejoint celle de la Cour européenne des droits de l'Homme, qui estime que « *le contenu de la correspondance n'a aucune incidence sur la question de l'ingérence* »[410] et qu'« *il n'y a pas de principe de minimis pour qu'il y ait ingérence : il suffit qu'une seule lettre ait été ouverte* » [411].

- **L'opacité pour les autres**
  En second lieu, le droit au respect du secret de la vie privée implique l'opacité de la vie privée pour les autres, comme cela a été précédemment dit, ce qui signifie que ces derniers n'ont pas la permission de prendre connaissance de ce qu'une personne fait, lit ou échange avec d'autres personnes, dans le cadre de sa sphère privée. Pour cette raison, toute forme de surveillance est placée sous le strict contrôle de la Cour européenne des droits de l'Homme[412].

En conclusion, même si certaines communications reçues ou émises par une personne ne sont pas des correspondances, elles restent protégées, a minima, par le droit au respect de la vie privée. Sur la base de ce principe, une mesure de filtrage qui conduirait à la surveillance ou à la conservation de données relatives au contenu de ce qu'une personne reçoit, envoie ou consulte, même s'il ne s'agit que de la consultation d'un site web d'une nature particulière, constituerait une ingérence dans le droit de cette personne au respect de sa vie privée. Une telle mesure constituerait également une ingérence dans le droit de cette personne à la protection de ses données personnelles.

---

[408] Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille, 1999, page 239 ; Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Ref. : 05MON10067), n° 636.

[409] Virginie Peltier, *Le secret des correspondances*, op. cit., page 239; Voir aussi Estelle De Marco, *L'anonymat sur Internet et le droit*, op. cit., n° 636.

[410] « Points-clés de jurisprudence, les notions de "domicile" et de "correspondance" », op. cit., se référant à l'arrêt *A. c/ France*, arrêt du 23 novembre 1993, séries A, n° 277 B, p. 49, §§ 35 et 37.

[411] « Points-clés de jurisprudence, les notions de "domicile" et de "correspondance" », op. cit., se référant à l'arrêt *Narinen c/ Finlande*, n° 45027/98, § 32, 1er juin 2004 : « *L'ouverture d'une lettre, toutefois, est suffisante pour constater une ingérence dans l'exercice par le requérant de son droit au respect de ses correspondances* » (traduit de l'anglais).

[412] Voir par exemple l'arrêt Copland c/ Royaume-Uni, n° 62617/00, 3 avril 2007, § 44 : « la collecte et la conservation, à l'insu de la requérante, de données à caractère personnel se rapportant à l'usage qu'elle faisait du téléphone, du courrier électronique et de l'Internet ont constitué une ingérence dans l'exercice du droit de l'intéressée au respect de sa vie privée et de sa correspondance, au sens de l'article 8 ». A propos de la surveillance d'une « scène publique par des moyens techniques », voir l'arrêt P.G. et J.H. c/ Royaume-Uni, n° 44787/98, § 57, CEDH 2001, IX, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=702094&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. A propos de surveillance téléphonique, voir par exemple Klass et autres c/ Allemagne, arrêt du 6 septembre 1978, séries A, n° 28, p. 21, § 41 ; Malone c/ Royaume-Uni, arrêt du 2 août 1984, séries A, n° 82, pp. 30-31, § 64 ; Kruslin c/ France, arrêt du 24 avril 1990, séries A, n° 176 A, p. 20, § 26.

La protection des données personnelles

Un autre aspect ou une autre sphère[413] du secret de la vie privée est la protection des données personnelles. Alors que la Cour européenne des droits de l'Homme protège ces données sous le visa de l'article 8 de la Convention, la Charte des droits fondamentaux de l'Union européenne déclare le droit à leur protection de manière indépendante, en son article 8[414]. Le droit à la protection des données personnelles est en conséquence un droit fondamental en Europe[415]. Il est assuré au niveau national par tous les Etats membres, lesquels devaient intégrer dans leurs droits internes respectifs les Directives européennes qui assurent la protection des données personnelles, les plus importantes étant les Directives 95/46/CE et 2002/58/CE (cette dernière étant actuellement en cours de révision). Les autorités à la protection des données personnelles veillent au respect de ces droits au sein des Etats membres et une autorité indépendante de même nature a été créée au niveau européen, à savoir le contrôleur européen de la protection des données (CEPD), pour veiller « *au respect de ces droits dans l'administration de l'UE* » [416].

Le principe de protection des données personnelles implique la confidentialité de ces données, lorsque celles-ci sont associées à des informations permettant l'identification directe ou indirecte d'une personne physique. Une adresse IP constitue par exemple une telle donnée. S'il existe un débat autour de la question de savoir si une adresse IP est une donnée personnelle[417], ce débat semble opérer une confusion entre la question de la définition des données personnelles et la question d'une éventuelle responsabilité.

En effet, une donnée personnelle est « *toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* » [418].

Une adresse IP répond objectivement à cette définition, dès lors qu'elle permet l'identification du titulaire d'un accès à Internet. La donnée personnelle consiste alors par exemple, a minima, en « *M. X, lequel **peut** être identifié, est le titulaire d'un accès Internet* » ou en « *M. X, lequel **peut** être identifié, est le titulaire d'un accès Internet qui a été utilisé le 12 juin 2009 à 10h00 pour accéder à un site web particulier* ». Une fois que ceci est dit, une telle identification ne permet pas d'établir un lien entre une personne physique et une situation donnée, telle que l'accès à un site web ou une infraction. La donnée personnelle va donner des informations sur le titulaire de l'accès qui a été utilisé pour consulter un site web ou pour commettre une infraction, mais ne fournira aucune information sur la personne qui a physiquement utilisé cet accès Internet pour accéder au dit site web ou pour commettre ladite infraction. Il s'agit là d'une question de responsabilité, qui n'a aucun lien avec la question de la définition de la donnée personnelle. Ceci dit, la conservation d'une adresse IP en lien avec

---

[413] Voir Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3ème éd., 1995, page 42.

[414] Cette disposition a été rédigée « *sur la base de l'article 286 du traité instituant la Communauté européenne et de la Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO n° L 281, 23.11.1995), de même que sur le fondement de l'article 8 de la CEDH et celui de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, laquelle a été ratifiée par tous les Etats membres* » (traduit de l'anglais) : site web de la Charte des droits fondamentaux de l'Union européenne, « Art 8. Protection of personal data » (Art. 8. Protection des données personnelles), disponible à cette adresse : http://www.eucharter.org/home.php?page_id=15.

[415] Site web du contrôleur européen de la protection des données, in « Le CEPD », « Introduction », disponible à cette adresse : http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/Home/EDPS.

[416] Site web du contrôleur européen de la protection des données, in « Le CEPD », « Introduction », disponible à cette adresse : http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/Home/EDPS.

[417] Voir par exemple Aoife White, « IP addresses are personal data, E.U. Regulator says » (« les adresses IP sont des données personnelles, déclare le régulateur européen »), Washingtonpost.com, 22 janvier 2008, disponible à l'adresse suivante : http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html.

[418] Article 2, a, de la Directive 95/46/CE.

une situation factuelle ayant eu lieu sur Internet est d'autant plus dangereuse que cette association ne peut être considérée comme une connaissance ou une preuve de responsabilité ou de comportement.

En conséquence, une mesure de filtrage d'Internet mise en place dans l'un des Etats membres de l'Union européenne ne devrait pas conduire à la conservation de données qui identifient ne serait-ce que le titulaire d'un accès à Internet, sans respecter les conditions énumérées par les directives européennes 95/46/CE[419], 2002/58/CE et 2006/24/CE, laquelle modifie la précédente, ainsi que par les lois nationales qui ont implémenté ces textes.

Une mesure de filtrage mise en place dans l'un des pays non membres de l'Union européenne mais qui ont accepté de respecter le droit à la vie privée, spécialement ceux qui sont parties à la Convention européenne des droits de l'Homme, ne peut pas plus conduire à un tel résultat sans que ne soient respectées les conditions posées par la Cour européenne des droits de l'Homme, lesquelles seront étudiées plus loin (« clause d'ordre public »). Ceci a notamment été souligné par le Groupe de protection des données, usuellement appelé « Groupe de l'article 29 »[420], lequel a considéré, sur la base du « *droit à la vie privée (article 8 de la Convention européenne et intégré de manière similaire dans le droit communautaire)* »[421], que « *la possibilité de rester anonyme est essentielle si l'on veut préserver les droits fondamentaux à la vie privée et à la liberté d'expression dans le cyberespace* »[422]. Cela a également été appuyé par la Cour européenne des droits de l'Homme, qui considère que « *la collecte et la conservation, à l'insu de la requérante, de données à caractère personnel se rapportant à l'usage qu'elle faisait du téléphone, du courrier électronique et de l'Internet ont constitué une ingérence dans l'exercice du droit de l'intéressée au respect de sa vie privée et de sa correspondance, au sens de l'article 8* » [423].

C'est encore l'opinion de juristes et de chercheurs, qui considèrent que toute information permettant de contrôler l'individu est dangereuse, même lorsqu'elle n'est pas utilisée, y compris dans un Etat démocratique[424]. Car « *même dans les corps de l'Etat les plus estimables et les plus respectables, il y a des tentations, des faiblesses, des fragilités* »[425]. Le secret est dès lors un « *problème de société* » [426], et certains auteurs estiment que la manière dont cette dernière en assure la protection permet de mesurer sa « *maturité*

[419] Par exemple, les données doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités » ; elles sont « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement » ; « la personne concernée a indubitablement donné son consentement », ou le traitement est nécessaire à la réalisation de l'un des objets listés dans la Convention : voir respectivement les articles 6b, 6e et 7a de la Directive 95/46/CE.

[420] Ce groupe a été créé par l'article 29 de la Directive 95/46/CE. L'article 15, 3 de la Directive 2002/58/CE, qui permet aux Etats de mettre en place une conservation préventive et systématique de certaines données techniques, déclare que « *le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électronique* ».

[421] Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, Recommandation 3/97, « L'anonymat sur Internet », 3 décembre 1997, WP 6, DG MARKT D/5022/97, site web de la Commission européenne, Justice et affaires intérieures, Liberté, sécurité et justice, Protection des données, Groupe de protection des données, Documents adoptés en 1997, page 4. Disponible à cette adresse : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp6_fr.pdf.

[422] Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, Recommandation 3/97, op. cit., page 6.

[423] *Copland c/ Royaume-Uni*, n° 62617/00, 3 avril 2007, § 44, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=815062&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[424] Voir Raymond Aron, *Essai sur les libertés*, éd. Hachette, coll. Pluriel, 1976, pp. 132-133. Sur l'ensemble du paragraphe, voir Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 84.

[425] Noël Chahid-Nourai, intervention à la table ronde « Secret et nouvelles technologies », colloque consacré au secret professionnel organisé par la Conférence des bâtonniers, Les petites affiches, n° 122, 20 juin 2001, pages 25 et s.

[426] Michel Benichou, « Le résistible déclin du secret », Les petites affiches, 20 juin 2001, n° 122, pages 3 et s.

démocratique »[427] et de savoir « *si elle a admis la primauté de l'homme ou si elle exige sa soumission* »[428]. Selon les tenants de cette doctrine, il est « *par conséquent utile, et même indispensable, de prévoir des systèmes de précaution* »[429].

6.6.1.4 La liberté de la vie privée et le filtrage d'Internet

La liberté de la vie privée est également protégée par la Convention européenne des droits de l'Homme.

La Commission européenne des droits de l'Homme considérait, en 1976, que le droit au respect de la vie privée incluait « *dans une certaine mesure, le droit d'établir et de développer des liens avec d'autres êtres humains, notamment dans le domaine affectif, pour développer et épanouir sa propre personnalité* »[430]. Elle confirma plus tard cette analyse, en ajoutant à ces liens « *les activités professionnelles et commerciales* »[431]. La Cour protège dès lors « *le droit à l'identité et au développement personnel ainsi que le droit pour tout individu de nouer et développer des relations avec ses semblables et le monde extérieur* » [432], le « *droit à l'auto-détermination et à l'autonomie personnelle* »[433] et « *l'intégrité physique et psychologique d'une personne* »[434]. La Cour expliqua également que « *le droit au respect de la vie privée assure à l'individu un domaine dans lequel il peut poursuivre librement le développement et l'accomplissement de sa personnalité* »[435], qui « *ne se limite pas aux mesures qui touchent une personne à son domicile ou dans ses locaux privés : il existe une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la vie privée* »[436].

La liberté de la vie privée peut en conséquence être comprise comme étant la liberté d'établir et de développer des relations avec autrui, y compris par voie des communications électroniques[437], mais aussi « *de faire des choix culturels, ludiques ou de consommation en ligne, ou simplement de s'informer, de naviguer librement sur le réseau* » [438].

---

[427] Michel Benichou, « Le résistible déclin du secret », Les petites affiches, 20 juin 2001, n° 122, pages 3 et s.

[428] Michel Bénichou, op. cit. ; sur les critiques de la « transparence », voir également Jacques Ribs, Ouverture de la manifestation de « Droit et démocratie » sur le thème d'« Internet et les libertés », Les petites affiches n° 224, 10 novembre 1999, pages 2 et s., spécialement page 3 : « *c'est donc un défi singulier pour la démocratie, pour la protection de la liberté individuelle et de la vie privée qui constituent des principes essentiels pour notre conception même de la démocratie* » ; Erik Izraelewicz, « La dictature de la transparence », Revue des deux mondes, février 2001, page 62.

[429] Noël Chahid-Nourai, intervention à la table ronde « Secret et nouvelles technologies », colloque consacré au secret professionnel organisé par la Conférence des bâtonniers, Les petites affiches, n° 122, 20 juin 2001, pages 25 et s.

[430] Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3ème éd., 1995, page 45, citant la décision *X. c/ Islande*, décision de la Commission, 18 mai 1976, année 1976, rec. n° 6825/74, page 343. Voir également Jacques Robert et Jean Duffar, *Droits de l'homme et libertés fondamentales,* Montchrestien, 7ème éd., 1999, page 437.

[431] Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3ème éd., 1995, page 45, se référant à la décision *Niemietz c/ Germany*, 16 décembre 1992, volume n° 251B, série A.

[432] *P.G. et J.H. c/ Royaume-Uni*, n° 44787/98, CEDH 2001, IX, § 56, se référant à *Burghartz c/ Suisse*, arrêt du 22 février 1994, séries A, n° 280 B, p. 28, §24. Voir également *Pretty c/ Royaume-Uni,* n° 2346/02, CEDH 2002, III, § 61, se référant au même arrêt. Voir également « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », op cit., se référant à *Friedl c/ Autriche*, arrêt du 31 janvier 1995, séries A, n° 305 B, décision de la Commission, p. 20, § 45.

[433] « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », op. cit., se référant à *Pretty c/ Royaume-Uni*, n° 2346/02, CEDH 2002, III, §§ 61 et 67.

[434] « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », Cour européenne des droits de l'Homme, 24/01/2007, disponible à cette adresse : http://www.echr.coe.int/NR/rdonlyres/49779DCC-6DBA-49BA-B1F1-4B554D860E56/0/COURT_n1968041_v2_Pointscl%C3%A9s_de_jurisprudence_Les_notions_de_Vie_priv%C3%A9e_et_de_Vie_familiale_.pdf, se référant à *X et Y c/ Pays-Bas*, arrêt du 26 mars 1985, séries A, n° 91, p. 11, § 22.

[435] *Brüggemann et Scheuten c/ Allemagne*, n° 6959/75, rapport de la Commission du 12 juillet 1977, Décisions et rapports 10, p. 115 (137 AV), § 55, disponible en anglais à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=open&documentId=816971&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[436] « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », op cit, se référant à *P.G. et J.H. c/ Royaume-Uni*, n° 44787/98, CEDH 2001, IX, § 56.

[437] Cf. supra, sous-section 6.6.1.3 et arrêt *Copland c/ Royaume-Uni*, n° 62617/00, 3 avril 2007, § 41. Pour un exemple de protection de la vie privée sur Internet, voir également *K.U. c/ Finlande*, requête n° 2872/02, arrêt du 2 décembre 2008, par exemple § 49: « *la liberté d'expression et la confidentialité des*

Une mesure de filtrage d'Internet qui méconnaîtrait de tels droits constituerait par conséquent une ingérence dans l'exercice du droit à la liberté de la vie privée. Tel serait le cas d'une mesure qui empêcherait les individus de faire certains choix en ligne, en bloquant l'accès à certains sites autorisés par la loi, ou qui obligerait ces mêmes individus à utiliser certains protocoles de communication au lieu de celui qui se trouverait bloqué. Tel serait également le cas d'une mesure de filtrage qui s'appliquerait spécifiquement à un internaute, en l'empêchant d'exercer son droit à la vie privée sur le réseau.

La liberté de correspondance

S'agissant de la liberté de correspondance, la Cour européenne des droits de l'Homme a surtout eu l'occasion d'analyser le droit de correspondre des détenus[439].

La liberté de correspondance, qui est le pouvoir de correspondre avec les personnes de son choix, est elle-même protégée par le droit au secret des correspondances, selon Madame Virginie Peltier. Cet auteur considère que « *il faut pouvoir être tranquille (…)* » pour que la correspondance « *soit réellement libre* »[440]. Cela vaut également pour les correspondances électroniques. Selon le même auteur, « *c'est la quiétude dans laquelle se déroule l'acte de correspondance qui détermine la liberté* » [441].

Une mesure de filtrage d'Internet qui aurait une incidence négative sur la liberté de correspondance entrerait par conséquent en conflit avec l'article 8 de la CEDH. Tel serait le cas, par exemple, d'une mesure de filtrage qui aurait pour résultat d'empêcher un individu de correspondre avec ses contacts, en bloquant un site web ou un domaine hébergeant une boite aux lettres ou un espace privé de discussion, ou en bloquant des contenus circulant via un protocole de pair à pair (ou en bloquant le protocole lui-même), empêchant par là-même une personne de recevoir ou d'envoyer un fichier en raison des mesures trop restrictives mises en place. De manière plus générale, tel serait encore le cas de toute mesure de filtrage d'Internet qui conduirait à bloquer l'utilisation d'un moyen ou d'un support de correspondance. De telles ingérences pourraient simultanément être qualifiées d'ingérences dans l'exercice du droit à la vie familiale, si la mesure empêchait un couple ou des enfants et leurs parents de communiquer entre eux. La Cour européenne des droits de l'Homme considère que « *la notion de vie familiale est un concept autonome* » [442] et que l'existence de cette part de vie est « *essentiellement une question de fait qui dépend de l'existence réelle dans la pratique de liens étroits* » [443]. « *Le fait de vivre ensemble sans être mariés peut constituer une situation de vie familiale* » [444], et « *même en l'absence de cohabitation il peut encore y avoir suffisamment de liens pour constituer une vie familiale* » [445].

---

communications sont des considérations essentielles et les utilisateurs de télécommunications et de services Internet doivent être assurés que leurs propres vie privée et liberté d'expression seront respectées ».

[438] Estelle De Marco, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », 4 juin 2009, Juriscom.net, page 4, disponible à l'adresse : http://www.juriscom.net/uni/visu.php?ID=1133 ; Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 137.

[439] Arrêt *Silver et autres*, publications de la Cour, série A, n° 61. Voir Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3ème éd., 1995, page 61, et note de bas de page n° 249.

[440] Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille, 1999, page 99. Voir également Estelle De Marco, *L'anonymat sur Internet et le droit*, op. cit., n° 146.

[441] Virginie Peltier, *Le secret des correspondances*, op cit, page 99.

[442] « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », Cour européenne des droits de l'Homme, 24/01/2007, disponible à cette adresse : http://www.echr.coe.int/NR/rdonlyres/49779DCC-6DBA-49BA-B1F1-4B554D860E56/0/COURT_n1968041_v2_Pointscl%C3%A9s_de_jurisprudence__Les_notions_de__Vie_priv%C3%A9e_et_de_Vie_familiale_.pdf, se référant à *Marckx c/ Belgique*, arrêt du 13 juin 1979, séries A, n° 31, p. 11, § 31, rapport de la Commission du 10 décembre 1977, séries B-29, p.44, § 69.

[443] « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », op. cit., se référant à *K. c/ Royaume-Uni*, n° 11468/85, décision de la Commission du 15 octobre 1986, Rapports et décisions 50, p. 199, 207.

[444] « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », op. cit., se référant à *Johnston et autres c/ Irlande*, arrêt du 18 décembre 1986, séries A, n° 112, p. 19, § 56.

[445] « Points-clés de jurisprudence, les notions de "vie privée" et de "vie familiale" », op. cit., se référant à *Kroon et autres c/ Pays-Bas*, arrêt du 27 octobre 1994, séries A, n° 297 C, p. 56, § 30.

Les autres droits qui se trouvent protégés par la Convention européenne des droits de l'Homme sous le visa du principe de respect de la vie privée ne seront pas traités dans ce rapport, puisque l'objectif de ce dernier est uniquement d'analyser les libertés avec lesquelles une mesure de filtrage peut se trouver en conflit.

Il est important de noter qu'une mesure de filtrage d'Internet peut être considérée comme étant en conflit avec une liberté fondamentale, dès lors qu'elle présente le risque de constituer une ingérence dans l'exercice de cette liberté. Ceci, *même si l'usage de la fonctionnalité* qui présente un tel risque *n'entre pas dans les objectifs assignés à la mesure de filtrage.* Sur ce point, nous pouvons nous référer aux propos de Monsieur Chahid-Nourai, qui fut Conseiller de l'Autorité française de protection des données personnelle (CNIL), au sujet du code INSEE français (N.I.R.), qui est un numéro d'identification donné aux personnes physiques : « *si le N.I.R. avait existé officiellement et opérationnellement en 1943 et si l'on avait voulu sélectionner tous les gens nés en Pologne parce que l'on pensait qu'ils étaient a priori susceptibles d'être juifs, on aurait eu la possibilité de le faire. Si l'on veut aujourd'hui sélectionner également tous les étrangers, il suffit de prendre le 99, lequel est le numéro d'identifiant des personnes nées à l'étranger, catégorie qui recouvre largement la précédente. Si l'on veut faire encore plus fin encore et si l'on veut sélectionner, par exemple, pour les discriminer, tous les gens nés en Iran, en Irak ou en Yougoslavie, on peut le faire (...). En période de crise, cela peut servir...* » [446].

Dès lors qu'une mesure de filtrage est susceptible de constituer une ingérence dans l'exercice d'une liberté fondamentale, sa mise en œuvre doit respecter la « clause d'ordre public » qu'applique la Cour européenne des droits de l'Homme, clause que nous décrirons au chapitre 7 de la présente étude.

[446] Noël Chahid-Nourai, intervention à la table ronde « Secret et nouvelles technologies », colloque consacré au secret professionnel organisé par la Conférence des bâtonniers, Les petites affiches, n° 122, 20 juin 2001, pages 25 et s. Voir aussi Estelle De Marco, *L'anonymat sur Internet et le droit*, op. cit., n° 80.

6.6.2 La liberté d'expression

6.6.2.1 Les textes principaux

La liberté d'expression est garantie par l'article 19 de la Déclaration universelle des droits de l'Homme, l'article 19 du Pacte international sur les droits civils et politiques, l'article 10 de la Convention européenne des droits de l'Homme et l'article 11 de la Charte des droits fondamentaux de l'Union européenne, dont le sens et la portée sont considérés comme étant « *les mêmes que ceux des droits garantis par la CEDH* »[447]. En conséquence, le droit à la liberté d'expression est un droit de l'Homme et une liberté fondamentale, et de fait, dans de nombreux Etats, une liberté publique. Il bénéficie autant aux adultes qu'aux enfants, même si la Convention des Nations Unies sur les droits de l'enfant lui ajoute la déclaration spécifique du droit des enfants à la liberté d'expression, en son article 13.

Sur la base de ces textes, ce droit inclut « *la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées* », « *sans considération de frontières* ». La DUDH, la CEDH et la Charte de l'Union européenne ajoutent que ce droit doit pouvoir être exercé « *sans qu'il puisse y avoir ingérence d'autorités publiques* ». La DUDH et le PIDCP ajoutent encore, à la définition de ce droit, la liberté de « *chercher* » des informations et des idées « *par quelque moyen d'expression que ce soit* », tandis que le PIDCP explique que ce droit peut être exercé « *sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix* ».

La Charte des droits fondamentaux de l'Union européenne prévoit enfin, au second paragraphe de son article 11, que « *la liberté des médias et leur pluralisme sont respectés* ». Ce paragraphe tire explicitement « *les conséquences du paragraphe 1 s'agissant de la liberté des médias* » et est basé, « *en particulier, sur la jurisprudence de la Cour de justice relative à la télévision, notamment l'affaire C-288/89 (arrêt du 25 juillet 1991, Stichting Collectieve Antennevoorziening Gouda et autres [1991] Recueil I-4007), et sur le protocole sur le système de radiodiffusion publique dans les Etats membres annexé au Traité instituant la communauté européenne et à présent à la Constitution, et sur la Directive du Conseil 89/552/EC (spécialement son 17ème considérant)* »[448].

Devoirs et responsabilités

S'agissant des limitations à cette liberté, le PIDCP et la CEDH prévoient que l'exercice du droit à la liberté d'expression comporte des « *devoirs et des responsabilités* » et peut être soumis à certaines restrictions. Ces dernières, selon le PIDCP, « *doivent toutefois être expressément fixées par la loi et (…) doivent (être) nécessaires (…) au respect des droits ou de la réputation d'autrui* », ou « *à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques* ». Selon la Convention européenne des droits de l'Homme, ces restrictions (ou autres formalités, conditions ou sanctions) doivent être « *prévues par la loi* » et doivent constituer « *des mesures nécessaires, dans une société démocratique* », à une liste restrictive d'objectifs. L'une et l'autre de ces deux dernières conditions correspondent à la « clause d'ordre public » que nous décrirons au chapitre 7 de la présente étude.

La liberté d'expression est encore protégée par de nombreuses Constitutions, au niveau national. En France, cette liberté est protégée par l'article 11 de la Déclaration des droits de

[447] Traduit de l'anglais. Site web de la Charte des droits fondamentaux de l'Union européenne, « Art 11. Freedom of expression and information » (Art 11. Liberté d'expression et d'information), disponible à cette adresse : http://www.eucharter.org/home.php?page_id=18.

[448] Traduit de l'anglais. Site web de la Charte des droits fondamentaux de l'Union européenne, « Art 11. Freedom of expression and information » (Art 11. Liberté d'expression et d'information), disponible à cette adresse : http://www.eucharter.org/home.php?page_id=18.

l'Homme et du citoyen de 1789[449], laquelle relève du « bloc de constitutionnalité » français. Le Conseil constitutionnel ajoute que « *la liberté d'expression et de communication est d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés* » [450].

6.6.2.2 La liberté d'expression et le filtrage d'Internet

La liberté d'expression, qui « *constitue l'un des fondements essentiels d'une société démocratique* » [451], comprend au moins la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans considération de frontière – selon les textes qui la consacrent.

La Cour européenne des droits de l'Homme ajoute que l'article 10 de la CEDH « *garantit non seulement le droit de communiquer des informations mais également, pour le public, le droit de les recevoir* » [452] et « *vaut non seulement pour les informations ou idées accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'Etat ou une fraction quelconque de la population* »[453]. S'agissant des limites de la critique admissible, elles sont « *plus larges à l'égard d'un homme politique, visé en cette qualité, que d'un simple particulier* » [454]. La Cour considère par ailleurs que « *compte tenu de son accessibilité et de sa capacité à stocker et à communiquer des quantités importantes d'informations, Internet joue un rôle important dans l'amélioration de l'accès du public à l'actualité et facilite la dissémination de l'information de manière générale. Le maintien des archives d'Internet est un aspect critique de ce rôle et la Cour considère dès lors que de telles archives tombent sous le coup de la protection de l'article 10* » [455].

Par conséquent, la liberté d'expression inclut le droit de recevoir des informations, notamment par l'intermédiaire d'Internet. Toute mesure de filtrage d'Internet qui empêcherait une personne d'accéder à un contenu serait dès lors en conflit avec cette liberté. Ce conflit serait encore plus grand si la mesure préconisait la suspension d'un accès à Internet, prévenant ou empêchant par là-même une personne d'utiliser l'ensemble du réseau Internet ou une partie de celui-ci.

Le Conseil constitutionnel français confirme cette analyse, en considérant que le droit d'accéder à Internet est protégé sous le principe de la liberté d'expression : « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la*

---

[449] L'article 11 prévoit : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi ».

[450] Décision n° 2009-580 DC du 10 juin 2009, J.O.R.F. du 13 juin 2009, p. 9675, § 15. Cette décision est disponible à l'adresse suivante : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html.

[451] *Sunday Times c/ Royaume-Uni*, arrêt du 26 avril 1979, requête n° 6538/74, séries A, n° 30, § 65, disponible à l'adresse suivante : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700016&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[452] Traduit de l'anglais. *Times newspapers LTD (n° 1 et 2) c/ Royaume-Uni*, arrêt du 10 mars 2009, requêtes n° 3002/03 et 23676/03, § 27, se référant à *Observer and Guardian c/ Royaume-Uni*, 26 novembre 1991, § 59(b), séries A, n° 216 et *Guerra et autres c/ Italie*, 19 février 1998, § 53, Recueil 1998-I. L'arrêt *Times newspapers LTD* est disponible en anglais à l'adresse suivante : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=848220&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[453] *Sunday Times c/ Royaume-Uni*, op cit., § 65, se référant à l'arrêt *Handyside c. Royaume-Uni*, requête n° 5493/72, arrêt du 7 décembre 1976, séries A, n° 24, p. 23, § 9.

[454] *Lindon, Otchakovsky-Laurens et July c/ France*, arrêt du 22 octobre 2007, requêtes n°s 21279/02 et 36448/02, § 46, disponible à l'adresse suivante : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=824753&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[455] Traduit de l'anglais. *Times newspapers LTD* (n° 1 et 2) *c/ Royaume-Uni*, op. cit., § 27.

participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services »[456].

Le Parlement européen considère également que l'interruption d'un accès Internet est en conflit avec les garanties accordées aux droits de l'Homme, sans toutefois préciser si la raison en est qu'Internet permet l'exercice de ces libertés, ou si l'accès à Internet est un droit fondamental en lui-même. Par une résolution du 10 avril 2008, le Parlement engage « *la Commission et les États membres à reconnaître qu'Internet est une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information, et, par conséquent, à éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telles que l'interruption de l'accès à Internet* »[457].

Dans le cadre de la réforme de la législation sur les télécommunications (paquet télécom), le Parlement réintroduisit, le 6 mai 2009, l'un de ses amendements de première lecture énonçant qu' « *aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux sans décision préalable des autorités judiciaires sauf lorsque la sécurité publique est menacée* »[458]. Le Parlement en conclut, dans son communiqué de presse, que « *l'accès à Internet ne peut pas être restreint sans décision préalable des autorités judiciaires* »[459]. Cet amendement, appelé « amendement Bono », « amendement 138 », ou « amendement 46 » lorsqu'il fut réintroduit au sein du projet de texte européen à l'occasion de sa seconde lecture en mars 2009[460], fut combattu par la France[461]. A l'heure de la rédaction de ce rapport, le destin de ce texte reste incertain car le Conseil de l'Union européenne s'y est opposé, dans le cadre de la procédure de conciliation lancée après le second vote du Parlement.

Plusieurs auteurs et membres du Parlement européen considérèrent que l'adoption de cet « amendement Bono » était une reconnaissance de l'accès à Internet en tant que droit fondamental[462]. Le Parlement européen lui-même expliqua, dans un communiqué de presse du 26 mars 2009, que « *la Charte des droits fondamentaux de l'Union ne mentionne pas*

---

[456] Décision n° 2009-580 DC du 10 juin 2009, J.O.R.F. du 13 juin 2009, p. 9675, § 12. Cette décision est disponible à l'adresse suivante : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html.

[457] Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe, 2007/2153(INI), § 23, accessible à cette adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//FR.

[458] « Pas d'accord sur le "paquet Télécom" », Société de l'information, Communiqué de presse, 6 mai 2009, disponible à cette adresse : http://www.europarl.europa.eu/news/expert/infopress_page/058-55086-124-05-19-909-20090505IPR55085-04-05-2009-2009-true/default_fr.htm.

[459] Ibid.

[460] Voir le site web de Guy Bono, membre du Parlement européen, « amendement 46 = Amendement 138 », communiqué de presse, 6 mars 2009, disponible à cette adresse : http://www.guy-bono.fr/article/articleview/8805/1/1378/, à cette adresse : http://www.temps-reels.net/article1846.html ou à cette adresse : http://www.d-s-f.net/index.php/article/articleview/8805/1/1795/.

[461] La France était, parallèlement, en train de débattre devant son propre Parlement du projet de loi dit « Création et Internet », lequel autorisait une autorité administrative nouvellement créée à prononcer la suspension de l'accès à Internet d'un utilisateur du réseau, lorsque l'adresse IP de ce dernier était mise en relation avec une infraction à des droits de propriété intellectuelle et que cet internaute n'était pas en mesure de démontrer son absence de responsabilité. Ce mécanisme fut censuré par le Conseil constitutionnel français, notamment car il ne respectait pas le principe de présomption d'innocence et car il confiait, à une autorité administrative, un pouvoir réservé au juge de l'ordre judiciaire. Voir la décision n° 2009-580 DC du 10 juin 2009, précitée.

[462] Voir par exemple « Le Parlement européen redit non à la coupure de l'accès à internet comme sanction », communiqué de presse, 26 mars 2009, accessible à cette adresse : http://www.guy-bono.fr/article/articleview/8880/1/2096/ ou à cette adresse : http://www.d-s-f.net/index.php/article/articleview/8880/1/1795/, citant Guy Bono: « *malgré les pressions multiples exercées par (le parti français) UMP et les autorités françaises, les députés européens sont restés sur leur ligne : l'accès à Internet est un droit fondamental pour l'inclusion sociale* » ; voir également Estelle De Marco, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », 4 juin 2009, Juriscom.net, page 5, note n° 32, disponible à cette adresse : http://www.juriscom.net/uni/visu.php?ID=1133.

directement l'accès à Internet, mais le "droit à la liberté d'expression". Ce droit comprend "la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques, et sans considération de frontières". Si l'accès à Internet était considéré comme un droit fondamental dans l'Union, la France pourrait se trouver en contradiction avec le droit européen »[463], faisant ainsi référence à l'adoption éventuelle de la « loi Hadopi » dans sa version contemporaine au communiqué.

Que l'accès à Internet soit ou non un droit fondamental indépendant, il est à tout le moins protégé en tant que moyen d'exercer la liberté d'expression. Toute mesure de filtrage d'Internet destinée à empêcher les personnes d'accéder à l'information est par conséquent en conflit avec cette liberté. De manière plus générale, il peut être dit que toute mesure de filtrage limite le droit à la liberté d'expression, dans une mesure plus ou moins grande selon les caractéristiques du filtrage et selon le degré de sur-blocage (ou filtrage excessif) que ce filtrage génère, puisque l'objectif clairement identifié d'une telle mesure est de limiter l'accessibilité des contenus.

6.6.2.3 Le droit spécifique des enfants à la liberté d'expression

A la lumière de l'analyse que fait la Cour européenne des droits de l'Homme du droit à la liberté d'expression (qui inclut le droit de recevoir des informations, notamment par l'intermédiaire d'Internet), il est possible de considérer que certains droits spécifiques à l'enfant, proclamés par la Convention des Nations Unies relative aux droits de l'enfant, ne sont en réalité que le rappel de détails du droit des enfants à la liberté d'expression, tel qu'il se trouve protégé par la CEDH.

La Convention prévoit que « *les États parties reconnaissent l'importance de la fonction remplie par les médias et veillent à ce que l'enfant ait accès à une information et à des matériels provenant de sources nationales et internationales diverses, notamment ceux qui visent à promouvoir son bien-être social, spirituel et moral ainsi que sa santé physique et mentale* »[464]. La Convention déclare par ailleurs que les Etats parties « *conviennent que l'éducation de l'enfant doit viser (…)* » à « *préparer l'enfant à assumer les responsabilités de la vie dans une société libre, dans un esprit de compréhension, de paix, de tolérance, d'égalité entre les sexes et d'amitié entre tous les peuples et groupes ethniques, nationaux et religieux, et avec les personnes d'origine autochtone* » [465].

En conséquence, toute mesure de filtrage d'Internet qui conduirait à empêcher les enfants d'accéder aux informations qui pourraient être utiles à leur développement et à leur éducation à une vie responsable entrerait en conflit avec la Convention internationale relative aux droits de l'enfant, et certainement avec le droit à la liberté d'expression de manière générale, particulièrement lorsque cette mesure ne serait pas placée sous le contrôle des parents. En effet, l'article 5 de la Convention prévoit que « *les États parties respectent la responsabilité, le droit et le devoir qu'ont les parents ou, le cas échéant, les membres de la famille élargie ou de la communauté, comme prévu par la coutume locale, les tuteurs ou autres personnes légalement responsables de l'enfant, de donner à celui-ci, d'une manière qui corresponde au développement de ses capacités, l'orientation et les conseils appropriés à l'exercice des droits que lui reconnaît la présente Convention* ».

La question est d'importance, car le débat relatif au filtrage d'Internet accueille parfois une discussion sur l'utilité de filtrer certains contenus en vue de protéger la santé et le

[463] « Les droits fondamentaux doivent aussi s'appliquer sur Internet », Parlement européen, communiqué de presse, 26 mars 2009, citation uniquement disponible en français à cette adresse : http://www.europarl.europa.eu/news/expert/infopress_page/017-52613-082-03-13-902-20090325IPR52612-23-03-2009-2009-false/default_fr.htm.
[464] Article 17 de la Convention.
[465] Article 29, d de la Convention.

développement des enfants[466]. Accéder aux contenus, sous le contrôle et l'assistance des parents, peut aussi aider les enfants à comprendre que certaines ressources en ligne peuvent être dangereuses et doivent être évitées (ou abordées d'une manière responsable). Ceci peut en conséquence contribuer à les éduquer à une vie responsable dans une société libre, en lien avec l'article 29 de la Convention. Quelle que soit la conclusion qui sera apportée à ce débat, il semble important de rappeler que « *les gouvernements doivent respecter le droit et la responsabilité des familles de diriger et de guider leurs enfants afin que ceux-ci, au fur et à mesure qu'ils grandissent, apprennent à utiliser leurs droits de manière appropriée* » [467].

[466] En septembre 2005, un projet de loi français qui n'a *in fine* pas été adopté entendait obliger les fournisseurs d'accès à Internet à filtrer automatiquement et par défaut tout site web susceptible e mettre les enfants « *en danger* », notion qui aurait couvert une large gamme de sites (Les fournisseurs d'accès à Internet « *mettent en œuvre auprès de tous leurs abonnés, de manière automatique, des dispositifs techniques performants et activés par défaut qui permettent de restreindre l'accès aux services de communication au public en ligne mettant en péril les mineurs* »). Voir Marc Rees, « Le filtrage par les FAI confirmé par le 1er Ministre », 22 septembre 2005, PC Inpact, disponible à l'adresse : http://www.pcinpact.com/actu/news/Le_filtrage_par_les_FAI_confirme_par_le_1er_Minist.htm.

[467] Traduit de l'anglais. Unicef, « Fact sheet: A summary of the rights under the Convention on the Rights of the Child » (« Fiche d'informations : un résumé des droits énoncés dans la Convention relative aux droits de l'enfant »), disponible sur le site web de l'Unicef, in « Les droits énoncés dans la Convention relative aux droits de l'enfant » (http://www.unicef.org/french/crc/index_30177.html), disponible en seule version anglaise à cette adresse : http://www.unicef.org/crc/files/Rights_overview.pdf.

6.6.3 Le droit des personnes handicapées d'accéder aux communications électroniques

Les personnes handicapées, à l'instar des personnes qui n'ont pas de handicap, bénéficient des droits fondamentaux qui sont notamment consacrés par la CEDH et le PIDCP. Pourtant, leur handicap peut parfois être une entrave à l'exercice plein et entier de leurs droits. Ces personnes peuvent être assistées, dans ce cadre, par l'utilisation des communications électroniques – services Internet inclus. Par exemple, Internet peut faciliter l'achat autonome de biens, les échanges avec des proches ou les communications de base avec le monde extérieur. L'usage d'Internet est dès lors, pour certaines personnes handicapées, plus qu'une simple liberté générale et plus qu'une liberté protégée par le droit à la liberté d'expression, dans l'hypothèse où accéder à Internet ne serait pas considéré comme un droit fondamental autonome[468]. Il s'agit d'un outil qui peut permettre à ces personnes d'exercer les libertés fondamentales qu'elles ne pourraient pas exercer d'une autre manière. Il s'agit donc d'un moyen d'exercice de ces droits et libertés, particulièrement du droit à la vie privée. Limiter l'usage de ce moyen pourrait être considéré comme une limitation de la liberté en cause elle-même, ainsi qu'il en a été jugé pour les personnes non handicapées s'agissant d'Internet et de la liberté d'expression.

En outre, une action positive est requise de la part des pays qui ont pris l'engagement de respecter les libertés fondamentales, dans le cadre des Nations Unies[469] ou du Conseil de l'Europe[470]. Ils doivent prendre les mesures nécessaires pour permettre aux personnes handicapées de « *jouir pleinement de tous les droits de l'homme et de toutes les libertés fondamentales* »[471].

Dans cet objectif, les pays doivent notamment « *encourager l'offre et l'utilisation de nouvelles technologies - y compris les technologies de l'information et de la communication, les aides à la mobilité, les appareils et accessoires et les technologies d'assistance - qui soient adaptées aux personnes handicapées, en privilégiant les technologies d'un coût abordable* »[472]. Le plan d'action de l'Union européenne en faveur des personnes handicapées 2003-2010 a lui-même pour objectif de « *permettre aux personnes handicapées de disposer des mêmes choix personnels et du même degré de contrôle de leur quotidien que les autres personnes* »[473]. Des mesures additionnelles, spécifiques aux personnes handicapées, sont prises dans le cadre des directives européennes qui réglementent les communications électroniques[474].

En conséquence, une mesure de filtrage d'Internet qui préviendrait les personnes handicapées d'accéder aux communications électroniques pourrait empêcher certaines d'entre elles d'exercer des droits fondamentaux que les personnes sans handicap seraient toujours en mesure d'exercer, malgré une interdiction d'utiliser le réseau Internet ou une partie de celui-ci. Par exemple, la législation européenne n'impose pas aux Etats membres d'aménager une exception aux droits d'auteur permettant la copie de fichiers au bénéfice des personnes handicapées. De fait, le filtrage de sites permettant cette fonctionnalité (en tant qu'éléments concernés par un blocage plus général de sites considérés comme contrevenant aux droits

---

[468] Voir la sous-section 6.6.2.2.
[469] Convention relative aux droits des personnes handicapées du 13 décembre 2006.
[470] Recommandation Rec(2006)5 du Comité des ministres aux Etats membres « sur le Plan d'action du Conseil de l'Europe pour la promotion des droits et de la pleine participation des personnes handicapées à la société : améliorer la qualité de vie des personnes handicapées en Europe 2006-2015 », adoptée par le Comité des ministres le 5 avril 2006 lors de la 961ème réunion des délégués des ministres, disponible à : https://wcd.coe.int/ViewDoc.jsp?id=986837&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75, section 1.2.1: « *Le Plan tient dûment compte des instruments, traités et programmes européens et internationaux pertinents, et notamment des travaux en cours sur le projet de convention internationale des Nations Unies sur les droits des personnes handicapées* ».
[471] Convention relative aux droits des personnes handicapées du 13 décembre 2006, préambule, v.
[472] Convention relative aux droits des personnes handicapées du 13 décembre 2006, article 4, 1, g.
[473] Voir le site de la Commission européenne, « emploi, affaires sociales et égalité des chances », « Personnes handicapées », disponible à cette adresse : http://ec.europa.eu/social/main.jsp?catId=429&langId=fr.
[474] Voir infra, chapitre 7.

d'auteur, tels que celui actuellement mis en œuvre par Eircom en Irlande[475]) serait nuisible aux droits des personnes handicapées. Une telle mesure causerait en conséquence plus de dommages, aux libertés des personnes handicapées, qu'elle n'en causerait aux libertés des personnes non handicapées. Il en serait de même d'une mesure de filtrage qui conduirait à empêcher une personne handicapée d'utiliser un protocole particulier de communication, important pour elle, par rapport aux effets qu'aurait la même interdiction sur les personnes non handicapées.

Cette problématique devra être prise en considération dans le cadre de toute discussion sur le filtrage, même si les droits des personnes handicapées, à l'instar du droit à la protection de la vie privée et du droit à la liberté d'expression, doivent être mis en équilibre avec les autres droits qui pourraient, inversement, justifier la mise en œuvre d'une mesure de filtrage.

[475] Voir par exemple le communiqué de presse d'Eircom, disponible en anglais à l'adresse suivante : http://news.eircom.net/breakingnews/16288287/ (dernière visite le 3 septembre, 2009).

6.7 Les droits et libertés fondamentales susceptibles de justifier une mesure de filtrage d'Internet

La section 6.6 a accueilli l'analyse de certains droits et libertés pouvant être mis en péril par une mesure de filtrage. Inversement, la protection d'autres droits et libertés pourrait œuvrer au soutien de cette même mesure. Trois de ces droits sont les suivants :

- Le droit des enfants à être protégés contre la violence,
- Le droit des personnes à ne pas subir de discrimination,
- Les droits de propriété intellectuelle.

6.7.1 Le droit des enfants à être protégés contre la violence

Les enfants sont fortement protégés contre la violence. Deux aspects de la protection de l'enfance présentent un intérêt particulier.

- Le premier est le nombre important de textes qui se concentrent sur la protection de l'enfance et non sur celle des adultes, tout en soulignant la prohibition de la violence mentale et physique, spécialement de nature sexuelle ;
- Le second est la prohibition de l'image elle-même d'un crime de nature sexuelle commis sur la personne d'un enfant, à travers l'interdiction de la pédopornographie.

La Convention des Nations Unies relative aux droits de l'enfant consacre le droit de l'enfant à être protégé « *contre toute forme de violence, d'atteinte ou de brutalités physiques ou mentales, d'abandon ou de négligence, de mauvais traitements ou d'exploitation, y compris la violence sexuelle, pendant qu'il est sous la garde de ses parents ou de l'un d'eux, de son ou ses représentants légaux ou de toute autre personne à qui il est confié* »[476]. Elle consacre encore le droit de l'enfant à être protégé « *contre l'exploitation économique* »[477], contre « *toutes les formes d'exploitation sexuelle et de violence sexuelle* »[478] et « *contre toutes autres formes d'exploitation préjudiciables à tout aspect de son bien-être* »[479]. Les Etats parties doivent par ailleurs prendre « *toutes les mesures appropriées pour faciliter la réadaptation physique et psychologique et la réinsertion sociale de tout enfant victime de toute forme de négligence, d'exploitation ou de sévices, de torture ou de toute autre forme de peines ou traitements cruels, inhumains ou dégradants, ou de conflit armé* »[480].

Tandis que la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains a pour objectif de « *combattre la traite des êtres humains, en garantissant l'égalité entre les femmes et les hommes* », objectif visant la protection des adultes comme des enfants, indépendamment de leur race ou de leur religion[481], la Convention sur la protection des enfants contre l'exploitation et les abus sexuels[482] poursuit l'objectif plus précis de « *prévenir et de combattre l'exploitation et les abus sexuels concernant des enfants* », de « *protéger les droits des enfants victimes d'exploitation et d'abus sexuels* » et de « *promouvoir la coopération nationale et internationale contre l'exploitation et les abus sexuels concernant des enfants* »[483]. Cette Convention, qui n'est pas encore entrée en vigueur en raison d'une pénurie

[476] Article 19 de la Convention.
[477] Article 32 de la Convention.
[478] Article 34 de la Convention.
[479] Article 36 de la Convention.
[480] Article 39 de la Convention.
[481] Article 1 de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains, STCE n° 197, ouvert à la signature le 16 mai 2005, entré en vigueur le 1er février 2008 (16 signatures non suivies de ratifications et 25 ratifications/adhésions le 19 août 2009), disponible à l'adresse suivante : http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=197&CM=7&DF=22/01/2010&CL=FRE. S'agissant du principe de non discrimination, voir l'article 3.
[482] Convention sur la protection des enfants contre l'exploitation et les abus sexuels, STCE n° 201, ouvert à la signature le 25 octobre 2007. La Convention est disponible à partir de l'adresse suivante : http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=7&DF=22/01/2010&CL=FRE.
[483] Article 1 de la the Convention.

de ratifications[484], ajoute que toutes les formes d'abus sexuels sur la personne d'un enfant « *mettent gravement en péril la santé et le développement psychosocial* » de ce dernier[485].

S'agissant de la prohibition des images d'une scène de crime lorsque la victime est un enfant, le protocole facultatif de la Convention relative aux droits de l'enfant, portant sur la vente d'enfants, la prostitution des enfants et la pornographie impliquant des enfants, prévoit que « *chaque État Partie veille à ce que, au minimum, les actes et activités suivants soient pleinement couverts par son droit pénal, que ces infractions soient commises au plan interne ou transnational, par un individu ou de façon organisée* », en énumérant notamment « *le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de vendre ou de détenir aux fins (mentionnées plus haut dans le protocole), des matériels pornographiques mettant en scène des enfants* ».

L'article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité prévoit que « *chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit* », énumérant « *la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique* », « *l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique* », « *la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique* », « *le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique* », et « *la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques* ».

Les deux aspects de la protection de l'enfance que nous avons mentionnés plus haut sont encore soulignés dans la Décision-cadre n° 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie[486], qui prévoit notamment que « *chaque État membre prend les mesures nécessaires pour que (certains) comportements intentionnels* », que le texte énumère, « *soient punis* », tels que « *le fait de contraindre un enfant à se livrer à la prostitution ou à participer à des spectacles pornographiques* », et « *le fait de se livrer à des activités sexuelles avec un enfant* » dans certaines circonstances elles aussi énumérées[487]. La Décision-cadre du Conseil prévoit en outre en son article 3 que les Etats membres prennent les mesures nécessaires pour que la production de pédopornographie soit punissable, « *lorsqu'(elle) ne peu(t) être légitim(ée)* », de même que « *la distribution, la diffusion ou la transmission de pédopornographie* », « *le fait d'offrir ou de rendre disponible de la pédopornographie* » et « *l'acquisition ou la détention de pédopornographie* ».

Ceci étant dit, seul le droit à la protection contre les crimes apparaît spécifiquement comme étant un droit de l'Homme, une liberté fondamentale et, dans la plupart des pays, une liberté publique. Le droit des enfants à ne pas être les victimes d'une image pédopornographique n'est en effet pas identifié en tant que tel dans les textes que nous avons analysés[488]. Ces textes ne visent pas à déclarer un tel droit, mais poursuivent plutôt l'objectif de favoriser la mise en œuvre, au sein des systèmes juridiques nationaux, de certaines mesures qui se veulent cruciales pour assurer la protection d'autres droits fondamentaux bénéficiant aux enfants, particulièrement le droit d'être protégés contre la violence sexuelle et le droit au développement.

---

[484] A la date du 19 août 2009, 35 pays avaient signé la Convention sans l'avoir ratifiée et 2 pays l'avaient ratifiée ou y avaient adhéré, alors que 5 ratifications incluant au moins 3 Etats membres du Conseil de l'Europe sont nécessaires pour permettre à la Convention d'entrer en vigueur. Voir la page y afférente du site web du Conseil de l'Europe, disponible à l'adresse suivante : http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=7&DF=22/01/2010&CL=FR.

[485] Préambule de la Convention, § 4.

[486] Journal officiel du 20 janvier 2004, L 013, pp. 0044-0048, disponible à cette adresse : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:FR:HTML.

[487] Article 2 de la décision-cadre du Conseil.

[488] Voir supra, 6.5.2.2.

Quoi qu'il en soit, l'importance de la lutte contre la pédopornographie, de même que l'importance de protéger les enfants de la violence et des entraves à leur développement personnel, sont très souvent un argument pour justifier la mise en œuvre de mesures de filtrage d'Internet. Dans certains pays, il s'agit souvent de la seule justification avancée par le gouvernement ou par les acteurs privés qui sollicitent la mise en œuvre d'une telle mesure – ils requièrent par la même, fréquemment, que cette mesure soit restreinte aux seuls contenus de pédopornographie.

Une telle justification, qui paraît particulièrement raisonnable, est toutefois difficile à comprendre d'un point de vue juridique. Il est juridiquement difficile de comprendre, en effet, en quoi une mesure de filtrage d'Internet devrait être limitée aux seuls contenus de pédopornographie, puisque la loi protège également, spécifiquement, d'autres catégories de personnes contre certaines atteintes, notamment les atteintes générées par la discrimination.

6.7.2 La protection des personnes contre la discrimination

Les droits de l'Homme et les libertés fondamentales bénéficient à tout individu sans distinction. Toutefois, puisque les discriminations ont été et peuvent demeurer une difficulté dans certains pays, plusieurs textes furent signés pour souligner le droit spécifique de tout individu à être protégé contre la discrimination. Ces textes visent « *toute distinction, exclusion, restriction ou préférence fondée sur la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, qui a pour but ou pour effet de détruire ou de compromettre la reconnaissance, la jouissance ou l'exercice, dans des conditions d'égalité, des droits de l'homme et des libertés fondamentales dans les domaines politique, économique, social et culturel ou dans tout autre domaine de la vie publique* »[489].

La Convention internationale des Nations Unies sur l'élimination de toutes les formes de discrimination raciale[490] prévoit en conséquence que « *chaque Etat partie doit, par tous les moyens appropriés, y compris, si les circonstances l'exigent, des mesures législatives, interdire la discrimination raciale pratiquée par des personnes, des groupes ou des organisations et y mettre fin* »[491]. Les Etats parties doivent également « *condamn(er) toute propagande et toutes organisations qui s'inspirent d'idées ou de théories fondées sur la supériorité d'une race ou d'un groupe de personnes d'une certaine couleur ou d'une certaine origine ethnique, ou qui prétendent justifier ou encourager toute forme de haine et de discrimination raciales ; ils s'engagent à adopter immédiatement des mesures positives destinées à éliminer toute incitation à une telle discrimination, ou tous actes de discrimination, et, à cette fin, tenant dûment compte des principes formulés dans la Déclaration universelle des droits de l'homme et des droits expressément énoncés à l'article 5 de la présente Convention* »[492].

En son article 1, le protocole n° 12 à la Convention européenne des droits de l'Homme pose une « interdiction générale de la discrimination », en précisant que « *la jouissance de tout droit prévu par la loi doit être assurée, sans discrimination aucune, fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation* ». Ainsi que nous l'avons analysé plus haut[493], la Directive du Conseil de l'Union européenne du 29 juin 2000, « relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique », interdit elle-même « *toute discrimination basée sur la race ou l'origine ethnique* »[494].

La protection des personnes contre la discrimination est dès lors de très haute importance, au niveau international, et est un droit de l'Homme et une liberté fondamentale. Il s'agit également, dans la plupart des pays, d'une liberté publique. Parmi les aspects de cette protection spécifique figure l'interdiction générale de la violence et de la torture, actes pouvant se trouver réprimés de manière plus sévère, au niveau national, lorsqu'ils sont commis pour des raisons racistes[495].

Sur Internet, les contenus visés par ces interdictions peuvent être des textes qui incitent à la discrimination, mais également des images de tortures ou de meurtres commis pour des motifs de haine raciale. De telles images, à l'instar de la torture et du meurtre en général,

---

[489] Article 1 de la Convention internationale sur l'élimination de toutes les formes de discrimination raciale.
[490] Adoptée et ouverte à la signature et à la ratification par la résolution de l'Assemblée générale n° 2106 (XX) du 21 décembre 1965, entrée en vigueur le 4 janvier 1969, disponible à l'adresse suivante : http://www2.ohchr.org/french/law/cerd.htm.
[491] Article 2, d, de la Convention.
[492] Article 4 de la Convention.
[493] Voir supra, sous-section 6.5.2.3.
[494] Voir le site web de l'Union européenne, Synthèses de la législation de l'UE, Egalité de traitement sans distinction de race ou d'origine ethnique, disponible à l'adresse suivante : http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33114_fr.htm.
[495] Voir par exemple les articles 222-3, 222-8 et 222-10 du Code pénal français, disponible à l'adresse : http://www.legifrance.gouv.fr/.

sont particulièrement choquantes et offriraient également une justification tout aussi valide que la pédopornographie au filtrage d'Internet, dans les situations où un tel filtrage serait possible et répondrait aux conditions posées au niveau international, conditions que nous étudierons au chapitre 7 de la présente étude.

D'un point de vue juridique, d'autres contenus tels que ceux qui sont en infraction avec des droits de propriété intellectuelle pourraient, suivant la même logique, justifier une mesure de filtrage d'Internet, puisqu'ils sont également contraires à la législation du Conseil de l'Europe. Ceci est vrai, même si de tels contenus sont moins préjudiciables à l'être humain que ceux que nous avons précédemment évoqués.

6.7.3 Les droits de propriété intellectuelle

Les droits de propriété intellectuelle sont protégés par de nombreux traités au niveau international. Notre étude limitera leur analyse aux textes qui en déclarent le principe, étant précisé que ces droits comprennent notamment les droits d'auteur et les droits connexes, ces deux derniers protégeant « *les droits des créateurs, artistes interprètes ou exécutants, producteurs et radiodiffuseurs, et (contribuant) au développement culturel et économique des nations* »[496].

Les droits de propriété intellectuelle sont en premier lieu protégés par l'article 27, 2 de la Déclaration universelle des droits de l'Homme, qui prévoit que « *chacun a droit à la protection des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur* ». Ces droits sont encore protégés par l'article 15, 1 du Pacte international sur les droits économiques, sociaux et culturels, selon lequel « *les Etats parties au présent Pacte reconnaissent à chacun le droit (…) de bénéficier de la protection des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur* ».

Au niveau du Conseil de l'Europe, la Cour européenne des droits de l'Homme protège les droits de propriété sur les biens immatériels sous le visa de l'article 1 du premier protocole additionnel à la CEDH[497]. Au niveau national, ces droits sont encore protégés, par exemple, par le Conseil constitutionnel français[498]. Au niveau de l'Union européenne, la Charte des droits fondamentaux prévoit elle-même que « *la propriété intellectuelle est protégée* », en son article 17, 2[499].

Le droit à la protection des droits de propriété intellectuelle est donc considéré comme un droit de l'Homme et une liberté fondamentale, et peut également être une liberté publique dans certains pays. Ce droit pourrait en conséquence être invoqué en justification d'une mesure de filtrage d'Internet, dès lors qu'une telle mesure serait effectivement en mesure de lui offrir protection.

Pourtant, certains auteurs[500] interprètent l'arrêt Promusicae de la Cour européenne de justice, au terme d'une lecture plutôt simpliste de celui-ci, comme exigeant, toutes proportions gardées, de rééquilibrer les droits en présence en rendant les droits de propriété intellectuelle plus importants qu'ils ne le sont déjà.

---

[496] Organisation mondiale de la propriété intellectuelle (OMPI), « Droits d'auteur et droits connexes », disponible sur le site web de l'OMPI à cette adresse : http://www.wipo.int/copyright/fr/.

[497] Voir par exemple *Anheuser-Busch Inc. c/ Portugal*, arrêt de la Cour du 11 janvier 2007, requête n° 73049/01, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=812724&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. La décision précise en son § 63 que « *la notion de "bien" évoquée à la première partie de l'article 1 du Protocole n° 1 a une portée autonome qui ne se limite pas à la propriété de biens corporels et qui est indépendante par rapport aux qualifications formelles du droit interne : certains autres droits et intérêts constituant des actifs peuvent aussi passer pour des "droits patrimoniaux" et donc des "biens" aux fins de cette disposition* ». Le § 71 de cette même décision rapelle que « *dans une affaire Melnitchouk c. Ukraine, qui concernait la violation alléguée des droits d'auteur du requérant, la Cour a réaffirmé que l'article 1 du Protocole n°1 s'appliquait à la propriété intellectuelle* ». Les §§ 67 et 68 rappellent qu'un brevet peut aussi relever « *du terme "biens" figurant à l'article 1 du Protocole additionnel* ».

[498] Voir par exemple la décision n°2006-540 DC du 27 juillet 2006, J.O.R.F. du 3 août 2006, p. 11541, §§ 13 et 14.

[499] Pour chacune des questions abordées dans ces deux premiers paragraphes, voir Christophe Caron, « Droit d'auteur et droits voisins », Litec, 2006, page 8.

[500] Voir, par exemple, Fanny Coudert et Evi Werkers, « In The Aftermath of the Promusicae Case: How to Strike the Balance? » (« Suite à l'affaire Promusicae : comment trouver l'équilibre? »), International Journal of Law and Information Technology Advance Access published online on October 25, 2008 (Journal international de droit et des technologies de l'information, Accès avancé, mis en ligne le 25 octobre 2008), disponible à partir de l'adresse http://ijlit.oxfordjournals.org/cgi/content/abstract/ean015.

6.8 Les dispositions spécifiques aux communications électroniques

Une mesure de filtrage d'Internet qui constitue une ingérence dans l'exercice de libertés doit être prescrite par la loi et respecter les autres conditions de la clause européenne d'ordre public, laquelle requiert souvent l'intervention d'un juge, ce dernier étant à même de contrôler la proportionnalité de la mesure dans le cadre des garanties devant s'appliquer à tout procès pénal.

Une telle mesure de filtrage, mise en œuvre au sein de l'Union européenne, doit en outre être compatible avec les dispositions européennes relatives aux communications électroniques. Ces dispositions sont essentiellement relatives aux obligations des prestataires de services Internet en termes de qualité de service, de service universel et de neutralité. Les règles relatives au régime de responsabilité des prestataires d'accès à Internet constituent par ailleurs une autre base d'arguments permettant à ces derniers de s'opposer à des mesures de filtrage qui seraient mises en œuvre hors le cadre d'une loi.

6.8.1 Les obligations de service universel et de qualité de service des prestataires de services Internet

En « *réponse à la convergence des technologies, qui rend de plus en plus possible la délivrance de toutes formes de contenus sur tous types de réseaux* », le Parlement et le Conseil de l'Union européenne adoptèrent « *cinq directives qui élargissent le cadre réglementaire relatif aux télécommunications afin de couvrir toutes les formes d'infrastructures de communications électroniques, incluant les réseaux câblés, les réseaux satellites, les réseaux utilisés pour la télédiffusion, les réseaux IP, les systèmes de communication sur réseaux électriques, de même que les réseaux traditionnels fixes et mobiles utilisés pour la voix et les données* »[501].

Parmi ces cinq directives, la « Directive cadre » 2002/21/CE[502] et la « Directive service universel » 2002/22/CE[503] incluent des dispositions relatives au service universel et à la qualité de certains services qui sont susceptibles d'entrer en conflit avec une mesure de filtrage d'Internet[504].

6.8.1.1 Le droit d'accéder à certains services de communication de base

La Directive européenne 2002/22/CE « *vise à assurer la disponibilité dans toute la Communauté de services (de communications électroniques) de bonne qualité accessibles au public grâce à une concurrence et un choix effectifs et à traiter les cas où les besoins des utilisateurs finals ne sont pas correctement satisfaits par le marché* »[505].

La Directive définit donc « *l'ensemble minimal des services d'une qualité spécifiée accessible à tous les utilisateurs finals, à un prix abordable compte tenu des conditions nationales spécifiques, sans distorsion de concurrence* »[506], ce qui correspond à la définition du « service universel »[507]. La Directive « *fixe également des obligations en matière de fourniture d'un certain nombre de services obligatoires (…)* »[508].

Selon l'article 3.1 de la Directive, « *les États membres veillent à ce que les services énumérés dans le (chapitre II) soient mis à la disposition de tous les utilisateurs finals sur leur territoire,*

---

[501] Traduit de l'anglais. Antony Oodan, Keith Ward, Catherine Savolaine, Mahmoud Daneshmand, Peter Hoath, Telecommunications Quality of Service Management, from legacy to emerging services, (*Gestion de la qualité de service des télécommunications, de l'héritage aux services émergents*), Institution of Electrical Engineers, IEE Telecommunications series 48, 2002, p. 382.

[502] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »), Journal officiel du 24 avril 2002, L 108/33.

[503] Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive "service universel"), Journal officiel du 24 avril 2002, L 108/51.

[504] A côté des directive 2002/21/CE et 2002/22/CE, les autres directives comprises dans le paquet Télécom sont la **Directive 2002/19/CE** du Parlement et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive «accès»), journal officiel du 24 avril 2002, L 108, pp. 0007-0020 ; la **Directive 2002/20/EC** du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive "autorisation"), Journal officiel du 24 avril 2002, L 108/21 ; la **Directive 2002/58/EC** du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), Journal officiel du 31 juillet 2002, L 201, pp. 0037-0047.

[505] Article 1 de la Directive. Voir aussi Antony Oodan, Keith Ward, Catherine Savolaine, Mahmoud Daneshmand, Peter Hoath, Telecommunications Quality of Service Management, from legacy to emerging services (*Gestion de la qualité de service des télécommunications, de l'héritage aux services émergents*), op. cit., p. 383.

[506] Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002, article 1, 2). Voir aussi le considérant n° 4 de la Directive.

[507] Voir le considérant n° 4 de la Directive: « Garantir un service universel (c'est-à-dire fournir un ensemble minimal de services déterminés à tous les utilisateurs finals à un prix abordable) (…) ».

[508] Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002, article 1, 2). Voir aussi le considérant n° 4 de la Directive.

indépendamment de leur position géographique, au niveau de qualité spécifié et, compte tenu de circonstances nationales particulières, à un prix abordable ».

Dans ce contexte, les Etats membres peuvent également, « *dans le cadre des obligations de service universel et en fonction des conditions propres à chacun d'eux, arrêter des mesures spécifiques en faveur des consommateurs vivant dans des zones rurales ou géographiquement isolées pour assurer leur accès aux services visés au chapitre II, ainsi que le caractère abordable de ces services, et garantir cet accès dans les mêmes conditions, en particulier aux personnes âgées, aux handicapés et aux personnes ayant des besoins sociaux spécifiques. De telles mesures peuvent également inclure celles qui sont directement ciblées vers les consommateurs ayant des besoins sociaux spécifiques en apportant une aide à des consommateurs identifiés, par exemple par le biais de mesures spécifiques, prises après examen des demandes individuelles, telles que les remises de dettes* » (considérant n° 7).

Les services inclus dans l'obligation de service universel sont « *des services de communication de base, incluant les communications par la voix et une connexion à Internet* »[509]. L'article 4 de la directive prévoit que « *les États membres veillent à ce que toutes les demandes raisonnables de raccordement en position déterminée au réseau téléphonique public et d'accès aux services téléphoniques accessibles au public en position déterminée soient satisfaites par une entreprise au moins* ». Le paragraphe 2 de ce même article précise que « *le raccordement réalisé doit permettre aux utilisateurs finals de donner et recevoir des appels téléphoniques locaux, nationaux et internationaux, des communications par télécopie et des communications de données, à des débits de données suffisants pour permettre un accès fonctionnel à Internet, compte tenu des technologies les plus couramment utilisées par la majorité des abonnés et de la faisabilité du point de vue technique* ».

Chacun de ces deux services, à savoir l'accès au réseau téléphonique public et l'accès à Internet, pourrait être impacté par une mesure de filtrage d'Internet.

6.8.1.1.1 *L'accès au réseau téléphonique public*

La Directive entend assurer aux citoyens de l'Union européenne la possibilité de se connecter au réseau téléphonique public, ainsi que la qualité du service fourni. Elle crée notamment un mécanisme d'évaluation de cette qualité en son article 11, 4, en ajoutant que les autorités réglementaires nationales, lesquelles sont définies par l'article 3 de la Directive 2002/21/CE, « *doivent être à même d'établir des objectifs de performance pour les entreprises assumant des obligations de service universel au moins en vertu de l'article 4. Ce faisant, les autorités réglementaires nationales prennent en considération le point de vue des parties intéressées (…)* ». D'autres obligations sont prévues, telles que l'obligation, pour les Etats, de veiller « *à ce que, en dehors de tout autre numéro national d'appel d'urgence spécifié par les autorités réglementaires nationales, tous les utilisateurs finals des services téléphoniques accessibles au public, y compris les utilisateurs des postes téléphoniques payants publics, puissent appeler gratuitement les services d'urgence en formant le "112", numéro d'appel d'urgence unique européen* » [510].

Toute mesure de filtrage d'Internet qui empêcherait un utilisateur d'accéder au réseau téléphonique public serait dès lors en conflit avec l'obligation de service universel. Tel serait le cas d'une mesure qui conduirait à la suspension ou à l'interruption d'une offre Internet « triple play », laquelle permet aux utilisateurs d'accéder non seulement à Internet, mais aussi au réseau téléphonique et à la télévision. Si les propositions de mise en place d'un système permettant l'interruption des accès à Internet ne sont aujourd'hui relatives qu'à l'accès au réseau Internet lui-même, et non à l'accès au réseau téléphonique qui pourrait se trouver

[509] Traduit de l'anglais. Site web de la Commission européenne, Europe's Information Society, Thematic portal, Policies, eCommunications, « Universal service »", disponible en anglais à l'adresse suivante : http://ec.europa.eu/information_society/policy/ecomm/current/consumer_rights/universal_service/index_en.htm.

[510] Article 26, 1 de la Directive 2002/22/CE.

inclus dans une offre globale[511], la difficulté de dissocier ces différents accès a été mise en lumière au niveau français[512]. Dans tous les cas, lorsque cette dissociation est techniquement réalisable, après implémentation sur le réseau de mécanismes spécifiques, de tels mécanismes peuvent être source de difficultés techniques ou de pannes, lesquelles peuvent logiquement conduire à de plus fréquentes interruptions du service téléphonique.

A côté des difficultés qu'une telle interruption d'accès à Internet peut poser au regard des obligations de service universel, cette mesure peut encore mettre des personnes en danger, lorsque le contrat d'accès à Internet est le seul à permettre l'usage du téléphone. Une telle mesure serait encore plus sévère à l'égard des personnes handicapées, dont le droit d'accéder aux communications électroniques semble être protégé sous le visa des libertés que ces personnes ne peuvent exercer qu'à l'aide de ces communications[513], et qui pourraient être plus particulièrement dépendantes d'une connexion permanente au réseau téléphonique public, au prix le plus abordable.

L'ensemble de ces développements appuie la nécessité de n'imposer la suspension ou l'interruption d'un accès à Internet en tant que sanction que dans certaines situations spécifiques, lorsque le comportement qui se voit sanctionné ne peut recevoir une réponse appropriée que par la voie de cette suspension ou interruption[514], après avoir vérifié que l'utilisateur d'Internet n'est pas, à cette occasion, privé de la possibilité de passer un appel téléphonique, au moins dans les cas de danger.

Cette conclusion est appuyée par le fait qu'un accès Internet est également un élément du service universel, tout au moins s'agissant d'un accès bas débit « fonctionnel ».

6.8.1.1.2 *L'accès à Internet*

L'article 4 de la Directive prévoit que la connexion « *en position déterminée au réseau téléphonique public* » doit être fournie aux citoyens *« à des débits de données suffisants pour permettre un accès fonctionnel à Internet, compte tenu des technologies les plus couramment utilisées par la majorité des abonnés et de la faisabilité du point de vue technique* ».

Le considérant 8 de la Directive ajoute que « *cette exigence se limite à un seul raccordement à bande étroite au réseau* » et que « *la rapidité à laquelle un utilisateur donné accède à Internet dépend d'un certain nombre de facteurs, par exemple du ou des fournisseurs de la connectivité à Internet ou de l'application pour laquelle une connexion est établie* ». Dès lors, ce paragraphe précise qu' « *il n'est pas indiqué d'exiger un débit de données ou un débit binaire spécifique au niveau communautaire* », remarquant que « *les modems en bande téléphonique actuellement disponibles offrent généralement un débit de données de 56 kbit/s et sont dotés de systèmes d'adaptation automatique du débit de données en fonction de la qualité variable des lignes, ce qui peut se traduire par un débit de données réel inférieur à 56 kbit/s* ».

En conséquence, l'obligation de service universel inclut au moins l'accès à Internet bas débit. Toute mesure de suspension ou d'interruption de service qui empêcherait une personne

---

[511] C'est du moins l'objectif de l'initiative française contre les atteintes aux droits de propriété intellectuelle.

[512] Voir par exemple le rapport de l'Autorité réglementaire française, appelée « ARCEP », au gouvernement français, dans le cadre des discussions sur le projet de loi dit « création et Internet ». L'autorité considère qu'un fournisseur d'accès à Internet (FAI) se doit « *d'assurer de manière permanente et continue l'exploitation des services de communications, et de garantir un accès ininterrompu aux services d'urgence. A défaut, le FAI s'exposerait à des sanctions administratives et pénales* » : « L'Arcep dénonce l'excès de précipitation de la loi Hadopi », 29 mai 2008, Pc Inpact, disponible à l'adresse : http://www.pcinpact.com/actu/news/43857-arcep-report-hadopi-olivennes-loi.htm ; Estelle Dumout, « Riposte graduée : l'Arcep demande au gouvernement de retoucher sa copie », 28 mai 2008, ZDNet, disponible à l'adresse : http://www.zdnet.fr/actualites/internet/0,39020774,39381371,00.htm. Voir également Jean Berbinau, Jean-Claude Gorichon, Dominique Varenne, « Création et Internet », rapport n° IV-3.3-2008 – décembre 2008, pp. 16 et s., rapport disponible à l'adresse suivante : http://www.lesechos.fr/medias/2009/0304/300333937.pdf.

[513] Voir supra, sous-section 6.6.3.

[514] Voir infra, sous-section 7.6.4.

d'accéder à Internet, a minima en bas débit, pourrait dès lors se trouver en contradiction avec la Directive.

En effet, l'obligation de service universel est essentiellement posée en termes de fourniture matérielle de connexion, afin d'assurer à chaque foyer la possibilité de se connecter à Internet, et non en termes de connexion effective. Permettre aux citoyens d'accéder à Internet reste un objectif qui doit être mis en équilibre avec les autres droits et libertés, ou l'intérêt général du public. Mais l'intégration de cette obligation au sein des obligations de service universel, qui constituent pour le Sénat français « *la traduction concrète des grands principes juridiques du service public : égalité, continuité, adaptabilité* »[515], consacre l'importance des communications électroniques pour l'exercice des libertés fondamentales, et un pays ne devrait pas délibérément restreindre le droit à l'usage de ces communications sans avoir une raison qui serait proportionnée à l'objectif à atteindre. L'accès à Internet est considéré comme ayant le même statut que le téléphone, au sein de l'Union européenne, et aucun pays ne semble avoir pensé, par exemple, à empêcher un citoyen d'accéder au réseau téléphonique public à partir de son domicile, en sanction d'une infraction pénale qu'il aurait commise en utilisant cette même connexion téléphonique.

La nécessité de ne pas empêcher une personne d'accéder à Internet ou à une partie de ce réseau hors le cadre d'une décision qui équilibrerait ce droit d'accès à un autre intérêt de valeur équivalente, décision qui devrait être prise par un tribunal[516], apparaît dans les projets de lois votés par le Parlement dans le cadre de la réforme de la législation de l'Union européenne sur les télécommunications.

Le nouveau paragraphe 3 bis de la Directive 2009/…/CE en préparation, amendant les directives 2002/21/CE, 2002/19/CE et 2002/20/CE[517], déclare que, « *reconnaissant que l'internet est essentiel pour l'éducation et pour l'exercice pratique de la liberté d'expression et l'accès à l'information, toute restriction imposée à l'exercice de ces droits fondamentaux devrait être conforme à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. La Commission devrait lancer une vaste consultation publique à ce sujet* ».

Le Point 8 du même projet de directive ajoute, au paragraphe 4 de l'article 8 de la Directive actuelle 2002/21/CE selon lequel « *les autorités réglementaires nationales soutiennent les intérêts des citoyens de l'Union européenne, notamment :* », les deux points suivants : « *g) en favorisant la capacité des utilisateurs finaux à accéder à l'information et à en diffuser ainsi qu'à utiliser des applications et des services de leur choix* », et « *h) en appliquant le principe selon lequel aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux sans décision préalable des autorités judiciaires, notamment conformément à l'article 11 de la Charte des droits fondamentaux de l'Union européenne concernant la liberté d'expression et d'information, sauf lorsque la sécurité publique est menacée, auquel cas la décision peut intervenir ultérieurement* ».

---

[515] Sénat, session ordinaire de 2003-2004, Annexe au procès-verbal de la séance du 15 octobre 2003, Rapport fait au nom de la commission des Affaires économiques sur le projet de loi relatif aux obligations de service public des télécommunications et à France Télécom, par M. Gérard Larcher, Sénateur, disponible à cette adresse : http://cubitus.senat.fr/rap/l03-021/l03-0210.html ; (citation in Exposé général, I, A, 1., b) les prestations de service universel, disponible à l'adresse suivante : http://cubitus.senat.fr/rap/l03-021/l03-0211.html).

[516] Voir infra, sous-section 7.8.2.

[517] Position du Parlement européen arrêtée en deuxième lecture le 6 mai 2009 en vue de l'adoption de la Directive 2009/…/CE du Parlement européen et du Conseil modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées , ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques, P6_TC2-COD(2007)0247, disponible à l'adresse suivante : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20090506+ITEMS+DOC+XML+V0//FR#BKMD-22.

Le nouveau paragraphe 22 bis de la Directive 2009/…/CE en préparation, amendant la Directive 2002/22/EC, la Directive 2002/58/EC et le Règlement (CE) n° 2006/2004[518], précise que « *la directive 2002/22/CE (directive "service universel") ne prescrit ni n'interdit les conditions imposées par les fournisseurs, conformément à la législation nationale, pour limiter l'accès des usagers aux services et applications et/ou leur utilisation, mais elle prévoit des informations concernant ces conditions. Les États membres qui souhaitent appliquer des mesures concernant l'accès des usagers aux services et applications et/ou leur utilisation doivent respecter les droits fondamentaux des citoyens, y compris en ce qui concerne la vie privée et le respect de la légalité, et toute mesure de ce type devrait tenir pleinement compte des objectifs politiques adoptés au niveau communautaire, tels que la poursuite du développement de la société de l'information communautaire* ».

L'article 1 de la même Directive 2009 amende la Directive 2002/22/CE en ajoutant en son article premier que « *la présente directive ne prescrit ni n'interdit les conditions imposées par les fournisseurs de services et communications électroniques accessibles au public pour limiter l'accès aux services et applications et/ou leur utilisation, lorsqu'elles sont autorisées par le droit national et conformes au droit communautaire, mais elle prévoit des informations concernant ces conditions. Les mesures nationales relatives à l'accès des utilisateurs finals aux services et applications, et à leur utilisation, via les réseaux de communications électroniques respectent les libertés et droits fondamentaux des personnes physiques, y compris eu égard à la vie privée et au droit à un procès équitable, tel qu'il figure à l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* »[519]. L'article ajoute que « *les dispositions de la présente directive en ce qui concerne les droits des utilisateurs finals s'appliquent sans préjudice de la réglementation communautaire relative à la protection des consommateurs, en particulier les directives 93/13/CEE et 97/7/CE, ni de la réglementation nationale conforme à la législation communautaire* »[520].

En outre, l'Internet à haut débit pourrait être inclus dans le service universel dans le futur.

Le Comité des ministres du Conseil de l'Europe, dans une recommandation qui a pu être considérée comme une reconnaissance de l'accès à Internet en tant que droit fondamental[521], se déclara en effet « *conscient de la valeur de service public de l'Internet, comprise comme étant le fait pour les personnes de compter de manière significative sur l'Internet comme un outil essentiel pour leurs activités quotidiennes (communication, information, savoir, transactions commerciales, loisirs) et de l'attente légitime qui en découle que les services de l'Internet soient accessibles et abordables financièrement, sécurisés, fiables et continus, et rappelant sur ce point la Recommandation Rec(2007)16 du Comité des Ministres sur des mesures visant à promouvoir la valeur de service public d'Internet* » [522].

---

[518] Position du Parlement européen arrêtée en deuxième lecture le 6 mai 2009 en vue de l'adoption de la directive 2009/.../CE du Parlement européen et du Conseil modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs, P6_TC2-COD(2007)0248, disponible à l'adresse suivante : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20090506+ITEMS+DOC+XML+V0//FR#BKMD-15.

[519] § 2 bis du nouvel article 1 de la Directive 2002/22/CE.

[520] § 3 du nouvel article 1 de la Directive 2002/22/CE.

[521] Voir Monica Ermert pour Intellectual Property Watch, « Council of Europe: Access to internet is a fundamental right » (« Conseil de l'Europe : l'accès à Internet est un droit fondamental »), 10 juin 2009, disponible en langue anglaise à cette adresse : http://www.ip-watch.org/weblog/2009/06/08/council-of-europe-access-to-internet-is-a-fundamental-right/ ou à cette adresse : http://oneworldsee.org/node/18675.

[522] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, § 12, disponible à l'adresse suivante : https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

A un niveau plus international encore, une déclaration commune du rapporteur spécial des Nations Unies pour la liberté d'opinion et d'expression, du représentant de l'OSCE pour la liberté des médias et du rapporteur spécial de l'OAS pour la liberté d'expression, énonce que « *le droit à la liberté d'expression impose à tous les Etats une obligation de consacrer les ressources nécessaires à la promotion d'un accès universel à Internet, y compris par l'intermédiaire de points d'accès publics* »[523].

Au niveau européen, la Commission européenne elle-même déclara au gouvernement français que « *la diffusion du haut débit* » était un « *objectif important* », et qu'un juste équilibre devait être trouvé entre celui-ci et « *le besoin de combattre le piratage en ligne* ». La Commission nota, à cette occasion, que « *la Présidence française de l'UE (soutenait) la conception du haut débit comme relevant du service universel* »[524].

S'agissant des modifications de la législation sur les télécommunications, le deuxième paragraphe du considérant n° 3 bis du projet de directive 2009/…/CE amendant la Directive 2002/22/EC, la Directive 2002/58/EC et le Règlement (CE) n° 2006/2004[525], ne limite plus l' « *exigence (…) à un seul raccordement à bande étroite au réseau* »[526]. Il prévoit qu' « *il n'est pas indiqué d'exiger un débit de données ou un débit binaire spécifique au niveau communautaire. Une certaine flexibilité est nécessaire, pour que les États membres puissent prendre, en cas de besoin, les mesures nécessaires pour qu'une connexion soit capable de supporter un débit de données suffisant pour permettre un accès fonctionnel à Internet, tel que le définissent les États membres, en tenant dûment compte des conditions spécifiques aux marchés nationaux, comme par exemple* ***la largeur de bande la plus utilisée par la majorité des abonnés dans un État membre donné*** *et la faisabilité technique, à condition que ces mesures aient pour objectif de réduire les distorsions de concurrence (…)* ». Le projet de directive ajoute, dans le même considérant, que « *ceci ne porte pas atteinte à la nécessité, pour la Commission, de procéder à un réexamen des obligations de service universel, qui pourrait porter notamment sur le financement de ces obligations, conformément à l'article 15 de la directive 2002/22/CE et, le cas échéant, de présenter des propositions de réforme afin de répondre aux objectifs de service public* ».

Si l'accès à Internet haut débit était reconnu dans le futur comme étant une composante du service universel, et si les modifications actuellement apportées à la législation de l'Union européenne relative aux télécommunications étaient finalement adoptées, des dispositions juridiques, spécifiques à l'Union européenne, rappeleraient qu'un Etat n'est pas autorisé à mettre en place de mesure de filtrage concernant un utilisateur d'Internet ou un contenu disponible sur ce réseau sans respecter la Convention européenne des droits de l'Homme, spécialement sa clause d'ordre public et le droit à un procès équitable devant un tribunal ou une cour de justice.

Quelles que soient les conclusions du débat sur le paquet Télécom, un accès à Internet doit en tout état de cause, actuellement, répondre à certaines exigences de qualité, qui pourraient être elles-aussi mises en danger par une mesure de filtrage d'Internet.

---

[523] Traduit de l'anglais. Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of Media and the OAS Special Rapporteur on Freedom of Expression, 21 décembre 2005, § 13, disponible en anglais à l'adresse suivante : http://www.article19.org/pdfs/standards/three-mandates-dec-2005.pdf.

[524] La Tribune.fr, « Loi antipiratage sur Internet: les observations de Bruxelles », 27 novembre 2008, disponible à l'adresse suivante : http://www.latribune.fr/entreprises/communication/telecom-internet/20081127trib000314818/loi-antipiratage-sur-internet-les-observations-de-bruxelles-.html.

[525] Position du Parlement européen arrêtée en deuxième lecture le 6 mai 2009 en vue de l'adoption de la directive 2009/.../CE du Parlement européen et du Conseil modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs, P6_TC2-COD(2007)0248, disponible à l'adresse suivante : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20090506+ITEMS+DOC+XML+V0//FR#BKMD-15.

[526] Voir supra, deuxième § de la présente sous-section.

6.8.1.2 La qualité du service d'accès à Internet

La Directive 2002/22/CE est notamment relative à la qualité de service, laquelle peut être définie comme « *l'impact sur les niveaux de performance collectifs, lié à l'ensemble des paramètres considérés comme pertinents dans le cadre d'un service. Les paramètres d'un service donné peuvent présenter différents niveaux de priorité et de performance en fonction des groupes d'utilisateurs* »[527].

La premier paragraphe de l'article 22 de cette Directive prévoit que « *les États membres veillent à ce que les autorités réglementaires nationales soient en mesure, après avoir pris en compte l'opinion des parties intéressées, d'exiger des entreprises offrant des services de communications électroniques accessibles au public la publication d'informations comparables, adéquates et actualisées sur la qualité de leurs services à l'attention des utilisateurs finals (…)* ». Le deuxième paragraphe de cet article ajoute que « *Les autorités réglementaires nationales peuvent préciser, entre autres, les indicateurs relatifs à la qualité du service à mesurer, ainsi que le contenu, la forme et la méthode de publication des informations, afin de garantir que les utilisateurs finals auront accès à des informations complètes, comparables et faciles à exploiter. Le cas échéant, les indicateurs, les définitions et les méthodes de mesure donnés dans l'annexe III pourraient être utilisés* ».

Les Etats membres qui ont implémenté cette Directive ont également pris des dispositions nationales en la matière. En France, par exemple, l'article L. 33-1 du Code des postes et des communications électroniques prévoit que « *l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur (…) les conditions de permanence, de qualité et de disponibilité du réseau et du service* ». L'article D. 98-4 du dit Code prévoit quant-à-lui, dans une première partie intitulée « *Conditions de permanence du réseau et des services* », que « *l'opérateur doit prendre les dispositions nécessaires pour assurer de manière permanente et continue l'exploitation du réseau et des services de communications électroniques et pour qu'il soit remédié aux effets de la défaillance du système dégradant la qualité du service pour l'ensemble ou une partie des clients, dans les délais les plus brefs. Il prend toutes les mesures de nature à garantir un accès ininterrompu aux services d'urgence. L'opérateur met en œuvre les protections et redondances nécessaires pour garantir une qualité et une disponibilité de service satisfaisantes* ».

Les opérateurs de communications électroniques doivent en conséquence faire en sorte que le service d'accès qu'ils fournissent soit d'une certaine qualité. Ils sont par ailleurs en charge du transport d'informations de service public. Les exigences y attachées peuvent s'ajouter aux obligations spécifiques que ces opérateurs peuvent avoir à respecter lorsqu'ils assurent, en outre, le service universel ou une obligation de service public.

Ceci dit, nous avons analysé au chapitre 5 de la présente étude que les réseaux sont techniquement très complexes et que la plupart des mesures de filtrage d'Internet sont susceptibles d'accroître les latences et le nombre des pannes. Ceci, car ces mesures nécessitent toujours l'implémentation de nouvelles fonctionnalités, sur des équipements qui n'ont pas été, originellement, conçus pour les supporter, ou l'implémentation de nouveaux équipements au niveau de l'équipement d'accès (DSLAM ADSL, DSLAM optique – FTTH – pour l'Internet fixe, Node B ou BTS pour l'Internet sans fil). L'ensemble de ces mesures empêche les opérateurs d'avoir une bonne visibilité, tant des opérations sur le réseau que sur le fonctionnement de ce dernier.

[527] Traduit de l'anglais. Antony Oodan, Keith Ward, Catherine Savolaine, Mahmoud Daneshmand, Peter Hoath, Telecommunications Quality of Service Management, from legacy to emerging services (*Gestion de la qualité de service des télécommunications, de l'héritage aux services émergents*), Institution of Electrical Engineers, IEE Telecommunications series 48, 2002, p. xxii (Glossary).

En conséquence, l'exploitation d'un réseau de communications électroniques et le filtrage sont philosophiquement en opposition, et demander à un opérateur de mettre en œuvre une mesure de filtrage place ce dernier dans une situation où deux obligations aux effets contradictoires doivent être respectées.

Cet état de fait justifie une nouvelle fois qu'il ne soit pas demandé à l'industrie d'un pays donné de mettre en œuvre une mesure de filtrage sur la base d'un contrat ou d'un accord avec le gouvernement, mais qu'une telle mesure soit prévue par une loi tenant compte de la possible interférence du filtrage avec les autres obligations légales que les opérateurs doivent respecter.

Une telle loi devrait également tenir compte de l'obligation de neutralité des prestataires de services Internet.

6.8.2 L'obligation de neutralité des prestataires de services Internet

Les prestataires de services Internet ont l'obligation de rester neutres vis-à-vis du contenu des communications électroniques échangées sur Internet, à l'instar d'autres catégories de transporteurs (par exemple les opérateurs de téléphone traditionnel ou les services postaux). Cette obligation est notamment justifiée par l'impératif de protection du secret de la vie privée et de la correspondance des utilisateurs d'Internet, outre la nécessaire protection de la liberté d'expression, qui implique que seul un juge puisse avoir le pouvoir d'interdire la distribution d'un contenu particulier[528].

Cette obligation de neutralité est consacrée par la Directive 2000/31/CE, dont l'objectif « *est de créer un cadre juridique pour assurer la libre circulation des services de la société de l'information entre les États membres et non d'harmoniser le domaine du droit pénal en tant que tel* »[529]. Le considérant n° 14 de cette même Directive précise que « *la mise en œuvre et l'application de la présente directive devraient être conformes aux principes* ***relatifs à la protection des données à caractère personnel, notamment pour ce qui est*** *(…)* ***de la responsabilité des intermédiaires*** ». Son considérant n° 15 ajoute que « ***le secret des communications est garanti*** *par l'article 5 de la directive 97/66/CE*[530]*. Conformément à cette directive, les États membres doivent interdire tout type d'interception illicite ou la surveillance de telles communications par d'autres que les expéditeurs et les récepteurs, sauf lorsque ces activités sont légalement autorisées* ».

La Directive 2002/58/CE prévoit quant-à-elle, en son article 5, 1, que « *les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité* ».

Au niveau national, les pays ont généralement pris des dispositions, également, pour garantir la confidentialité des communications, au moins à l'occasion de l'implémentation de la Directive. En France, par exemple, l'obligation de neutralité des prestataires de services Internet est actuellement prévue par le Code des postes et des communications électroniques (CPCE). Son article L. 33-1 prévoit que « *l''établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur (…) b) Les conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications* ». L'article D. 98-5 de ce même Code prévoit encore que « *l'opérateur prend les mesures nécessaires pour garantir la neutralité de ses services vis-à-vis du contenu des messages transmis sur son réseau et le secret des correspondances* ». Aux termes de l'article L. 32-1, II, 5° du CPCE, le ministre en charge des communications électroniques et l'autorité réglementaire nationale doivent veiller au respect de cette obligation. Des dispositions pénales assurent en outre le respect, de manière plus générale, du secret des correspondances[531].

---

[528] Voir infra, section 7.8.

[529] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), Journal officiel du 17 juillet 2000, L 178, pp. 0001 – 0016, Considérant n° 8, disponible à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML.

[530] La Directive 97/66/CE a été abrogée et remplacée par la Directive 2002/58/CE.

[531] L'article 432-9 du Code pénal français prévoit que « *le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le*

A cette obligation, pour les prestataires de services Internet, de rester neutres vis-à-vis du contenu des messages échangés sur leur réseau, la Directive ajoute l'impossibilité, pour un Etat membre, d'« *imposer aux prestataires, pour la fourniture des services visée aux articles 12 (simple transport ou "mere conduit"), 13 (forme de stockage dit "caching") et 14 (hébergement), une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites* »[532].

En conséquence de ces principes, un prestataire de services Internet ne peut choisir de transmettre ou de ne pas transmettre un message en fonction de son contenu, excepté sur la base d'une obligation légale qui justifierait son non-respect du principe de neutralité.

Un prestataire de services Internet n'a pas la permission de surveiller les contenus échangés sur son réseau, excepté sur la base d'une obligation spécifique prévue par la loi, dans l'objectif de préserver un objectif légitime.

Une mesure de filtrage d'Internet qui impliquerait la surveillance de contenus échangés sur les réseaux afin d'identifier des contenus illégaux particuliers ne serait elle-même pas permise, sauf si elle était spécifiquement prévue par une loi respectant la clause européenne d'ordre public. Entreraient dans cet exemple les mesures qui permettraient la surveillance de contenus transmis sur Internet par un utilisateur, que celui-ci écrive sur un forum particulier ou qu'il transmette un fichier via le protocole FTP (File Transfer Protocol).

Plus loin, une telle loi ne pourrait pas prévoir une obligation générale, à la charge des prestataires de services Internet, de surveiller l'ensemble des contenus qu'ils transmettent. Ce principe européen peut être un sérieux obstacle à la mise en œuvre d'une mesure de filtrage, puisque toute mesure de ce type implique de surveiller l'ensemble des contenus envoyés ou reçus par l'intermédiaire d'un protocole donné, afin de filtrer les contenus particuliers qui doivent l'être.

En l'absence d'une loi qui les obligerait à filtrer certains types de contenus, les fournisseurs d'accès à Internet ne peuvent en tout état de cause pas surveiller ou filtrer des contenus web sans se placer en infraction avec les conditions de leur régime de responsabilité tel que prévu par la Directive de l'Union européenne, et risquer en conséquence de devenir responsables de l'ensemble des contenus qu'ils transmettent.

---

détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45000 euros d'amende » ; « *Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu* ». L'article 226-15 du Code pénal prévoit que « *le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende* » ; « *Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ».

[532] Article 15 de la Directive.

6.8.3 Le régime de responsabilité des prestataires d'accès à Internet

L'article 12 de la Directive 2000/31/CE prévoit que « *les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire : a) ne soit pas à l'origine de la transmission ; b) ne sélectionne pas le destinataire de la transmission ; et c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission* ».

L'article 12.3 ajoute que ces dispositions « *n'affecte(nt) pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation* ».

Ces dispositions ont également été intégrées dans les droits internes des Etats membres. En France, l'article L. 32-3-3 du CPCE prévoit que « *toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission* ».

En conséquence, un prestataire d'accès à Internet qui sélectionnerait certains contenus afin de les filtrer, sans y être contraint par la loi, serait susceptible de ne plus répondre aux conditions fixées par ce régime spécifique de responsabilité. Un tel prestataire prendrait de fait le risque de voir sa responsabilité engagée devant un tribunal pour chaque contenu illégal qui transiterait potentiellement par ses services, tel qu'une violation de droits d'auteur ou une diffamation. Une telle situation serait source de grande insécurité juridique. Elle mettrait en danger le secteur lui-même de la fourniture d'accès, et plus généralement le développement technologique du pays.

Chapitre 7 METTRE LES LIBERTES FONDAMENTALES EN EQUILIBRE

7.1 Introduction

Du point de vue du Pacte international sur les droits civils et politiques et de la Convention européenne des droits de l'Homme, la question de la mise en équilibre des libertés se révèle toujours dans l'hypothèse d'une limitation apportée à une liberté protégée, dans l'objectif d'en préserver une autre.

Dans le cadre d'une mesure de filtrage d'Internet, les droits de l'enfant, le droit des personnes à la non discrimination, ou les droits de propriété intellectuelle, doivent être mis en équilibre avec les droits et libertés qui leurs sont opposés.

Certains des droits consacrés par le Pacte international sur les droits civils et politiques et la Convention européenne des droits de l'Homme sont « intangibles », tels que le droit à la vie ou le droit de ne pas être torturé, tandis que d'autres sont « conditionnels », parce qu'ils peuvent être l'objet de dérogations et/ou de limitations[533], tels que le droit au respect de la vie privée et le droit à la liberté d'expression.

Le présent chapitre analyse l'ensemble des problématiques liées à de telles limitations. La section 7.2 propose une description de la clause européenne d'ordre public, dont les principes sont autant de directives permettant de s'assurer qu'une limitation, apportée aux droits fondamentaux, est légitime. La section 7.4 étudie le principe de « but légitime », qui permet d'identifier l'objectif dans lequel une mesure de filtrage d'Internet est mise en œuvre et de savoir si cet objectif est raisonnable. Cette section passe en revue une série d'objectifs concrets que peut avoir une mesure de filtrage et explique les raisons pour lesquelles chacun d'entre eux peut être vu, ou non, comme légitime. La section 7.5 étudie le principe de « nécessité dans une société démocratique » et s'attache à vérifier si le filtrage d'Internet répond à un besoin social impérieux. Plusieurs besoins sociaux spécifiques y sont identifiés à cette occasion et passés en revue. Ce principe de nécessité inclut l'impératif selon lequel toute limitation apportée aux libertés fondamentales doit être proportionnée au but légitime qui se trouve poursuivi.

La section 7.6 confronte le critère de proportionnalité à différentes mesures de filtrage d'Internet, en fonction des services que ces mesures concernent et des objectifs qu'elles tentent d'atteindre. La section 7.7 analyse les ingérences supplémentaires que peuvent rendre possibles certaines mesures de filtrage dans l'exercice de libertés, et les raisons pour lesquelles des garanties sont nécessaires pour s'assurer que le mécanisme de filtrage n'étendra pas ses fonctionnalités au delà de celles qui sont prévues pour atteindre son but légitime originel. La section 7.8 se concentre sur le rôle du juge, lorsqu'il s'agit de déterminer la proportionnalité d'une mesure de filtrage et les contenus pouvant être bloqués. Elle décrit les difficultés qui peuvent se poser lorsque ce rôle est joué par d'autres acteurs. La section 7.9 conclut ces développements en proposant un sommaire des étapes à suivre afin de s'assurer qu'une mesure de filtrage d'Internet est légitime dans une société démocratique. La

[533] Frédéric Sudre, op. cit., pages 44-45.

section 7.10 accueille enfin une liste d'études additionnelles, qui seraient nécessaires pour évaluer précisément la légitimité de plusieurs mesures de filtrage d'Internet.

7.2 La clause « d'ordre public »

Une limitation apportée à une liberté dite conditionnelle doit respecter certaines conditions, qui dépendront directement de la nature de la liberté ou du droit considéré. Toute mesure de filtrage d'Internet doit respecter les conditions dans lesquelles la limitation d'une liberté fondamentale est possible.

Ces conditions sont posées par la Convention européenne des droits de l'Homme et, dans une certaine mesure, par le Pacte international sur les droits civils et politiques, au sein d'une dite « clause d'ordre public », contrôlée et clarifiée par la Cour européenne des droits de l'Homme.

La possibilité de limiter l'exercice de droits conditionnels peut prendre deux formes différentes.

- Certaines dispositions consacrant des droits conditionnels énumèrent restrictivement les conditions dans lesquelles une limitation est acceptable, comme que le fait l'article 5 de la CEDH relative au droit à la liberté et à la sécurité[534].
- D'autres dispositions consacrant des droits conditionnels, telles que les articles 8 et 10 de la CEDH relatifs au droit au respect de la vie privée et au droit à la liberté d'expression, prévoient, sous la forme d'un principe général ou d'une « clause générale d'ordre public »[535], que les ingérences doivent être « *prévues par la loi* », être inspirées par « *un ou des buts légitimes* » au regard de l'article qui déclare le droit conditionnel en cause et être « *nécessaire(s), dans une société démocratique, pour atteindre ce ou ces buts* » [536].[537]

Cette clause d'ordre public recouvre en conséquence les trois principes majeurs suivants :

- La compétence exclusive de la loi pour limiter les libertés ;
- La nécessité de poursuivre un ou des buts légitimes, parmi ceux énumérés par la Convention ;
- La « nécessité » de l'ingérence « dans une société démocratique », ce qui est interprété par la Cour européenne des droits de l'Homme comme impliquant que l'ingérence, « *dans une société qui entend demeurer démocratique* »[538],
    - Réponde à un « *besoin social impérieux* »[539], et
    - Soit « *proportionnée au but légitime poursuivi* »[540].

---

[534] L'article 5 prévoit six cas possibles de dispense, qui ne peuvent être mis en œuvre que « *selon les voies légales* ».
[535] Frédéric Sudre, op. cit., pages 44-45.
[536] *Sunday Times c/ Royaume-Uni*, requête n° 6538/74, 26 avril 1979, séries A, n° 30, § 45, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700016&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. Voir aussi *Times newspapers LTD* (n° 1 et 2) *c/ Royaume-Uni*, arrêt du 10 mars 2009**,** requêtes n° 3002/03 et 23676/03, § 37 : « *Une telle ingérence constitue une violation de l'article 10 lorsqu'elle n'est pas "prévue par la loi", inspirée par un ou plusieurs buts légitimes au regard de l'article 10 § 2 et "nécessaire, dans une société démocratique, pour atteindre ce ou ces buts"* ».
[537] Sur cette discussion voir également Jeremy McBride, « Proportionality and the European Convention on Human Rights » (« La proportionnalité et la Convention européenne des droits de l'Homme »), in *The principle of Proportionality in the Laws of Europe* (*Le principe de proportionnalité dans les lois d'Europe*), édité par Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et s., notamment p. 24.
[538] Opinion dissidente commune à M. Wiarda, M. Cremona, M. Thór Vilhjálmsson, M. Ryssdal, M. Ganshof van der Meersch, Sir Gerald Fitzmaurice, Mme Bindschedler-Robert, M. Liesch et M. Matscher, Juges, § 8, disponible sous l'arrêt *Sunday Times*, op. cit.
[539] Sunday Times c/ Royaume-Uni, op. cit., § 59.

Cette clause d'ordre public, telle qu'interprétée par la Cour européenne des droits de l'Homme, serait légitime à s'appliquer également à toute limitation du droit à la liberté d'expression garanti par l'article 19 du PIDCP[541], puisque cet article emploie quasiment la même formulation que la Convention européenne des droits de l'Homme[542]. Les pays parties au PIDCP mais non à la CEDH pourraient s'inspirer de l'interprétation de la Cour, dans un objectif d'harmonisation de l'interprétation de la loi internationale dans le domaine des droits de l'Homme. S'agissant de l'article 17 du PIDCP relatif au droit à la vie privée[543], le texte n'utilise pas la même formule que la CEDH et pourrait dès lors permettre des ingérences plus importantes que cette dernière, de la part de pays qui choisiraient de ne pas respecter les critères plus restrictifs de celle-ci et de s'en tenir à l'interdiction des ingérences « arbitraires » ou « illégales ».

En conséquence, les conditions énumérées dans cette clause d'ordre public, qui s'appliquent également aux droits que déclare la Charte des droits fondamentaux de l'Union européenne[544] et qui ont une influence sur les cours constitutionnelles nationales telles que le Conseil constitutionnel français[545], doivent être respectées dans le cadre de toute mesure de filtrage d'Internet qui constituerait une ingérence dans l'exercice du droit à la liberté d'expression dans les 164 pays qui sont parties au PIDCP. Ces conditions doivent également être respectées par les 47 pays parties à la CEDH. Elles doivent encore être respectées dans le cadre d'une mesure de filtrage qui constituerait une ingérence dans l'exercice du droit à la vie privée, au moins dans les pays parties à la CEDH. Le non respect de ces conditions fait de l'ingérence « *une violation* »[546] de l'article 8 ou de l'article 10 de la CEDH. De fait, il nous semble important de procéder à une analyse détaillée du filtrage à la lumière de chacune de ces conditions.

---

[540] *Sunday Times c/ Royaume-Uni*, op. cit., § 62. Voir également Frédéric Sudre, op. cit., pages 43 et s. ; Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 86.

[541] L'article 19 prévoit, en son point n° 3, que « l'exercice (de la liberté d'expression) comporte des devoirs spéciaux et des responsabilités spéciales. Il peut en conséquence être soumis à certaines restrictions qui doivent toutefois être expressément fixées par la loi et qui sont nécessaires : (a) au respect des droits ou de la réputation d'autrui ; (b) à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques ».

[542] Excepté le fait qu'il ne se réfère pas à une « société démocratique » et qu'il énumère moins de buts légitimes dans lesquels une ingérence est acceptable.

[543] Aux termes de l'article 17 : « 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation » ; « 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

[544] Aux termes de l'article 52 de la Charte de l'UE : « Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ». Cette disposition « est destinée à assurer la nécessaire cohérence entre la Charte et la CEDH en érigeant en principe que, dès lors que les droits garantis par la présente Charte correspondent à des droits qui sont également garantis par la CEDH, le sens et la portée de ces droits, limitations autorisées incluses, sont les mêmes que ceux que leur donne la CEDH » (traduit de l'anglais). Voir le site web de la Charte des droits fondamentaux de l'Union européenne, in « 7. General Provisions » (« 7. Dispositions générales »), « Art. 52. Scope of guaranteed rights » (« Art. 52 : portée des droits garantis »), disponible à cette adresse : http://www.eucharter.org/home.php?page_id=62.

[545] Le Conseil constitutionnel français reconnaît la compétence exclusive du Parlement pour apporter des limitations aux libertés, sur le fondement de l'article 34 de la Constitution et de l'art. 4 de la Déclaration française des droits de l'Homme et du citoyen de 1789. Ce Conseil considère également que le législateur « *ne peut limiter l'exercice d'une liberté qu'en raison d'un impératif constitutionnel* » (voir Frédérique Lafay, note sous la décision du Conseil constitutionnel du 18 janvier 1995, JCP 95, II, 22 525). Le Conseil constitutionnel considère par ailleurs que « *les atteintes portées à l'exercice (des libertés) doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi* » (voir par exemple la décision n° 2009-580 DC du 10 juin 2009, J.O.R.F. du 13 juin 2009, p. 9675, § 15).

[546] Sunday Times c/ Royaume-Uni, op. cit., § 45.

7.3 Le principe de légalité

Chaque fois que la Cour européenne des droits de l'Homme est amenée à se prononcer sur une violation alléguée du droit à la vie privée ou du droit à la liberté d'expression, elle vérifie en premier lieu si l'ingérence était « *prévue par la loi* »[547].

Selon la Cour, cette formule, qui correspond à plusieurs formules anglaises que sont notamment « *in accordance with the law* » (en accord avec la loi), « *prescribed by law* » (prescrit par la loi), ou « *provided for by law* » (prévu par la loi)[548], lesquelles doivent être conciliées, « *dans la mesure du possible* », afin de d'« *atteindre le but et réaliser l'objet (du) traité* », implique que la loi considérée réponde au moins à deux conditions[549] :

- En premier lieu, il est nécessaire que « *la loi soit suffisamment accessible* », ce qui signifie que « *le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné* »[550].

  La notion de loi est ici comprise « *dans son acception "matérielle" et non "formelle*" ». Elle inclut dès lors « *le droit non écrit* », « *les textes de rang infralégislatif* », et parfois la jurisprudence, laquelle « *joue traditionnellement un rôle considérable dans les (pays continentaux), à telle enseigne que des branches entières du droit positif y résultent, dans une large mesure, des décisions des cours et tribunaux* ». « *Dans un domaine couvert par le droit écrit, la "loi"* » est dès lors « *le texte en vigueur tel que les juridictions compétentes l'ont interprété en ayant égard, au besoin, à des données techniques nouvelles* »[551].

- En second lieu, « *on ne peut considérer comme une "loi" qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite* ». Le citoyen doit dès lors, « *en s'entourant au besoin de conseils éclairés, (…) être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé* »[552]. Cette exigence de clarté de la loi a également été rattachée au principe de sécurité juridique par la Cour européenne de justice[553]. Au niveau national, cette exigence a été déduite de l'article 34 de la Constitution française par le Conseil constitutionnel français[554], lequel considère plus généralement que les principes de clarté, d'accessibilité et d'intelligibilité de la loi imposent au législateur « *d'adopter des dispositions suffisamment précises et des formules non équivoques afin de prémunir les sujets de droit*[555] *contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire* »[556].

---

[547] Voir par exemple, s'agissant du droit à la vie privée, *Niemietz c/ Allemagne*, arrêt du 16 décembre 1992, séries A no. 251 B, p. 33, § 34, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700220&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[548] La Cour considère que ces notions font « également foi mais ne concord(ent) pas entièrement ».

[549] Voir *Sunday Times c/ Royaume-Uni*, arrêt du 26 avril 1979, requête n° 6538/74, séries A, n° 30, § 48, disponible à cette adresse : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700016&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[550] *Sunday Times c/ Royaume-Uni*, op. cit., § 49. Sur cette question, voir également Pascale Deumier, « La publication de la loi et le mythe de sa connaissance », Les petites affiches, 6 mars 2000, n° 46.

[551] Toutes les citations proviennent de l'arrêt de la Cour européenne des droits de l'Homme *Kruslin c/ France*, arrêt du 24 avril 1990, séries A, n° 176 A, p. 20, § 29. Sur cette question voir également Frédéric Sudre, op. cit., page 43 ; R. Koering-Joulin, D. 90, chron. p. 187.

[552] Toutes les citations proviennent de l'arrêt de la Cour européenne des droits de l'Homme *Sunday Times c/ Royaume-Uni*, op. cit., § 49. Voir également Frédéric Sudre, op. cit., page 43 ; Steve Foster, *Human Rights and Civil Liberties* (*Droits de l'Homme et libertés publiques*), 2ème éd., 2008, p. 464.

[553] Voir Frédéric Pollaud-Dulian, « A propos de la sécurité juridique », RTDCiv. (3) juill.-sept. 2001, p. 487, réf. p. 489.

[554] Décision n° 2001-455 DC du 12 janvier 2002, J.O.R.F. du 18 janv. 2002, p. 1 053, § 9 ; décision n° 2004-503 DC du 12 août 2004, J.O.R.F. du 17 août 2004, p. 14 648, § 29.

[555] Pour une définition du sujet de droit en droit international, qui a le même sens en droit interne français au regard de la loi française, voir *Collected courses of the Hague Academy of International Law (Recueil des cours de l'Académie de droit international de La Haye)*, vol. 5, vol. 255, 1996, 464 p., page 51 : « *la définition classique d'un sujet de droit renvoie à une entité capable de posséder des droits et des devoirs sur*

Toute mesure de filtrage, a minima lorsqu'elle est mise en œuvre dans le cadre de la CEDH, doit dès lors être prévue par une loi répondant à ces derniers critères. La possibilité, au niveau national, de prévoir le filtrage dans un texte qui ne serait pas de nature législative dépend essentiellement des dispositions de la Constitution nationale concernée. Si cette dernière, par exemple, prévoit que le Parlement seul peut limiter les droits à la vie privée et à la liberté d'expression, ou si elle a pour effet de ne donner ce pouvoir qu'au Parlement, toute mesure de filtrage doit être prévue par un texte provenant de cette même institution. La France est un exemple d'un tel système.

Aux termes de l'article 34 de la Constitution française[557], le législateur ne peut pas reporter sur les autorités administratives ou juridictionnelles le soin de fixer les règles concernant les libertés[558]. Cela fait obstacle, par exemple, à tout accord sur le filtrage qui serait établi entre l'industrie des services Internet et le gouvernement français, ou à toute décision administrative en ce sens.

Le seul type d'accord qui pourrait permettre la mise en place d'une mesure de filtrage, ou d'un mécanisme pouvant plus ou moins être comparé à une telle mesure[559], serait un contrat entre l'internaute et son prestataire de service Internet. Tel serait le cas, premièrement, d'un contrat par lequel l'internaute consentirait ouvertement à ne pas accéder à certains types de contenus, à la condition que ce choix soit libre et qu'il ne lui soit pas imposé[560]. Tel serait le cas, également, d'une clause organisant la possibilité, pour le prestataire de services Internet, de mettre fin au contrat en cas de violation, par l'utilisateur, de certaines règles non abusives de conduite (règles ayant pour objet de préserver l'intégrité du service offert à l'utilisateur)[561]. La légalité d'une telle mesure dépendrait essentiellement du type de contenus concernés, de la nature de la violation susceptible de déclencher l'application de la mesure et des preuves recueillies à cet effet. Il est en effet possible d'imaginer qu'un tel contrat, non rédigé de manière raisonnable, puisse être considéré comme étant en infraction avec les dispositions de la Directive de l'Union européenne concernant les clauses abusives dans les contrats conclus avec les consommateurs (Directive 93/13/CE).

Le juge civil français reste toujours compétent pour vérifier la légitimité d'une telle mesure de filtrage ou d'une telle résiliation de contrat. Ce juge est également compétent pour prononcer une mesure de filtrage sous certaines conditions, mais uniquement car cette possibilité est déjà prévue dans le cadre des articles 808 et 809 du Code de procédure civile[562], de même que par l'article 6, I, 8 de la loi n° 2004-575[563]. Les prestataires de services Internet français peuvent mettre en œuvre des mesures de blocage du spam, en vertu du principe général,

---

le fondement de la loi internationale et ayant la possibilité de défendre ces droits par la voie de recours internationaux » (traduit de l'anglais).

[556] Décision n° 2004-503 du 12 août 2004, op. cit., § 29.

[557] L'article 34 prévoit que seule l'autorité législative « fixe les règles concernant (…) les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques (…) ».

[558] Décision n° 2004-503 DC du 12 août 2004, J.O.R.F. du 17 août 2004, p. 14 648, § 29.

[559] Nous évoquerons notamment la résiliation d'un contrat, qui n'est, sur le plan juridique, pas la même chose qu'une mesure de filtrage.

[560] Une telle mesure de filtrage, si elle ne pouvait pas être refusée, pourrait être considérée par le juge comme une clause abusive, puisqu'elle limiterait sans légitimité le droit à la liberté d'expression de l'utilisateur et pourrait limiter le droit de ce dernier à la liberté de sa vie privée.

[561] Voir par exemple T. Com. Paris, jugement du 5 mai 2004, *Microsoft Corp. et AOL France c/ Monsieur K.*, disponible sur le site Juriscom.net à cette adresse : http://www.juriscom.net/jpt/visu.php?ID=510. Voir également infra, sous-section 7.5.1.

[562] Aux termes de l'article 808 : « Dans tous les cas d'urgence, le président du tribunal de grande instance peut ordonner en référé toutes les mesures qui ne se heurtent à aucune contestation sérieuse ou que justifie l'existence d'un différend ». Aux termes de l'article 809 : « Le président peut toujours, même en présence d'une contestation sérieuse, prescrire en référé les mesures conservatoires ou de remise en état qui s'imposent, soit pour prévenir un dommage imminent, soit pour faire cesser un trouble manifestement illicite » ; « Dans les cas où l'existence de l'obligation n'est pas sérieusement contestable, il peut accorder une provision au créancier, ou ordonner l'exécution de l'obligation même s'il s'agit d'une obligation de faire ».

[563] Loi du 21 juin 2004, JORF n°143 du 22 juin 2004, page 11168. Son article 6, I, 8 prévoit que « l'autorité judiciaire peut prescrire en référé ou sur requête, à (tout prestataire d'hébergement Internet) ou, à défaut, à (tout prestataire d'accès à Internet), toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ».

confirmé par le Code pénal français[564], qui permet à toute personne de se défendre elle-même ou de défendre ses biens (la notion pouvant inclure les services) contre les attaques. Par ailleurs, l'obligation qu'ont les prestataires de services Internet de maintenir une qualité de service[565] est elle-même de nature à justifier une mesure de filtrage du spam.

[564] Le Code pénal français prévoit, en son article 122-5, §2, que « *n'est pas pénalement responsable la personne qui, pour interrompre l'exécution d'un crime ou d'un délit contre un bien, accomplit un acte de défense, autre qu'un homicide volontaire, lorsque cet acte est strictement nécessaire au but poursuivi dès lors que les moyens employés sont proportionnés à la gravité de l'infraction* ».

[565] Voir par exemple l'article L. 33-1 du Code des postes et des communications électroniques, qui prévoit, en son I, § 4, que « *l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur (…) les conditions de permanence, de qualité et de disponibilité du réseau et du service* ».

7.4 Le principe de but légitime

La Convention européenne des droits de l'Homme et, s'agissant de la liberté d'expression, le PIDCP, énumèrent restrictivement les buts légitimes pouvant motiver une ingérence dans l'exercice d'une liberté fondamentale.

S'agissant du droit à la vie privée, la CEDH permet les ingérences lorsqu'elles sont nécessaires (art. 8) :

- *« à la sécurité nationale, à la sûreté publique, au bien-être économique du pays,*
- *à la défense de l'ordre et à la prévention des infractions pénales,*
- *à la protection de la santé ou de la morale,*
- *ou à la protection des droits et libertés d'autrui ».*

S'agissant du droit à la liberté d'expression, la CEDH permet des ingérences lorsqu'elles sont nécessaires (art. 10) :

- *« à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique,*
- *à la défense de l'ordre et à la prévention du crime,*
- *à la protection de la santé ou de la morale,*
- *à la protection de la réputation ou des droits d'autrui,*
- *pour empêcher la divulgation d'informations confidentielles*
- ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire *».*

S'agissant du droit à la liberté d'expression, le PIDCP permet des ingérences lorsqu'elles sont nécessaires (art. 19) :

- « *Au respect des droits ou de la réputation d'autrui* »,
- « *A la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques ».*

Pour être légitime, une mesure de filtrage doit en conséquence poursuivre l'un des objectifs énumérés dans le texte qui s'applique à elle, selon la Convention à laquelle le pays en cause est partie, et selon la liberté fondamentale que cette mesure limite. Par exemple, un pays partie à la CEDH ne peut mettre en œuvre une mesure de filtrage d'Internet qui constituerait une ingérence dans l'exercice du droit à la vie privée, si cette mesure poursuit un objectif différent de ceux qui sont énumérés à l'article 8 de la CEDH.

La détermination de l'intérêt ou de l'objectif poursuivi par une mesure de filtrage peut, en fonction de la nature de celle-ci, se révéler être une question cruciale. Nous nous proposons d'analyser ci-dessous chaque grande catégorie de filtrage d'Internet, afin, d'une part, d'offrir une image détaillée de l'ensemble des débats relatifs au filtrage d'Internet, et, d'autre part, de faciliter la comparaison entre les caractéristiques du filtrage de la pédopornographie sur Internet et celles des autres types de filtrage. Ces mesures sont actuellement débattues dans certains pays à la lumière des objectifs légitimes qu'énumèrent les textes internationaux.

7.4.1 Le filtrage du spam et la protection des droits de propriété intellectuelle

L'initiative la plus simple à comprendre semble être le filtrage du spam. Les objectifs de ce filtrage sont clairement, d'une part, la protection des droits du prestataire de service Internet de préserver l'existence de son service de messagerie électronique, et, d'autre part, la protection de la liberté de correspondance de l'utilisateur de ce même service. En conséquence, le but d'une mesure de filtrage du spam, laquelle peut limiter la liberté de correspondance et dès lors le droit au respect de la vie privée, semble être « *la protection des droits et libertés d'autrui* », qui *se trouve être* un but légitime aux termes de l'article 8 de la CEDH.

S'agissant d'une mesure de filtrage d'Internet mise en place sur un réseau de pair à pair (P2P) ou sur le web, qui aurait pour objectif de bloquer des fichiers ou d'empêcher les internautes d'accéder à des fichiers constituant une infraction à des droits de propriété intellectuelle, l'intention serait de protéger les droits des titulaires de droits. Une telle mesure, qui génèrerait au moins des limitations de la liberté d'expression[566] et, potentiellement, des limitations du droit à la vie privée[567], répondrait a priori au but de protection « *des droits d'autrui* », qui est également un but légitime aux termes des articles 8 et 10 de la CEDH et de l'article 19 du PIDCP. Il serait par ailleurs nécessaire, plus loin, d'analyser le contexte plus large de cette mesure (proportionnalité en termes de coûts, « dommages collatéraux » aux réseaux, sur-blocage, etc.) afin de déterminer la légalité de la mesure dans l'ensemble de ses détails.

Si le but de chacune de ces mesures de filtrage semble ne présenter aucune ambigüité, il reste difficile de déterminer clairement les buts légitimes (par opposition aux motivations subjectives) d'une mesure de filtrage qui empêcherait les internautes d'accéder à un contenu considéré comme illégal, disponible sur le web ou sur un autre réseau, que le contenu « bloqué » soit ou non disponible (facilement et gratuitement) via un autre protocole ou via un mécanisme de contournement de la mesure (tel qu'un serveur proxy).

[566] Voir supra, sous-section 6.6.2.2.
[567] Voir supra, sous-section 6.6.1.

7.4.2 Le but de protection des intérêts de la victime

L'un des objectifs poursuivis par une mesure de filtrage visant des contenus illégaux peut être la protection de l'intérêt de la victime à ne pas être vue dans le cadre d'une scène de crime (par exemple en cas d'images d'abus sur un enfant ou de haine raciale, lorsque la victime y est clairement identifiable). Un tel objectif répond au but légitime déjà exposé de *« protection des droits d'autrui »*, lorsque la mesure qu'il motive limite soit le droit à la vie privée, soit le droit à la liberté d'expression. Toutefois, sur le terrain de la protection de la vie privée, il doit être noté que toutes les images d'abus sur enfants ne permettent pas d'en identifier les victimes. En effet, si de telles identifications étaient aisément possibles, l'analyse détaillée de ces images conduirait à un nombre plus important d'investigations couronnées de succès.

Par ailleurs, il pourrait également être avancé que les victimes pourraient avoir un intérêt à être vues dans le cadre de cette même scène de crime, car cette circonstance faciliterait les signalements de ce crime et encouragerait les investigations afin qu'en soient retrouvés les auteurs, les producteurs et les distributeurs, en plus des victimes elles-mêmes.

Il semble qu'un tel débat ne puisse pas être tranché sans une étude qui tiendrait compte de l'opinion des spécialistes, des citoyens et des victimes identifiées et secourues elles-mêmes. Cette étude devrait s'efforcer de déterminer quels sont les intérêts des victimes, d'une part vis-à-vis des personnes susceptibles d'accéder accidentellement à leurs images (et la proportion que représentent ces personnes), et d'autre part vis-à-vis des personnes qui cherchent volontairement à accéder à de telles images. Le résultat d'une telle étude permettrait de déterminer si la protection des intérêts des victimes peut, dans ces circonstances, être utilisée en justification d'une mesure de filtrage.

7.4.3 Le but de prévention de l'accès à des contenus illégaux : protection de la morale ou de la sensibilité des personnes

Un autre objectif que peut poursuivre une mesure de filtrage visant des contenus illégaux est la protection des personnes contre la vue de ces contenus, pour des considérations morales ou afin de protéger la sensibilité des personnes les plus faibles de la société, ce qui peut également être interprété comme visant la protection de la santé de ces dernières. Chacun de ces objectifs peut correspondre au but légitime de « protection de la santé ou de la morale », prévu par les articles 8 et 10 de la CEDH, ainsi que par l'article 19 du PIDCP.

Toutefois, si le but de protection des personnes les plus faibles peut être vu comme légitime, le lien entre la prévention de l'accès à des contenus illégaux et la morale semble en revanche très faible, spécialement en Europe, puisque les personnes y signalent généralement les contenus illégaux comme la pédopornographie afin que des investigations puissent être menées, pour le crime que ces images véhiculent, et non parce que la morale pourrait en souffrir. Selon la Cour européenne des droits de l'Homme, qui considère que « *le pouvoir national d'appréciation (des Etats) n'a pas une ampleur identique pour chacun des buts énumérés à l'article 10* », « *l'idée que les États contractants "se font des exigences de (la protection de la morale)" (…) varie dans le temps et l'espace, spécialement à notre époque* », et « *les autorités de l'État se trouvent en principe mieux placées que le juge international pour se prononcer sur le contenu précis de ces exigences* »[568].

Dès lors, la légitimité de ce but dépend de la conception de la morale propre au pays concerné. En d'autres termes, cette légitimité dépend de la question de savoir si la société de ce pays considère que les contenus illégaux doivent être combattus pour le crime qu'ils dépeignent, ou si elle considère que les personnes doivent prioritairement être protégées de la vue de ces contenus. Dans le premier de ces cas, il semble que la protection de la morale ne puisse pas être validement invoquée en justification d'une mesure de filtrage. Dans le second de ces cas, alors que la protection de la morale pourrait apparaître comme un but légitime, la protection des personnes contre l'accès à certains contenus déterminés pour des raisons de morale pourrait ne pas correspondre à l'acception démocratique de liberté d'accès à l'information, à tout le moins dans les démocraties libérales[569].

---

[568] *Sunday Times c/ Royaume-Uni,* précité, § 59, se référant à l'arrêt *Handyside c/ Royaume-Uni*, requête n° 5493/72, arrêt du 7 décembre 1976, séries A, n° 24.

[569] Voir par exemple la déclaration commune du représentant de l'OSCE pour la liberté des medias, et de Reporters sans frontières pour garantir la liberté d'expression sur Internet, 17-18 juin 2005, disponible à l'adresse http://www.osce.org/documents/rfm/2005/06/15239_fr.pdf : « *Dans une société démocratique et ouverte, chaque citoyen peut décider des informations auxquelles il veut accéder sur Internet. Le filtrage ou la classification ("rating") des contenus en ligne par un gouvernement est inacceptable. Les filtres ne doivent être installés que par les internautes eux-mêmes. Toute mesure de filtrage à un niveau supérieur (national ou même local) est en contradiction avec le principe de libre circulation de l'information* » ; la Déclaration commune du rapporteur spécial des Nations Unies pour la liberté d'opinion et d'expression, le représentant de l'OSCE pour la liberté des médias et le rapporteur spécial de l'OAS pour la liberté d'expression (Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of Media and the OAS Special Rapporteur on Freedom of Expression), 21 décembre 2005, disponible en anglais à l'adresse www.article19.org/pdfs/standards/three-mandates-dec-2005.pdf: « *Les systèmes de filtrage qui ne sont pas placés sous le contrôle de l'utilisateur – qu'ils soient imposés par un gouvernement ou par un fournisseur de services commerciaux – sont une forme de censure a priori et ne peuvent être justifiés (...)* » (traduit de l'anglais) ; la Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, disponible à l'adresse : https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 : « *Rappelant la Déclaration du Comité des Ministres du 28 mai 2003 sur la liberté de la communication sur l'Internet, qui souligne que les autorités publiques ne devraient pas, au moyen de mesures générales de blocage ou de filtrage, refuser l'accès du public à l'information et autres communications sur l'Internet, sans considération de frontière, mais que cela n'empêche pas l'installation de filtres pour la protection des mineurs, notamment dans des endroits accessibles aux mineurs tels que les écoles ou les bibliothèques* » ; « *Il est essentiel que les internautes connaissent, comprennent et sachent utiliser les filtres internet pour pouvoir exercer pleinement leurs libertés et leurs droits fondamentaux dont, notamment, la liberté d'expression et d'information, et prendre une part active aux processus démocratiques. Lorsqu'un utilisateur est confronté à un filtre, il doit être informé qu'un filtre est activé et, s'il y a lieu, il doit savoir reconnaître et contrôler le niveau de filtrage auquel est soumis le*

7.4.4 Le but de prévention des infractions

Un autre objectif pouvant motiver une mesure de filtrage d'Internet visant des contenus illégaux peut être la répression des infractions.

- En premier lieu, certaines voix font valoir que la consultation régulière d'images à caractère pédopornographique pourrait conduire certaines personnes à devenir pédophiles alors qu'elles ne l'étaient pas. La recherche en la matière n'en est qu'au stade des balbutiements[570]. Il serait nécessaire de démontrer d'urgence la réalité et l'ampleur d'une telle hypothèse, par le biais d'une étude qui expliquerait le processus de « passage à l'acte » et mettrait en lumière le pourcentage que représente la population « à risque », avant que le motif de prévention du crime, dans ce contexte précis, puisse être considéré comme réel et puisse donc légitimer le filtrage au regard de la CEDH et du PIDCP.

- En second lieu, il est parfois expliqué qu'une mesure de filtrage d'Internet serait en mesure de contrer le commerce de la pédopornographie, et dès lors de prévenir la commission d'infractions. Un tel objectif semble légitime, puisque l'existence d'un commerce exploitant les enfants ne peut être niée. Une autre question est toutefois celle de l'impact réel, à court et long terme, d'une mesure de filtrage sur ce commerce, question qui sera analysée dans la section 7.5.

  Nous y verrons que, sur ce point, une étude de l'impact réel du filtrage sur ce type de commerce serait nécessaire, afin de déterminer si l'objectif de prévention du crime est réalisable (avec des résultats durables), et donc légitime. Une telle étude devrait par exemple montrer la proportion approximative des actes de commerce effectués par l'intermédiaire des sites web qui se trouvent ou qui pourraient être bloqués. Elle devrait encore analyser les différentes méthodes qui existent pour accéder à ces sites web, le potentiel que présentent les techniques disponibles en termes de contournement des filtres et l'impact que ces méthodes et techniques auraient sur une mesure de filtrage. Elle devrait également étudier les autres protocoles de communication utilisés pour vendre les contenus litigieux, ainsi que le taux potentiel de transfert de ces contenus comme de leurs clients entre le web et ces autres protocoles, en cas de mise en place d'une mesure de filtrage.

---

contenu qu'il consulte. Il devrait, en outre, avoir la possibilité de contester le blocage ou le filtrage du contenu, et de demander des explications et la mise en place de solutions ».

[570] Voir par exemple Michael Seto, « Assessing the Risk of Sexual Offending Posed by Child Pornography Offenders », Centre for Addiction and Mental Health and University of Toronto, presentation at the 2nd International Symposium on online child exploitation (« Evaluation du risque de délinquance sexuelle présenté par les adeptes de la pédopornographie », Centre pour les addictions et la santé mentale et Université de Toronto, présentation au 2ème symposium international sur l'exploitation des enfants en ligne), disponible en anglais à l'adresse suivante : http://www.innovationlaw.org/Assets/events/Symposium2007/Seto+Presentation.pdf.

7.4.5 Le but de répression des infractions

Généralement, le filtrage d'Internet n'a pas pour but de réprimer les infractions, puisqu'une mesure de filtrage ne permet pas de retirer le contenu litigieux du réseau. Il est dès lors clair que la mesure de filtrage peut, quasiment dans tous les cas, être contournée[571], et qu'elle ne facilite pas les investigations destinées à trouver les victimes et les auteurs de l'infraction en cause (même si l'objet de la mesure n'est pas celui-ci).

Ceci dit, certains pays pourraient décider de filtrer une personne en sanction d'un crime ou d'une autre infraction, c'est-à-dire d'imposer à cette personne la suspension, la limitation ou l'interruption de son accès à Internet, en réponse à son acte. Une telle sanction pourrait être considérée comme poursuivant également un but de prévention du crime, en évitant la commission d'une nouvelle infraction. Dans ces deux cas, la mesure de filtrage aurait un but légitime, dans le cadre de l'application de la clause d'ordre public.

C'est une telle sanction que la France tenta d'implémenter dans son projet de loi dit « création et Internet », en réponse aux violations en ligne de droits de propriété intellectuelle. Ce projet de loi fut censuré sur cette question précise par le Conseil constitutionnel, qui considéra notamment que l'interruption d'un accès à Internet ne pouvait être décidée que par l'autorité judiciaire, lorsque les libertés en présence étaient d'une part la liberté d'expression et d'autre part un droit de propriété immatérielle, et qu'une telle sanction ne pouvait être prise qu'au terme d'une procédure respectant le principe de présomption d'innocence, deux exigences auxquelles le projet de loi ne répondait pas. La France prépare actuellement un nouveau projet de loi visant à tenir compte de ces principes.

Un but légitime, poursuivi par la loi autorisant une mesure de filtrage d'Internet, ne suffit pas à légitimer la limitation d'une liberté dans le contexte de l'application de la clause de la CEDH. La mesure doit encore être *nécessaire dans une société démocratique*.

[571] Voir supra, sections 4.7 et 5.5.

7.5 Le principe de nécessité dans une société démocratique

Le troisième et dernier principe que comprend la clause d'ordre public est le principe de « nécessité », que la Cour européenne des droits de l'Homme interprète comme impliquant qu'une ingérence dans les droits et libertés, « *dans une société qui entend demeurer démocratique* »[572], réponde à un « *besoin social impérieux* » [573] et soit « *proportionnée au but légitime poursuivi* »[574].

Certains juges ajoutèrent qu' « *il n'est pas de société démocratique sans que "le pluralisme, la tolérance et l'esprit d'ouverture" (…) se traduisent effectivement dans son régime institutionnel, que celui-ci soit soumis au principe de la prééminence du droit, qu'il comporte essentiellement un contrôle efficace de l'exécutif, exercé, sans préjudice du contrôle parlementaire, par un pouvoir judiciaire indépendant (…), et qu'il assure le respect de la personne humaine* »[575].

Le principe de nécessité implique dès lors deux éléments : un besoin social impérieux et la proportionnalité de l'ingérence au but légitime qu'elle poursuit.

7.5.1 Un besoin social impérieux

Selon la Cour européenne des droits de l'Homme, « *l'adjectif "nécessaire" (…) implique l'existence d'un "besoin social impérieux"* » ; il « *n'est pas synonyme d'"indispensable", il n'a pas non plus la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun"* »[576]. La Cour ajoute que « *la marge nationale d'appréciation* » accordée par l'article 10 de la CEDH aux Etats membres va « *de pair avec un contrôle européen* », lequel « *porte tant sur la loi de base que sur la décision l'appliquant, même quand elle émane d'une juridiction indépendante* ».

Une mesure de filtrage d'Internet doit dès lors correspondre à un besoin réel de la société, la satisfaction de ce dernier impliquant encore que la mesure soit efficace. Par exemple, le blocage du spam semble répondre à de telles exigences, puisqu'il permet de bloquer un volume important de spam, tous les jours, permettant par là-même au service de rester utilisable et à même de répondre aux besoins des internautes en termes de liberté de correspondre. Une conclusion analogue est moins évidente à émettre s'agissant des autres types de mesures de filtrage d'Internet.

7.5.1.1 La protection des droits de propriété intellectuelle

Il semble difficile d'affirmer qu'une mesure de filtrage d'Internet servant les intérêts des titulaires de droits de propriété intellectuelle répond à un besoin social impérieux.

En réalité, le modèle économique de l'industrie du film et de la musique sur Internet fait actuellement l'objet d'un débat de société, questionnant notamment le faible nombre de

---

[572] Opinion dissidente commune à M. Wiarda, M. Cremona, M. Thór Vilhjálmsson, M. Ryssdal, M. Ganshof van der Meersch, Sir Gerald Fitzmaurice, Mme Bindschedler-Robert, M. Liesch et M. Matscher, juges, § 8, disponible sous l'arrêt *Sunday Times c/ Royaume-Uni*, requête n° 6538/74, 26 avril 1979, séries A, n° 30, disponible à l'adresse suivante : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700016&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[573] *Sunday Times c/ Royaume-Uni*, op. cit., § 59.

[574] *Sunday Times c/ Royaume-Uni*, op. cit., § 62. Voir également Frédéric Sudre, « La dimension internationale et européenne des libertés et droits fondamentaux », in *Libertés et droits fondamentaux*, sous la direction de Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11ème éd., 2005, page 33, not. pages 43 et s. ; Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 86.

[575] Opinion dissidente commune à M. Wiarda et autres, juges, disponible sous l'arrêt *Sunday Times*, précité, § 8 de l'opinion, se référant aux arrêts suivants : *Handyside c/ Royaume-Uni*, requête n° 5493/72, arrêt du 7 décembre 1976, séries A, n° 24, § 49 ; *Klass et autres c/ Allemagne*, arrêt du 6 septembre 1978, séries A, n° 28, §49.

[576] *Sunday Times c/ Royaume-Uni*, op. cit., § 59.

contenu mis légalement à disposition en ligne, et s'interrogeant sur les niveaux appropriés de rémunération des artistes. De fait, le filtrage d'Internet n'est peut-être pas le meilleur moyen de préserver les intérêts des titulaires de droits, ce débat ne pouvant être tranché qu'au terme d'une étude qui se pencherait sur l'ensemble de ces éléments ainsi que sur les réactions et opinions de la société.

Quel que soit le résultat de cette discussion sur le modèle économique des ayants droits, et même si une mesure de filtrage destinée à protéger les intérêts de ces derniers était vue, in fine, comme un besoin réel et actuel, resterait la question de l'utilité et de l'efficacité de la mesure. Nous avons pu étudier, dans notre sous-section 5.4.6, qu'une mesure de filtrage appliquée sur un réseau de pair à pair (P2P) conduirait probablement, en quelques mois, au chiffrement des échanges P2P[577]. Une telle situation empêcherait toute tentative ultérieure de filtrage, de même qu'une quelconque surveillance des contenus échangés en P2P. Une mesure de filtrage appliquée au web peut par ailleurs être contournée très facilement, tant par l'internaute que par le propriétaire du site. Une mesure de filtrage du web ou du P2P ne semble dès lors pas adaptée à la lutte contre les infractions aux droits de propriété intellectuelle, puisqu'elle n'empêche pas les individus de s'échanger les fichiers concernés.

7.5.1.2 La sauvegarde de la morale et la protection des personnes contre la vue de contenus à caractère pédopornographique

Une mesure de filtrage d'Internet destinée à prévenir l'accès des personnes à des contenus illégaux peut avoir pour but la sauvegarde de la morale, ou la protection de la sensibilité de certaines personnes. Dans une telle situation, dès lors que la mesure de blocage ne concerne que des personnes qui n'auraient accédé à ce contenu que de manière accidentelle, cette mesure peut être vue comme utile, en ce qu'elle protège des personnes contre la vue de contenus qu'elles ne souhaitent pas voir.

L'existence d'un besoin social impérieux dépend toutefois de deux éléments additionnels. D'une part, elle dépend du volume de la population à protéger – autrement dit du pourcentage de la population qui accède accidentellement aux contenus illégaux ou immoraux ainsi bloqués – ainsi que de l'efficacité de la mesure à assurer la protection de ces personnes. D'autre part, l'existence d'un besoin social impérieux dépend du pourcentage de contenus susceptibles de heurter les personnes considérées mais qui ne seront pas bloqués par la mesure (par choix ou car ces contenus ne sont pas illégaux). En effet, une mesure de filtrage d'Internet qui ne filtrerait que certains types de contenus choquants ou immoraux, et peut-être des moindres, pourrait être considérée comme insuffisamment utile pour générer un besoin social.

Dès lors, il serait nécessaire de procéder à une étude relative à chacune de ces problématiques. Une telle étude pourrait mettre en lumière le volume de la population à protéger (ce qui impliquerait notamment de connaître le pourcentage des tentatives d'accès aux contenus litigieux dont sont à l'origine des robots ou d'autres machines présentes sur le réseau), ses caractéristiques, et l'impact de la mesure de filtrage sur les sites web bloqués (pour savoir si certains d'entre eux réapparaissent, dans quelle

[577] Voir aussi Jean Cédras, *Le téléchargement illicite d'œuvres protégées par le droit d'auteur*, Rapport à Monsieur le Ministre de la Culture et de la Communication, avril 2007, disponible à l'adresse : www.odebi.org/docs/RapportCedras.pdf ou http://www.laquadrature.net/files/rapport_cedras.pdf page 19 :« *Ces logiciels tels Kaméléon, Mute ou Share sont équipés d'un système de cryptage très élaboré, rendant en outre le filtrage et l'identification des utilisateurs pratiquement impossible. Certes, même si la communication est cryptée, on peut toujours savoir quelles sont les adresses IP de l'émetteur et du destinataire. Mais pour matérialiser l'infraction, en revanche, il faut pouvoir analyser le flux, et donc "casser" le cryptage, ce qui est ardu. Mieux vaut donc aller directement perquisitionner le disque dur de l'internaute et cela même avant d'avoir atteint une présomption forte d'un comportement délictueux, ce qui est problématique au regard des libertés individuelles* » ; voir également Jack Germain, « Encrypted File Sharing : P2P Fights Back » (« Partage de fichiers chiffrés : le P2P contre-attaque »), TechNews World, article du 27 mai 2004, disponible à l'adresse : http://www.technewsworld.com/story/34052.html?wlc=1250777621.

mesure et sous quel délai, et si les nouveaux sites web présentent les mêmes caractéristiques d'accessibilité que les premiers). Une telle étude devrait également analyser le pourcentage que représente chaque type de contenus facilement accessibles sur Internet. Dans ce cadre, elle pourrait mettre l'accent sur les principales catégories identifiées de contenus répréhensibles (pédopornographie, meurtres, viols, autres types de violences ou de tortures), mais également s'attacher à l'étude de chacun des contenus pouvant heurter une population spécifique, en s'appuyant par exemple sur les règles généralement mises en place par les utilisateurs de filtres sur postes clients.

Si une telle étude démontrait qu'une mesure de filtrage d'Internet était nécessaire à la protection de la morale, s'agissant de cet objectif spécifique, la réalité de ce besoin social dépendrait encore du concept même de la morale, dans la société concernée. Nous avons pu analyser que la définition de cette notion varie selon les pays, et une mesure de filtrage ayant pour objectif de protéger la morale ne peut être légitime que si la société considère que cette notion inclut principalement le besoin de protéger les personnes contre la vue de contenus illégaux, et moins le besoin de fédérer les citoyens autour d'un objectif de signalement et de lutte contre les crimes que ces contenus véhiculent. Puisque la notion de morale devrait être déterminée par la majorité des citoyens dans une société démocratique, la protection du contenu de cette notion devrait également correspondre à un besoin social. En conséquence, l'existence d'un besoin social impérieux dépendra essentiellement de la manière dont une société évalue, par exemple, la pédopornographie, autrement dit si cette société est en position de « défense » ou « d'attaque » vis-à-vis de cette infraction.

7.5.1.3 La protection des victimes

Une mesure de filtrage d'Internet peut avoir pour objectif de protéger l'image des victimes d'infractions, telles que la pédopornographie ou l'incitation à la haine raciale. Un tel objectif pourrait toutefois être remis en cause[578] par des personnes qui soutiendraient que le premier intérêt de la victime peut être de faire connaître le crime qu'elle a subi et de permettre aux citoyens d'exprimer des demandes d'investigations.

Nous avons identifié le besoin de conduire une étude sur cette question, dans notre sous-section 7.4.2. Si une telle étude confirmait que le premier intérêt des victimes était de ne pas être vues (a minima par les pédophiles), le filtrage d'Internet dans ce but pourrait dès lors être considéré comme une réponse possible à un besoin social impérieux. Dans un tel contexte, il est toutefois intéressant de noter l'existence d'un groupe d'aide aux victimes appelé « Missbrauchsopfer gegen Internetsperren » (Victimes d'abus contre le filtrage d'Internet), qui fait activement campagne contre le filtrage, en Allemagne.

Quoi qu'il résulte de ce débat, une mesure de filtrage d'Internet ne sera en mesure de répondre à ce besoin de manière appropriée que si elle se montre capable de masquer effectivement l'image des victimes à l'égard des personnes qui auront été identifiées comme heurtant les intérêts de ces dernières en accédant à leur image, parmi les deux groupes de personnes précédemment identifiés - c'est-à-dire les personnes recherchant de telles images et les personnes y accédant involontairement. Il se pourrait, plus loin, que la mesure de filtrage doive protéger l'image des victimes à l'égard de ces deux catégories de personnes. Une étude sur la capacité d'une telle mesure à atteindre cet objectif serait dès lors également requise.

[578] Voir supra, sous-section 7.4.2.

7.5.1.4 La prévention des infractions

Une mesure de filtrage d'Internet peut avoir pour but de prévenir les infractions, en empêchant certaines personnes de devenir pédophiles (ce qui ne pourra devenir un argument raisonné qu'après une étude appropriée, ainsi que nous l'avons analysé dans notre sous-section 7.4.4), en perturbant le modèle économique de la vente de pédopornographie, ou en empêchant les échanges de ressources à caractère pédopornographique.

La prévention du passage à l'acte chez les non-pédophiles

L'utilité d'une mesure de filtrage d'Internet implique, en premier lieu, de s'assurer que le blocage conduira effectivement, par exemple, à empêcher la population considérée comme pouvant passer à l'acte à la suite de la consultation de contenus à caractère pédopornographique, d'accéder à de tels contenus. Sur cette question, l'étude que nous avons requise en notre sous-section 7.4.4 devrait également s'attacher à identifier les différents protocoles Internet utilisés par la population à risque concernée pour accéder à des contenus à caractère pédopornographique, et le comportement prévisible de ces personnes en cas de filtrage appliqué à l'un de ces protocoles. Un autre sujet d'étude pourrait être de vérifier si les personnes devenues pédophiles après avoir visionné certains contenus ne seraient jamais passées à l'acte si elles n'avaient pas accédé à ces images. Une telle étude pourrait montrer si le filtrage permet effectivement de prévenir la pédophilie, ou si les personnes concernées seraient dans tous les cas passées à l'acte, soit après avoir contourné les filtres, soit après avoir utilisé un protocole de communication non filtré, ou soit, encore, malgré un accès plus restreint à des contenus illégaux.

L'entrave au commerce de la pédopornographie et à son modèle économique

S'agissant de l'objectif de contrer le commerce de la pédopornographie et son modèle économique, l'utilité d'une mesure de filtrage ne devrait également pas pouvoir être admise avant qu'une étude appropriée n'ait été diligentée. Une telle étude devrait par exemple montrer la proportion approximative des actes de commerce effectués par l'intermédiaire des sites web qui se trouvent ou qui pourraient être bloqués. Cette étude devrait également analyser les différents moyens qui permettent d'accéder à ces sites web, et l'impact durable qu'auraient ces derniers sur une mesure de filtrage, en termes, par exemple, de contournement de la mesure. Elle devrait étudier les autres protocoles de communication utilisés pour vendre les contenus litigieux, ainsi que le taux potentiel de transfert de ces contenus comme de leurs clients entre le web et ces autres protocoles, en cas de mise en place d'une mesure de filtrage.

La prévention des échanges de pédopornographie

S'agissant du but de prévention des échanges de pédopornographie, la démonstration de l'utilité d'une mesure de filtrage et de l'effectivité de sa réponse à un besoin social impérieux impliquerait qu'une étude soit diligentée aux fins de démontrer que le filtrage conduirait effectivement à empêcher de tels échanges, dans une proportion raisonnable. Une telle étude pourrait examiner la proportion approximative de pédopornographie accessible via le protocole dont le filtrage est planifié, au regard de la proportion approximative des contenus de même nature qui se voient distribués par les délinquants via d'autres protocoles. Cette étude pourrait encore analyser l'impact qu'aurait la mesure projetée sur le comportement des personnes qui distribuent de la pédopornographie ou y accèdent via le protocole filtré, afin de prendre la mesure du taux potentiel de transfert des contenus et des consommateurs de contenus entre ce dernier protocole et les autres.

Si l'ensemble de ces études démontrait que, dans de telles situations, le filtrage est capable d'atteindre le but qu'il poursuit, au moins dans une ampleur suffisamment significative, laquelle aura une incidence au niveau de l'évaluation de la proportionnalité

de l'initiative, nous serions en mesure de confirmer l'utilité de cette initiative, et la réalité de sa réponse à un besoin social impérieux.

7.5.1.5 La répression des infractions

Une dernière question à aborder est le blocage de l'accès à Internet d'une personne afin de prévenir ou de réprimer un délit ou un crime, ainsi que la France est en train de le planifier dans le cadre de son projet de loi appelé « protection pénale de la propriété littéraire et artistique sur Internet », déposé devant le Sénat le 24 juin 2009 suite au rejet par le Conseil constitutionnel d'une partie de la précédente petite loi dite « création et Internet », qui prévoyait un mécanisme similaire. L'utilité d'une telle mesure ne peut pas réellement être questionnée, puisque l'internaute ne pourra plus accéder à Internet depuis son domicile, à tout le moins par l'intermédiaire d'une connexion enregistrée sous son propre nom. Il sera donc plus difficile, à cet utilisateur sanctionné, de commettre une nouvelle infraction.

La question est toutefois de savoir si une telle mesure répond à un besoin social impérieux. La réponse est difficile à apporter, puisqu'elle dépend de la place que la société accorde à Internet, non seulement en tant que loisir ou outil de travail académique, mais encore en tant que moyen d'interaction entre les citoyens et l'Etat (voir par exemple le site http://www.service-public.fr/). En Europe, cette place est substantielle, à tel point que certains auteurs et entités semblent considérer l'accès à Internet comme étant un droit fondamental autonome[579]. A tout le moins, l'accès à Internet est considéré comme un moyen d'exercice de deux libertés fondamentales – le droit au respect de la vie privée et le droit à la liberté d'expression[580]. Dès lors, si la prévention et la répression des infractions est un besoin social impérieux, la coupure d'un accès à Internet ne peut être analysée comme un besoin social que si cette interruption est proportionnée aux actes qui doivent être prévenus ou punis. Il s'agira là d'une question de circonstances.

Deux premières analyses ont été faites de cette question, au niveau français.

- Déconnexion due à des faits de spamming
  La première analyse a été livrée par le juge français à l'occasion de la résiliation du contrat d'accès d'un utilisateur d'Internet, suite à l'envoi de spam, sur le fondement du droit des contrats. Même si une telle déconnexion n'est pas une mesure de filtrage et est relative au droit civil et non au droit pénal, l'affaire reste intéressante à analyser, en ce qu'elle donne un exemple d'évaluation de la proportionnalité entre une action et une « sanction ». Le 5 mai 2004, le juge français considéra qu'un prestataire de services Internet pouvait mettre fin au contrat d'un spammeur pour sa violation des dispositions contractuelles, reconnaissant que l'interdiction de pratiquer le spam était mentionnée dans le contrat et que le prestataire de services avait souffert d'un dommage du fait de cette pratique, tant en termes de réputation qu'en raison des ressources qu'il consacrait à la lutte contre le phénomène[581]. Précédemment, le 15 janvier 2002, la Cour d'appel de Paris avait considéré qu'un prestataire de services Internet pouvait mettre fin à un contrat d'accès pour faits de spam, car l'utilisateur, en faisant « *un usage manifeste et répétitif de (la) technique* » du spam, avait « *perturbé gravement les équilibres du réseau, provoquant de nombreuses réactions de la part d'internautes mécontents dont les messageries étaient surchargées et qui devaient alors supprimer les messages non sollicités en supportant le coût et les désagréments de cette mise à jour* »[582].

[579] Voir supra, sous-section 6.6.2.
[580] Voir supra, sous-sections 6.6.1.2 et 6.6.2.2.
[581] T. Com. Paris, jugement du 5 mai 2004, *Microsoft Corp. et AOL France c/ Monsieur K.*, disponible sur le site de Juriscom.net à cette adresse : http://www.juriscom.net/jpt/visu.php?ID=510.
[582] TGI Paris, réf., 15 janvier 2002, *Monsieur P. V. c/ Société Liberty Surf et Société Free*, disponible sur le site de Juriscom.net à cette adresse : http://www.juriscom.net/txt/jurisfr/cti/tgiparis20020115.htm.

- Déconnexion suite à une violation de droits de propriété intellectuelle
  La deuxième analyse fut celle du Conseil constitutionnel français. Dans sa décision du 10 juin 2009, le Conseil considèra que, sur un terrain où s'opposaient les « *droits des titulaires du droit d'auteur et de droits voisins* » et le droit, pour toute personne, « *de s'exprimer et de communiquer librement, notamment depuis son domicile* », les juridictions de l'ordre judiciaire étaient les seules institutions qui pouvaient recevoir le pouvoir de décider de la légitimité de restreindre ou d'empêcher l'accès d'une personne à Internet[583]. Ainsi que nous pouvons le voir, cette décision ne discuta pas réellement de la mesure de déconnexion à la lumière de l'infraction particulière qui aurait donné lieu à une telle sanction, puisque le Conseil considéra les infractions aux droits d'auteur dans leur ensemble. Cette décision est donc également relative au débat sur la proportionnalité entre l'ingérence et le but légitime poursuivi, qui est la dernière exigence de la clause d'ordre public.

7.5.2 La proportionnalité de la mesure au but légitime poursuivi

L'ingérence que constitue une mesure de filtrage d'Internet dans l'exercice d'une liberté fondamentale doit être proportionnée au but légitime poursuivi par cette mesure, en plus d'être prévue par la loi pour poursuivre l'un des objectifs limitativement énumérés par la CEDH (ou le PIDCP), et de répondre à un « besoin social impérieux ».

7.5.2.1 Le critère de proportionnalité

Le principe de proportionnalité est « *reconnu en tant que principe central gouvernant la mise en œuvre des droits et libertés* » garantis par la Convention européenne des droits de l'Homme et ses protocoles additionnels[584]. Permettant « *une certaine évaluation de l'ampleur que peut prendre une limitation particulière afin de garantir un objectif donné* »[585], le principe de proportionnalité répond au besoin « *d'équilibre entraîné par la mise en œuvre des droits* » qui se trouvent concernés par la clause d'ordre public puisque, sans l'existence de ce principe, « *les dispositions de la Convention seraient sujettes à des restrictions qui priveraient les droits et libertés de tout leur contenu dès lors que ces restrictions seraient prescrites par la loi et poursuivraient un but légitime* »[586], en plus de répondre à un besoin social impérieux.

Un certain nombre de facteurs permettant de « *déterminer où se trouve l'équilibre dans des cas particuliers* » a été mis en lumière par M. Jeremy Mc Bride[587], au travers des arrêts de la Cour européenne des droits de l'Homme.

L'un de ces facteurs est « *l'effet général d'une limitation donnée* »[588]. Par exemple, « *les activités politiques de certains fonctionnaires de l'administration locale* » peuvent être sujettes à des restrictions « *lorsque leur visibilité est de nature à établir aux yeux du public (…) un lien*

---

[583] Voir la décision n° 2009-580 DC du 10 juin 2009, J.O.R.F. du 13 juin 2009, p. 9675, § 16, décision disponible à cette adresse : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html : « *les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins* ».

[584] Traduit de l'anglais. Jeremy McBride, « Proportionality and the European Convention on Human Rights » (« La proportionnalité et la Convention européenne des droits de l'Homme »), in *The principle of Proportionality in the Laws of Europe* (*Le principe de proportionnalité dans les lois d'Europe*), édité par Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et s., citation p. 23.

[585] Traduit de l'anglais. Jeremy McBride, op. cit., p. 24.

[586] Traduit de l'anglais. Jeremy McBride, op. cit., p. 24.

[587] Jeremy McBride, op. cit., p. 24 et s.

[588] Traduit de l'anglais. Jeremy McBride, op. cit., p. 24.

entre ces fonctionnaires et le programme d'un parti politique déterminé, puisque ces fonctionnaires (restent) libres de rejoindre le parti de leur choix et de s'engager dans certaines activités politiques »[589]. Inversement, il « *a été considéré comme inacceptable* » d'interdire « *au requérant de faire certaines déclarations relatives aux dangers des fours à micro-ondes* », car cette mesure « *frappait la substance même de sa thèse, l'empêchant en pratique de fournir sa contribution au débat public* »[590].

Un autre facteur utilisé par la Cour européenne des droits de l'Homme est de savoir « *s'il existait des raisons suffisantes de croire qu'un intérêt particulier était en péril* ». Par exemple, dans l'affaire précédemment citée, « *il n'était pas démontré que la vente de fours à micro-ondes avait été affectée par les commentaires du requérant* »[591].

Par ailleurs, cette analyse peut conduire la Cour européenne des droits de l'Homme à apprécier « *la proportionnalité du comportement précis qui se trouve limité* ». Par exemple, la Cour, pour évaluer le caractère approprié ou non de « *commentaires de journalistes sur les circonstances dans lesquelles des juges et politiciens avaient pris une décision* », vérifia si ces journalistes « *se fondaient sur des éléments factuels suffisants pour leur permettre de bénéficier de la protection, étendue à l'expression des jugements de valeur, de l'article 10* » [592].

Plus loin, la Cour vérifie si le but de l'ingérence « *peut être atteint de manière satisfaisante par d'autres moyens, moins restrictifs de droits* »[593]. Par exemple, « *le fait d'enjoindre à un journaliste de divulguer ses sources à l'origine d'une fuite sur les affaires financières d'une entreprise a été considéré comme injustifié (…) puisque l'objectif était de prévenir la dissémination d'une information confidentielle et que cet intérêt légitime avait déjà été préservé par une injonction interdisant la publication des informations originellement divulguées* »[594].

M. McBride décèle également, dans le cadre des décisions de la Cour européenne des droits de l'Homme, une « *approche variable* » [595] de ce qu'il appelle le « *test de proportionnalité* »[596], selon les libertés sujettes à ingérence. Il voit cette approche variable comme « *particulièrement évidente dans le cadre du contrôle des limitations apportées à la liberté d'expression* »[597], limitations qui doivent être fortement justifiées pour prévaloir, « *la charge de la justification (incombant) particulièrement à l'Etat défendeur* »[598]. Un autre exemple est « *l'empressement considérable à accepter que la croyance selon laquelle la morale est en danger est justifiée* »[599].

---

[589] Traduit de l'anglais. Jeremy McBride, op. cit., p. 25, se référant à *Ahmed et autres c/ Royaume-Uni*, arrêt de la Cour, 2 septembre 1998.
[590] Traduit de l'anglais. Jeremy McBride, op. cit., p. 25, se référant à l'affaire *Hertel c/ Suisse*, arrêt de la Cour, 25 août 1998.
[591] Traduit de l'anglais. Jeremy McBride, op. cit., p. 25. Dans le même sens, le « Groupe de l'article 29 » notait que « *les représentants des forces de l'ordre n'ont réussi à fournir aucune preuve de la nécessité de mesures d'une telle ampleur* », dans son Avis 9/2004 sur le projet de décision cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme, adopté le 9 novembre 2004, WP99, citation page 4, disponible à l'adresse suivante : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_fr.pdf.
[592] Traduit de l'anglais. Jeremy McBride, op cit, pp. 25 et 26, se référant à *De Haes et Gijsels c/ Belgique*, arrêt de la Cour, 24 février 1997, et *Oberschlick c/ Autriche* (n°2), arrêt de la Cour, 1er juillet 1997.
[593] Traduit de l'anglais. Jeremy McBride, op. cit., p. 26.
[594] Traduit de l'anglais. Jeremy McBride, op. cit., p. 26, se référant à *Goodwin c/ Royaume-Uni*, arrêt de la Cour, 27 mars 1996.
[595] Traduit de l'anglais. Jeremy McBride, op. cit., pages 28 et s.
[596] Traduit de l'anglais. Jeremy McBride, op. cit., p. 29.
[597] Traduit de l'anglais. Jeremy McBride, op. cit., p. 30.
[598] Traduit de l'anglais. Jeremy McBride, op. cit., p. 30.
[599] Traduit de l'anglais. Jeremy McBride, op. cit., p. 30.

7.6 Le filtrage d'Internet et le critère de proportionnalité

L'analyse de la proportionnalité d'une mesure de filtrage au but qu'elle poursuit, à la lumière de l'ensemble des critères que nous avons analysés ci-dessus, requiert de distinguer entre chacune de ces mesures, selon leur objectif.

7.6.1 Le filtrage du spam

Le filtrage du spam a pour but de préserver l'existence et la qualité du service offert par le prestataire de messagerie, ainsi que de préserver la liberté de la vie privée de l'utilisateur. Il s'avère que cette mesure remplit ses objectifs, dans une proportion raisonnable. En conséquence, il peut être dit que l'effet général de la mesure est proportionné, dès lors que (i) cette mesure préserve effectivement la possibilité d'utiliser les services de messagerie électronique et le protocole SMTP, que (ii) les expéditeurs bloqués conservent la possibilité de joindre l'équipe du prestataire de services pour solutionner leur problème d'envoi de messages et pour envoyer ces messages à nouveau, et que (iii) l'utilisateur peut choisir d'utiliser ou non les filtres qui délivreront les messages suspectés d'être des spams dans un répertoire dédié.

Le filtrage du spam est par ailleurs justifié par un réel péril mettant en danger les services de messagerie, tandis que le comportement précis qui se trouve limité est le droit d'envoyer des messages électroniques sans respecter les règles mises en place par les prestataires de services Internet pour éviter des volumes de spam trop importants. Cette ingérence semble être raisonnable, au regard du danger qui existe, pour l'utilisateur, de ne plus jamais pouvoir envoyer de messages électroniques ou de perdre confiance dans les services de messagerie.

Enfin, il ne semble pas, à cette heure, qu'une *mesure moins restrictive* puisse préserver le but poursuivi par une mesure de filtrage du spam.

7.6.2 Le filtrage du pair à pair ou du web dans l'intérêt des industries culturelles

Une mesure de filtrage du web ou du pair à pair (P2P) qui servirait les intérêts des titulaires de droits de propriété intellectuelle aurait probablement un effet général plus négatif.

- Premièrement, si le filtrage du pair à pair conduisait au chiffrement des communications de pair à pair de manière à empêcher l'ensemble ou la plupart des actions de surveillance des contenus, il deviendrait quasiment ou totalement impossible de surveiller ces communications, même lorsqu'une telle opération serait autorisée sous conditions (par exemple dans le cadre d'investigations ayant pour objectif de traduire des délinquants devant un tribunal, ou pour des raisons statistiques, sans conservation de données personnelles).
- Deuxièmement, une telle mesure génèrerait des coûts importants pour l'industrie de l'accès à Internet[600], le gouvernement[601] et les utilisateurs d'Internet[602].
- Troisièmement, une telle mesure conduirait au blocage de fichiers conformes à la loi (en ce que la reconnaissance technique reste aujourd'hui imparfaite), ce qui limiterait la liberté de communication et la liberté de la vie privée dans une mesure plus grande que celle qui serait nécessaire pour protéger les intérêts des titulaires de droits[603]. L'analyse d'une mesure de filtrage du web conduite dans le même but mènerait à une conclusion analogue, excepté le fait que le chiffrement est seulement possible sur le protocole https, non sur le protocole http, et que les coûts en seraient moins élevés, pour les prestataires de services et le gouvernement.

S'agissant du critère commandant qu'il y ait « *des raisons suffisantes de croire* » que les intérêts des titulaires de droits sont « *en péril* », nous pouvons dire qu'il n'existe aucune preuve d'un tel danger. Il n'existe aucune preuve de la nature et de l'étendue des pertes potentielles qu'auraient souffertes les titulaires de droits en raison de la violation de leurs droits sur le web ou par l'intermédiaire du pair à pair, en ce que les études, sur ce point, restent imprécises. Ces études ne prennent pas en compte, par exemple, le nombre de personnes ayant accédé à une ressource illégale mais qui auraient payé pour l'acquérir, si elle avait été légalement disponible en ligne. Elles ne prennent pas plus en compte la question de la vente potentielle de produits dérivés (billets de concerts, merchandising, etc.) qui pourrait être généré par un premier accès à une ressource illégale. Des analyses en ce sens ont déjà été initiées, mais une étude plus approfondie serait hautement nécessaire dans le cadre de ce débat[604].

---

[600] Le coût d'implémentation, pour l'industrie de l'accès à Internet, d'un mécanisme permettant de bloquer les utilisateurs dans interrompre le service téléphonique et le service de télévision, lorsque cela est possible, a été estimé à « *70 million d'euros au minimum pour la période 2009-2012* » : Jean Berbinau, Jean-Claude Gorichon, Dominique Varenne, « Création et Internet », rapport n° IV-3.3-2008 – Décembre 2008, p. 35, rapport disponible à cette adresse : http://www.lesechos.fr/medias/2009/0304/300333937.pdf.

[601] Dans les pays où le coût des mesures mises en place dans l'intérêt général doivent être prises en charge par le gouvernement, comme en France (voir par exemple la décision du Conseil constitutionnel n° 2000-441 DC du 28 décembre 2000. Ce principe a également été confirmé dans plusieurs dispositions de la loi française).

[602] L'utilisateur pourrait voir le prix de son abonnement à Internet augmenter, tandis qu'il devrait dans tous les cas supporter le poids de latences et de pannes plus nombreuses, touchant le réseau.

[603] S'agissant de la non pertinence du filtrage du P2P, voir par exemple Philippe Astor, « Filtrage du P2P : les tests du SNEP font un flop », 8 avril 2008, Electron Libre, http://electronlibre.info/Filtrage-du-P2P-les-tests-du-SNEP,060 ; Damien Bancal, « Filtrage du trafic P2P : le grand bide », 10 avril 2008, Zataz.com, http://www.zataz.com/news/16894/Filtrage-du-trafic-P2P;-le-grande-bide.html ; A. Brugidou et G. Kahn, « Etude des solutions de filtrage des échanges de musique sur Internet dans le domaine du peer-to-peer », rapport d'étude, 9 mars 2005, http://ww.culture.gouv.fr/culture/actualites/rapports/filtrage/charte.pdf ; Guillaume Champeau, « Hadopi SE2E04 : faites entrer les juristes », 5 mai 2009, Numerama, http://www.numerama.com/magazine/12826-Hadopi-SE2E04-faites-entrer-les-juristes.html. S'agissant de la question du filtrage du web, voir aussi Marc Rees, « Free ne veut pas entendre parler de filtrage et explique pourquoi », 5 novembre 2008, PC Inpact, http://www.pcinpact.com/actu/news/47097-free-filtrage-forum-droits-internet.htm.

[604] Voir par exemple une étude d'Ipsos Allemagne concluant que « *la possibilité de télécharger illégalement est pour certaines personnes une introduction à (l'acquisition du goût pour) la musique* » : Pyrolyse Bred, « The chinese, champions of illegal music downloads » (« les Chinois, champions du téléchargement illégal de musique »), 24 septembre 2009, http://pyrolysebred.baywords.com/index.php/2009/09/24/the-chinese-

Une mesure de filtrage mise en place dans l'intérêt du secteur de la musique et du film, dont l'objectif serait d'empêcher les personnes d'échanger de la musique ou des vidéos protégées sans le consentement des titulaires de droits sur ces œuvres, pourrait être vue comme proportionnée au regard du troisième critère que nous avons retenu pour évaluer la proportionnalité d'une ingérence, puisqu'un tel échange n'est un comportement ni acceptable, ni proportionné. Toutefois, cette conclusion sur la proportionnalité doit être mesurée aux autres impacts que peut provoquer la mesure concernée. Cette dernière est, en addition, susceptible d'empêcher les mêmes personnes d'accéder à des fichiers sur lesquels elles ont tous les droits et qui sont protégés sous le visa du droit à la liberté d'expression ou du droit au respect de la vie privée, un tel accès consistant en un comportement proportionné.

Finalement, il semble que la protection des droits de propriété intellectuelle puisse être assurée « *par d'autres moyens, moins restrictifs de droits* ». Par exemple, l'industrie culturelle est autorisée, en France, à collecter des données relatives à des violations de ses droits, spécialement sur les réseaux de pair à pair, dans le but de porter les affaires découvertes devant un tribunal[605].

---

champions-of-illegal-music-downloads/ ; « Weltweit laden 44 Prozent der Internet-User illegal Musik aus dem Internet ; Piraten sind gleichzeitig größte legale Konsumenten – auch in Deutschland » (« 44 pour cent des utilisateurs d'Internet téléchargent de la musique illégale, au niveau mondial – Les pirates sont simultanément les plus gros consommateurs légaux – également en Allemagne »), press release (communiqué de presse), 18 septembre 2009, http://knowledgecenter.ipsos.de/docdetail.aspx?c=1043&sid=67F6B1C4-CC4A-4636-A948-1860CB7A00B1&did=2df20c44-f4c4-4e37-a746-e785070a02da et Nil Sanyas, « Quel est le réel champion du piratage : enfin la réponse! », PC Inpact, 21 sept. 2009, http://www.pcinpact.com/actu/news/53141-reel-champion-piratage-reponse-ipsos.htm ; voir également la délibération de l'Autorité française de protection des données personnelles n° 2008-101 du 29 avril 2008, avis n° 08008030, présentant l'avis de l'Autorité sur le projet de loi français dit « création et Internet », disponible à cette adresse : http://www.laquadrature.net/wiki/HADOPI_avis_CNIL, ou au sein du rapport de la « Quadrature du Net », « Hadopi, "riposte graduée" : une réponse inefficace, inapplicable et dangereuse à un faux problème », 9 février 2009, disponible à cette adresse : http://www.laquadrature.net/files/LaQuadratureduNet-Riposte-Graduee_reponse-inefficace-inapplicable-dangereuse-a-un-faux-probleme.pdf, p. 23. Dans cet avis, l'Autorité française de protection des données personnelles observe « *que les seuls motifs invoqués par le gouvernement afin de justifier la création du mécanisme confié à l'HADOPI (c'est-à-dire l'autorité administrative chargée de sanctionner l'internaute dans le cadre du projet de loi français « création et Internet ») résultent de la constatation d'une baisse du chiffre d'affaire des industries culturelles. A cet égard, elle déplore que le projet de loi ne soit pas accompagné d'une étude qui démontre clairement que les échanges de fichiers via les réseaux "pair à pair" sont le facteur déterminant d'une baisse des ventes dans un secteur qui, par ailleurs, est en pleine mutation du fait notamment, du développement de nouveaux modes de distribution des œuvres de l'esprit au format numérique* » (Observations liminaires). Voir également Jean Cédras, *Le téléchargement illicite d'œuvres protégées par le droit d'auteur*, Rapport à Monsieur le Ministre de la Culture et de la Communication, avril 2007, disponible à l'adresse : www.odebi.org/docs/RapportCedras.pdf ou http://www.laquadrature.net/files/rapport_cedras.pdf, n° 6, pages 9 et 10.

[605] Voir l'article 9, 4 de la loi n° 78-17 du 6 janvier 1978. Voir également, par exemple, la décision du Conseil constitutionnel n° 2009-580 DC du 10 juin 2009, J.O.R.F. du 13 juin 2009, p. 9675, §§ 25-27, disponible à l'adresse : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html.

7.6.3 Le filtrage de contenus illégaux présents sur le web ou un réseau de pair à pair (P2P)

7.6.3.1 … dans le but de protéger l'image de la victime

L'« effet général » que vise une mesure de filtrage du web ou du pair à pair mise en place dans le but de protéger l'image des victimes est d'empêcher les individus de voir l'image de la victime dans le cadre d'une scène de crime. Un tel effet semble proportionné, à condition que l'intérêt du public ne soit pas mieux servi par une connaissance plus directe de l'existence de tels crimes, connaissance qui est aussi un droit protégé sous le visa de l'article 10 de la CEDH[606]. Toutefois, ce caractère proportionné ne semble pouvoir être admis qu'aussi longtemps que la mesure de filtrage n'a pas pour effet de filtrer d'autres types de contenus. Malheureusement, d'autres contenus seront probablement bloqués en raison de la faiblesse des systèmes de filtrage d'Internet. Par ailleurs, une image à caractère pédopornographique peut tout à fait refléter la scène d'un crime sans pour autant permettre d'en reconnaître la victime[607], ce qui sera le cas lorsque le visage de cette dernière ou d'autres informations permettant de l'identifier n'apparaîtront pas. L'effet général de la mesure devra encore être évalué au regard de l'efficacité de la mesure de filtrage et du risque de contournement de celle-ci.

S'agissant des "*raisons de croire*" que les intérêts de la victime sont « *en péril* », les intérêts des victimes[608] pourraient également être servis par une meilleure information du public sur les crimes qu'elles ont soufferts, afin d'encourager les signalements aux services chargés de les réceptionner, de stimuler une augmentation de la pression des citoyens sur les gouvernements afin que ces derniers agissent contre ces crimes, et, en conséquence, d'améliorer les investigations et les ressources qui leurs sont dédiées. Cette position est celle qui a été adoptée par l'association allemande des victimes contre le filtrage d'Internet, qui fait valoir, par exemple, que les actions contre les sites web illégaux sont d'une priorité bien plus grande que le filtrage, particulièrement en ce qu'une telle mesure risque d'entraîner une moindre perception du problème par le public[609]. Cette question requiert de plus amples débats, dans le cadre des indications données par la Cour européenne des droits de l'Homme.

S'agissant du critère de « *la proportionnalité du comportement précis qui se trouve limité* », la mesure de filtrage que nous analysons a pour but d'empêcher les individus de voir les victimes d'un crime. La proportionnalité d'un tel comportement peut être analysée à la lumière de l'intérêt du public à identifier une telle victime, et dépendra de la motivation de chaque personne qui verra le contenu concerné. Ces motivations peuvent compter parmi les suivantes :

- Un désir ou une volonté de voir un crime par curiosité, comportement qui ne semble pas proportionné,
- Le désir d'en savoir plus à propos d'un crime, afin d'agir contre lui,
- Aucune motivation, si ce n'est le désir de ne pas voir de telles images.

La proportionnalité de ces trois comportements est en conséquence relative, dès lors que la mesure de filtrage n'empêche pas les personnes de visualiser des contenus conformes à la loi, ce qui limiterait le comportement très proportionné de recevoir des informations, comportement protégé sous le visa du droit à la liberté d'expression.

Enfin, s'agissant de la question de savoir si le but de la mesure de filtrage peut être « *atteint de manière satisfaisante par d'autres moyens, moins restrictifs de droits* », elle semble

[606] Voir supra, sous-section 6.6.2.2.
[607] Outre le fait que la victime puisse ne pas être reconnaissable, la loi française réprime par exemple la pédopornographie lorsque l'infraction n'est pas réelle mais dessinée.
[608] Voir supra, sous-sections 7.4.2 et 7.5.1.3.
[609] Voir le site web http://mogis.wordpress.com/ (visité pour la dernière fois le 4 septembre 2009).

dépendre totalement de la coopération internationale et du souhait des autres pays de préserver les intérêts des victimes, puisque le crime et sa victime ne sont plus visibles si et lorsque le contenu est retiré des serveurs du prestataire d'hébergement.

7.6.3.2 … dans le but de protéger la morale, ou dans le but de protéger les intérêts des personnes sensibles

Une mesure de filtrage du web ou du pair à pair (P2P) mise en place dans le but de protéger la morale ou de protéger les personnes sensibles aura tout d'abord l'effet général d'empêcher les personnes d'accéder accidentellement à des contenus considérés comme contraires à la morale ou choquants, tels que la pédopornographie. Une telle mesure pourrait toutefois conduire à empêcher ces personnes d'accéder à des contenus non controversés, en raison de la faiblesse des mécanismes de filtrage. Elle ne permettra pas, plus loin, d'empêcher l'accès des délinquants à ces mêmes contenus. En conséquence, l'effet général de la mesure pourrait être une dépréciation du droit à la liberté d'expression, tandis que les délinquants auraient toujours accès aux contenus illégaux immoraux ou choquants. Il semble qu'une telle situation ne serait pas très proportionnée.

S'agissant de « *la proportionnalité du comportement précis qui se trouve limité* », la mesure de filtrage a ici pour but de protéger les personnes contre la vue de contenus qui sont soit contraires à la notion de morale dans leur pays, soit dangereux pour leur sensibilité. Le premier de ces comportements ne semble pas être proportionné, notamment en ce que nous avons vu que la Cour européenne des droits de l'Homme considère que « *la notion de morale doit être concédée, quelle que soit la protection qu'un Etat considère comme lui étant appropriée* »[610], sous la réserve selon laquelle la protection des personnes contre l'accès à certains contenus définis, pour des considérations morales, pourrait ne pas correspondre à la conception démocratique du droit à la liberté d'accès à l'information, à tout le moins dans les démocraties libérales[611]. S'agissant du deuxième des comportements que nous mentionnions ci-dessus, la question de sa proportionnalité ne semble pas avoir beaucoup de sens, puisque les personnes concernées demandent elles-mêmes à être protégées contre leur liberté de voir certains contenus heurtant leur sensibilité. Toutefois, la mesure de filtrage aura également pour effet d'empêcher des personnes non-sensibles d'accéder à ces mêmes contenus. S'agissant du but exclusif de protéger la sensibilité, la mesure ne semble pas, en ce cas, proportionnée. Par ailleurs, tout test de proportionnalité devrait aussi évaluer la probabilité statistique qu'une personne protégée accède malgré tout, accidentellement, aux contenus concernés par la mesure de filtrage.

S'agissant de la question de savoir si les intérêts de la morale sont en péril lors de l'accès à des contenus illégaux prédéterminés, nous pouvons considérer que c'est le cas, dès lors que la notion de la morale qu'a le pays concerné interdit ces contenus spécifiques. La santé mentale des personnes sensibles peut également être mise en danger par l'existence de contenus pouvant les heurter.

Enfin, s'agissant de la question de savoir si la protection de la morale peut être assurée « *de manière satisfaisante par d'autres moyens, moins restrictifs de droits* », nous pouvons dire que certaines mesures alternatives, telles que les filtres sur postes clients, seraient plus appropriées.

- En premier lieu, nous avons montré que les personnes souhaitant accéder aux contenus illégaux immoraux ou choquants peuvent toujours contourner les filtres concernant le web, dès lors que le contenu reste en ligne, et que le filtrage du pair à pair conduirait au chiffrement des communications de pair à pair, empêchant ainsi

[610] Traduit de l'anglais. Jeremy McBride, « Proportionality and the European Convention on Human Rights » (« La proportionnalité et la Convention européenne des droits de l'Homme »), in *The principle of Proportionality in the Laws of Europe* (*Le principe de proportionnalité dans les lois d'Europe*), édité par Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et s., citation p. 30. Voir supra, dans notre sous-section 7.5.2.1 concernant « le critère de proportionnalité ».

[611] Voir supra, sous-section 6.3.2.

toute tentative de blocage, excepté à l'origine et à la terminaison de la communication, c'est-à-dire, par exemple, sur la machine de l'utilisateur.

- En second lieu, les personnes sensibles qui doivent être protégées des contenus choquants ne sont certainement pas toutes heurtées de la même manière par le même type de contenus, et devraient par ailleurs être protégées contre l'ensemble des contenus choquants, y compris lorsque ces derniers ne sont pas illégaux. La question de savoir ce qui est choquant pour un individu est très subjective, et la plupart des contenus légaux pourraient être considérés comme dérangeants et préjudiciables par les individus dont la sensibilité ne conduit pas à une intervention directe de la part des gouvernements.

Une même conclusion peut être atteinte s'agissant de la protection de la santé et de l'éducation des enfants, cette dernière semblant raisonnablement requérir la possibilité, pour les enfants, d'avoir accès aux informations utiles pour leur développement et leur éducation à une vie responsable[612], tandis que leurs parents ont le droit de leur donner l'éducation qu'ils pensent être la meilleure[613]. La protection de ces deux catégories de personnes – enfants et personnes sensibles – semble requérir l'utilisation seule de filtres sur postes clients, lesquels permettent une totale individualisation de la protection tout en étant moins restrictifs en termes de préservation des libertés, puisque le filtre s'applique uniquement à la personne concernée.

7.6.3.3 … dans le but de prévenir les infractions

Une mesure de filtrage appliquée au web ou au pair à pair (P2P) dans le but de prévenir les infractions devrait avoir pour objet d'empêcher les personnes de commettre ou d'encourager une infraction en achetant, téléchargeant ou vendant des contenus illégaux (ou en accédant simplement à ces contenus, s'il était démontré que des personnes peuvent devenir pédophiles après avoir été à leur contact). Toutefois, actuellement, il n'est pas véritablement possible de savoir si un tel objectif serait atteint par une mesure de filtrage, puisque qu'aucune étude ne l'a démontré[614]. Si tel était le cas, un tel effet pourrait être vu comme *légitime*, pour autant qu'une mesure de filtrage puisse être suffisamment efficace pour dissuader les personnes concernées d'accéder aux contenus illégaux via d'autres protocoles ou via des mécanismes de contournement de filtres.

Toutefois, la *proportionnalité* de cet effet dépendrait du pourcentage de la population qui cesserait de commettre des infractions après avoir été préservée de l'accès à des contenus illégaux, au regard du volume des restrictions apportées aux libertés par la mesure de filtrage. Si ce pourcentage était bas, le niveau de limitation des autres libertés devrait lui aussi être bas. Autrement dit, l'effet général de la mesure sur les autres libertés devrait être faible, afin que la mesure puisse être considérée comme proportionnée. Ce pourcentage serait bas s'il était par exemple démontré qu'un nombre important de délinquants (qui ne représentent déjà qu'une petite fraction de l'ensemble de la population) continuaient à commettre des infractions. La raison pourrait en être soit qu'ils contournent la mesure de blocage, soit qu'ils auraient dans tous les cas commis leur infraction, sans considération de la mesure de filtrage.

L'effet général de la mesure ne pourrait pas, par exemple, consister en une réduction significative de la liberté d'expression ou de la liberté de la vie privée de chaque citoyen, par le blocage de fichiers ou de pages web conformes à la loi, lesquels constituent l'objet d'exercice ou le moyen d'exercice de ces libertés, ou par une augmentation du coût de l'accès à Internet ou une diminution de la qualité générale de l'accès à Internet, qui serait due aux caractères onéreux et complexe des mesures techniques à mettre en œuvre pour assurer l'absence de blocage de contenus légaux.

[612] Voir supra, sous-section 6.6.2.3.
[613] Voir supra, sous-section 6.6.2.3.
[614] Voir supra, sous-section 7.4.4.

S'agissant du *péril encouru* par l'intérêt de prévention des infractions, nous pouvons dire qu'il est réel. Il n'est ceci dit aucunement démontré, malheureusement, qu'une mesure de filtrage conduirait à réduire le nombre de ces infractions, alors que cette même mesure pourrait parallèlement restreindre certains comportements légitimes et proportionnés.

Le comportement qui se trouverait limité serait celui de contribuer au volume d'infractions commises en accédant à des contenus illégaux. Toutefois, les signalements de contenus illégaux et les demandes, adressées aux gouvernements, d'allouer plus de ressources à la lutte contre le crime seraient également limités, de même que le droit des personnes de connaître le volume de contenus illégaux restant présents sur Internet, spécialement si le gouvernement n'accompagnait pas la mesure de filtrage d'une mise à jour régulière concernant la réalité de la situation. En outre, dès lors que la mesure de filtrage conduirait à filtrer des contenus légaux, le comportement qui se trouverait limité serait le droit d'accéder à des informations conformes à la loi, lequel est protégé sous le visa du droit à la liberté d'expression.

Enfin, s'agissant de la question de savoir si la prévention des infractions pourrait être *assurée par d'autres moyens, moins restrictifs de droits*, il apparaît que certains outils d'aide à l'investigation existent déjà, permettant aux enquêteurs de remonter, en premier lieu, aux auteurs de délits ou de crimes et à leurs victimes et, en second lieu, de localiser les personnes qui accèdent régulièrement à des contenus à caractère pédopornographique. Ces outils et systèmes pourraient être perfectionnés, et leur développement, dans le respect des droits et libertés, semblerait plus approprié qu'une mesure de filtrage, dans un objectif de prévention des délits et des crimes.

Il existe également certaines initiatives, telles que celle de la « coalition financière européenne contre la distribution d'images à caractère pédopornographique sur Internet », que la Commission européenne a soutenu financièrement, et qui semble, sur le principe, constituer un bon moyen de contribuer à l'affaiblissement du commerce de la pédopornographie[615]. Il serait également utile que les Etats rapportent au Secrétariat des Nations Unies pour les droits de l'enfant, dans une section qui deviendrait un standard, les détails de leurs efforts pour se mettre en conformité avec l'article 34 de la Convention. De manière similaire, les organisations non gouvernementales devraient systématiquement inclure, dans leurs rapports informels, une évaluation de conformité avec l'article 34 de la Convention. Améliorer l'attention du public, tant sur les efforts faits dans le sens d'une coopération internationale aux fins d'obtenir le retrait des contenus à caractère pédopornographique depuis leur source, que sur les obstacles que cette coopération rencontre, apparaîtrait comme de nature à produire des résultats positifs.

[615] Voir « La Commission européenne financera la coalition financière européenne pour la lutte contre la distribution d'images à caractère pédopornographique sur Internet », communiqué de presse, 3 mars 2009, disponible à cette adresse : http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/342&format=HTML&aged=0&language=fr&guiLanguage=fr.

7.6.4 Le filtrage d'une personne dans un but de prévention et de répression des infractions

L'effet général du filtrage d'une personne dans un but de répression et de prévention des infractions est d'empêcher cette personne d'accéder à Internet, et parfois même aux services de téléphone et de télévision[616]. Un tel effet est particulièrement lourd puisqu'il prive complètement la personne concernée de sa liberté de recevoir et de communiquer des informations électroniques, de sa liberté d'exercer son droit à la vie privée et familiale et de sa liberté de correspondre, dans l'univers électronique[617]. Dès lors, une telle sanction est particulièrement sévère, et ne peut être considérée comme proportionnée que si elle se trouve justifiée au regard de l'infraction commise et du but poursuivi au travers de la répression de cette dernière, voire de sa prévention.

S'agissant du *péril encouru* par l'intérêt de prévention et de répression des infractions, nous pouvons dire, ainsi que nous l'avons fait à la précédente sous-section, qu'un tel péril est réel. Et il est clair qu'une mesure de filtrage prise contre une personne conduirait à réduire ce péril, puisqu'il deviendrait plus difficile à celle-ci de commettre une infraction par la voie d'Internet.

S'agissant du comportement qui se trouverait limité, il s'agirait simplement mais entièrement du droit d'accéder à Internet, lequel est une « *vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information* »[618], et se trouve protégé par le droit à la liberté d'expression, même s'il n'est pas actuellement considéré comme étant un droit fondamental autonome[619].

Toutefois, ce comportement, utile et propice au développement personnel, n'a en rien à voir avec un comportement qui consisterait à accéder uniquement à Internet pour commettre une contravention, un délit ou un crime. Il serait donc plus conforme au principe de proportionnalité, en réponse à de telles infractions, de poursuivre un autre objectif que le blocage total d'un accès à Internet.

Enfin, s'agissant de la question de savoir si la répression et la prévention des infractions pourrait être *assurée par d'autres moyens, moins restrictifs de droits*, la réponse dépendra certainement des infractions en question, en ce que nous savons que la société a d'ores et déjà développé une large gamme de sanctions contre les crimes et les délits.

---

[616] Les offres dites « triple play » permettent d'accéder simultanément à Internet, au téléphone et à la télévision. L'interruption de l'offre, sans distinction entre les services, conduirait à une interruption de l'ensemble de ces derniers en même temps.

[617] Voir les sous-sections 6.6.1 et 6.6.2.

[618] Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe, 2007/2153(INI), § 23, disponible à l'adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//FR. Voir également supra, sous-section 6.6.2.2.

[619] Voir supra, sous-section 6.6.2.2.

7.7 Les autres conséquences du principe de stricte nécessité des ingérences

Les conséquences qu'une mesure de filtrage d'Internet peut basiquement générer en termes d'ingérence dans l'exercice de libertés ont déjà été mises en lumière. Toutefois, plusieurs mesures de filtrage peuvent autoriser des ingérences additionnelles, en raison de la nature des mécanismes qui sont utilisés pour les mettre en œuvre.

A titre d'exemple, certains mécanismes de filtrage du spam peuvent permettre à un prestataire de services de scanner tout message envoyé ou reçu, ce qui autorise d'autres ingérences telles que la conservation de données personnelles en relation avec l'ensemble du message ou certains mots de son contenu. Ce mécanisme peut par ailleurs faciliter le signalement aux autorités d'un message contenant certains mots-clefs ou images, présumant d'un acte illégal, ou de l'utilisateur qui a envoyé ou reçu un tel message[620].

Une mesure de filtrage du web ou d'un réseau de pair à pair pourrait aussi permettre au prestataire de services ou à l'entité en charge des opérations relatives au mécanisme de filtrage de collecter et de conserver des données relatives au contenu de communications envoyées, reçues ou consultées, avec ou sans données permettant l'identification de l'expéditeur, du destinataire ou du surfeur. Le scan de fichiers de pair à pair pourrait également permettre, à l'instar de notre exemple relatif au filtrage du spam, le signalement aux autorités de contenus potentiellement illégaux, accompagné ou non de données permettant d'identifier les utilisateurs concernés.

De telles initiatives constitueraient des ingérences supplémentaires, disproportionnées, dans l'exercice du droit au respect de la vie privée et du droit à la liberté d'expression.

Toute mesure qui constitue une ingérence dans l'exercice de certaines libertés doit voir sa proportionnalité évaluée, en premier lieu, au regard du but légitime qui lui a été assigné, et, en second lieu, au regard de son effet général. Cet effet général ne doit pas aller au delà de ce qui est nécessaire pour atteindre le but poursuivi, et, dans tous les cas, doit « *ménager un certain périmètre* » pour l'exercice de la liberté qui se voit ainsi limitée, et non « *provoquer (l') extinction* » de cette dernière[621].

- La proportionnalité d'une mesure de filtrage du spam sera généralement évaluée dans le cadre du but qu'elle poursuit, à savoir la protection de la liberté de correspondance des utilisateurs et le droit du prestataire de services Internet de défendre son propre service contre les menaces qui peuvent l'atteindre.
- La proportionnalité d'une mesure de filtrage des infractions aux droits de propriété intellectuelle sera généralement évaluée dans le cadre du but qu'elle poursuit, de protection des intérêts des titulaires de droits.
- La proportionnalité d'une mesure de filtrage de la pédopornographie peut être évaluée dans le seul cadre d'un but de protection de la morale, de protection des droits de l'enfant ou de la sensibilité des personnes.

Dans toutes ces situations, la mesure mise en œuvre ne permet pas de poursuivre un but différent de celui qui a été utilisé pour son évaluation et qui a été autorisé. En conséquence, une mesure de filtrage du spam ou une mesure de filtrage visant les atteintes à des droits de propriété intellectuelle ne peut pas être utilisée, par exemple, dans un but de détection du crime[622].

---

[620] Voir supra, sous-section 5.4.3.

[621] Traduit de l'anglais. Jeremy McBride, « Proportionality and the European Convention on Human Rights » (« La proportionnalité et la Convention européenne des droits de l'Homme »), in *The principle of Proportionality in the Laws of Europe* (*Le principe de proportionnalité dans les lois d'Europe*), édité par Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et s., citation p. 24.

[622] La finalité de l'ingérence est également un critère d'évaluation de la légitimité des ingérences dans l'exercice du droit à la protection des données personnelles : voir la Directive 95/46/CE.

S'agissant de mesures de filtrage d'Internet qui seraient mises en œuvre dans un but de répression ou de prévention des infractions, leur proportionnalité devrait être évaluée au regard de l'effet général que produit l'ensemble de leurs caractéristiques techniques, effet général qui devrait être limité au strict nécessaire permettant de répondre au besoin social impérieux qui les a motivées. Par exemple, une mesure de filtrage de la pédopornographie qui serait mise en œuvre dans le but de prévenir certaines personnes de devenir pédophiles et de porter atteinte à l'activité commerciale de vente de pédopornographie ne pourrait pas conduire à la surveillance de l'accès à Internet de certaines personnes, sauf si une telle surveillance répondait elle-même à un besoin social impérieux dans un but de lutte contre le crime, et qu'elle était prise en compte dans le cadre de l'évaluation de la proportionnalité de la mesure dans son ensemble.

Dans tous les cas, l'effet général de ce type de mesures ne peut pas impliquer qu'une liberté soit privée de l'essentiel de son contenu. Toutefois, la surveillance de chaque communication aux fins de conserver des informations personnelles en relation avec un contenu vu, envoyé ou reçu, ou aux fins de signaler chaque infraction ou un type particulier d'infractions aux autorités, annihile le droit à la confidentialité de la vie privée et nuit gravement au droit à la liberté de la vie privée[623]. La non-proportionnalité d'une telle mesure a été confirmée sans équivoque par la Cour européenne des droits de l'Homme dans son arrêt *Klass* : « *quant au choix des modalités (d'un) système de surveillance, la Cour relève que le législateur national jouit d'un certain pouvoir discrétionnaire. (...) La Cour souligne néanmoins que les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée* »[624]. Une déclaration analogue fut également faite par l'avocat général Kokott de la Cour européenne de justice à propos de l'affaire C-275/06 (affaire « Promusicae »), dans le paragraphe 82 de son avis : « *l'on peut légitimement douter qu'il soit compatible avec les droits fondamentaux de stocker les données relatives au trafic de tous les utilisateurs, c'est-à-dire, en somme, de les conserver en vue d'une utilisation ultérieure, même en l'absence de tout soupçon concret* ».

Une telle absence de proportionnalité fut également critiquée par le Groupe de l'article 29 sur la protection des données, dans son « avis sur le projet de décision cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme » : « *Le stockage global de routine de l'ensemble des données de trafic, des données sur les utilisateurs et les participants proposé dans le projet de décision ferait de la surveillance autorisée dans ces circonstances exceptionnelles la règle générale. Cela serait manifestement démesuré. Le projet de cadre s'appliquerait, non seulement à certaines personnes qui seraient surveillées en application de lois spécifiques, mais à tous les particuliers qui utilisent les communications électroniques. En plus, toutes les communications envoyées ou reçues seraient couvertes. Les mesures qui pourraient s'avérer utiles pour faire respecter la loi ne sont pas toutes souhaitables ou ne sauraient être toutes considérées comme une mesure nécessaire dans une société démocratique, en particulier si cela aboutit à l'enregistrement systématique de toutes les communications électroniques. La décision cadre n'a fourni aucun argument de nature à persuader que la conservation des données de trafic à grande échelle de ce type constitue l'unique option viable pour lutter contre la criminalité ou protéger la sécurité nationale* »[625].

---

[623] La réalité de ce droit implique qu'il soit exercé dans la confidentialité. Voir notre sous-section 6.6.1.

[624] *Klass et autres c/ Allemagne*, requête n° 5029/71, arrêt du 6 septembre 1978, séries A, n° 28, § 49, disponible à l'adresse suivante : http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=699944&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649.

[625] Groupe de l'article 29 sur la protection des données, avis 9/2004 sur le projet de décision-cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications

En conclusion, chaque fois qu'une mesure de filtrage est autorisée, certaines garanties doivent être prises afin que cette mesure ne soit pas utilisée d'une manière qui pourrait provoquer une plus grande ingérence dans les libertés. Ce principe s'applique également aux mesures poursuivant un but légitime et dont les fonctionnalités de base ne limitent pas les libertés de manière disproportionnée, car de telles mesures sont toujours susceptibles de présenter l'un des risques analysés ci-dessus. Ces garanties peuvent être techniques, et consister en la mise sous contrôle des fonctionnalités qui pourraient menacer plus avant les libertés, ou juridiques, et consister en la prohibition des fonctionnalités concernées elles-mêmes ou de leur utilisation, lorsque ces dernières ne sont pas essentielles au fonctionnement du mécanisme de blocage.

Par ailleurs, un juge doit chaque fois être mis en mesure de contrôler la proportionnalité de toute mesure spécifique de filtrage.

publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme, adopté le 9 novembre 2004, WP99, citation page 4, disponible à l'adresse suivante : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_fr.pdf.

7.8 La compétence du juge pour contrôler la proportionnalité des ingérences dans l'exercice des libertés fondamentales

La Cour européenne des droits de l'Homme procède au contrôle des mesures, prises par les Etats contractants, qui constituent des ingérences dans l'exercice de libertés fondamentales, ainsi qu'au contrôle de leur évaluation par les juges nationaux. Les juridictions nationales sont également compétentes pour connaître des contestations relatives à la mise en place d'une mesure de filtrage, appliquée par exemple à un citoyen, ou à un contenu que ce citoyen aurait souhaité envoyer, recevoir ou consulter.

Dès lors, toute mesure de filtrage mise en place à l'initiative d'un prestataire de services Internet peut être remise en cause devant le juge – à tout le moins dans les pays qui sont parties à la CEDH.

Toutefois, si avoir le droit de remettre en cause une décision qui limite l'une de ses libertés est pour le citoyen un droit fondamental[626], l'exercice de ce droit suppose que la liberté en cause a d'ores et déjà connu une limitation, dont le citoyen a déjà dû subir les effets. Pour cette raison, il reste important que, dans certaines situations, un juge puisse intervenir avant que la décision de limiter un droit ne soit prise. S'agissant du filtrage d'Internet, ces situations sont celles dans lesquelles il est nécessaire, d'une part, d'évaluer puis de constater l'illégalité d'un contenu ou d'une action, et, d'autre part, d'apprécier la proportionnalité de la réponse à apporter à une situation illégale.

7.8.1 L'évaluation de l'illégalité et sa déclaration

Dans les pays où l'autorité judiciaire est indépendante du pouvoir législatif et du pouvoir exécutif, ce qui devrait être le cas dans toutes les démocraties libérales[627], seul un juge devrait avoir la compétence de constater l'illégalité d'un contenu, d'une situation ou d'une action. Ce pouvoir exclusif, prévu par le système juridique national, implique que ce contenu, cette situation ou ce comportement, soit qualifié de « potentiellement » illégal jusqu'à ce qu'un juge ait été mis en mesure de se prononcer sur la question de son illégalité.

En ce qui concerne les contenus illégaux à filtrer, toute autre approche qui permettrait à un gouvernement, ou même à une entité privée, de décider ce qui est ou non illégal et dès lors ce que les personnes ont le droit de voir ou de ne pas voir, serait inacceptable dans une société démocratique[628], sauf dans les cas où les utilisateurs d'Internet auraient le contrôle des filtres mis en place[629].

---

[626] Article 6 de la CEDH ; article 14 du PIDCP.

[627] Larry Diamond, « Defining and Developing Democracy » (« Définir et développer la démocratie »), in Robert Alan Dahl, Ian Shapiro et José Antônio Cheibud, *The democracy sourcebook*, p. 35 : « *Précisément, les démocraties libérales présentent les composantes suivantes : (…) le pouvoir exécutif est contraint, constitutionnellement et dans les faits, par le pouvoir autonome des autres institutions gouvernementales (telles qu'une autorité judiciaire indépendante, un parlement et d'autres mécanismes de responsabilité horizontale* »).

[628] Voir par exemple Conseil de l'Europe, Déclaration du Comité des ministres sur les droits de l'homme et l'état de droit dans la société de l'information, 13 mai 2005, disponible à cette adresse : https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)56&Language=lanFrench&Ver=final&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 : « *Les Etats membres doivent préserver et renforcer les mesures juridiques et pratiques pour éviter la censure de l'Etat et du secteur privé. D'autre part, ils doivent veiller au respect du Protocole additionnel à la Convention sur la cybercriminalité et des autres conventions en vigueur qui incriminent les actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. A cet égard, les Etats membres doivent promouvoir l'établissement de cadres d'autorégulation et de corégulation par les acteurs du secteur privé (comme l'industrie des TIC, les prestataires de services Internet, les fabricants de logiciels, les fournisseurs de contenus et la Chambre internationale de commerce). Ces cadres doivent assurer la protection de la liberté d'expression et de communication* » ; « *Les Etats membres doivent promouvoir, par des moyens appropriés, des normes techniques compatibles dans l'environnement numérique, y compris des normes relatives à la radiodiffusion numérique, permettant aux citoyens d'accéder le plus largement possible aux contenus* » ; La déclaration commune de la Commission des Nations unies pour les droits de l'Homme, l'OSCE et l'OAS (the Joint declaration by UN commission of human rights, OSCE and OAS), 21 décembre 2005, disponible en anglais à l'adresse : www.article19.org/pdfs/standards/three-mandates-dec-2005.pdf : « *Les systèmes de filtrage qui ne sont pas placés sous le contrôle de l'utilisateur – qu'ils soient imposés par un gouvernement ou par un*

Par ailleurs, constater l'illégalité d'un contenu particulier implique de reconnaître a minima la réalisation de l'élément matériel d'une infraction, même si aucune poursuite n'a été initiée contre son auteur, et même si la responsabilité de cet auteur n'était pas reconnue dans le cadre d'un procès spécifique. Le constat d'illégalité est dès lors un premier stade pouvant conduire à une accusation délictueuse ou criminelle. Plus loin, ce premier constat d'illégalité pourrait être pris en compte par le tribunal ou la cour, qui, dans un second temps, serait amené à se prononcer sur la responsabilité du propriétaire du contenu, et ne procèderait donc pas à une seconde analyse de la question. Dans tous les cas, le filtrage consiste en une privation du droit de distribuer un contenu spécifique. En conséquence de l'ensemble de ces observations, il serait approprié et conforme à la CEDH d'appliquer à ce constat d'illégalité les garanties attachées au procès pénal.

S'agissant des accusations pénales, la Cour européenne des droits de l'Homme requiert le respect des garanties prévues à l'article 6 de la CEDH, relatif à un procès équitable, et notamment l'existence d'un tribunal indépendant et impartial. Sa conception large de la notion de « matière pénale » conduit la Cour à appliquer également ces principes aux autorités administratives qui seraient chargées par la loi nationale de prononcer certaines sanctions[630]. Dès lors, une personne ayant commis un acte pouvant être qualifié de délictueux ou de criminel doit être jugée par un tribunal indépendant et impartial qui, en Europe, est généralement une juridiction de l'ordre judiciaire. La déclaration de sa responsabilité permettra ainsi au juge de prononcer une sanction appropriée.

---

prestataire de services commerciaux – sont une forme de censure a priori et ne peuvent être justifiés. La distribution des systèmes de filtrage conçus pour les utilisateurs finaux ne devrait être permise que lorsque ces produits fournissent une information claire aux utilisateurs finaux sur la manière dont ils fonctionnent et sur les écueils potentiels liés à leur caractère extrêmement intrusif ».

[629] Voir par exemple la Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, disponible à l'adresse suivante : https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 : « *En coopération avec le secteur privé et la société civile, les Etats membres devraient veiller à ce que les utilisateurs soient informés des filtrages actifs en place et, s'il y a lieu, à ce qu'ils soient capables de les activer et de les désactiver ou d'en modifier le niveau (…)* » ; « *Dans ce contexte, il est souhaitable que la société civile soit encouragée à sensibiliser les utilisateurs aux avantages et aux dangers potentiels des filtres. Cela devrait inclure la promotion de l'importance d'un accès libre et non entravé à l'Internet afin que tous ses utilisateurs exercent et jouissent pleinement de leurs droits de l'homme et de leurs libertés fondamentales, en particulier le droit à la liberté d'expression et d'information, et le droit à la vie privée, ainsi que de leur droit à participer activement à la vie publique et aux processus démocratiques* ».

[630] Certains pays comme la France, transfèrent certains pouvoirs du juge à certaines autorités administratives ad hoc. Un tel transfert de pouvoir doit respecter certaines conditions, en plus de respecter les garanties attachées au procès pénal. Sur cette discussion voir Estelle De Marco, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », 4 juin 2009, Juriscom.net, pages 2 *et s.*, disponible à cette adresse : http://www.juriscom.net/uni/visu.php?ID=1133. Voir également Jean-François Brisson, « Les pouvoirs de sanction des autorités de régulation : les voies d'une juridictionnalisation », AJDA 1999, p. 847.

7.8.2 La proportionnalité de la réponse à une situation ou à un acte illégal, ou encore à une ingérence dans l'exercice de ses droits par autrui

La proportionnalité d'une mesure de filtrage d'Internet est généralement difficile à évaluer, car elle dépend essentiellement du « but légitime » qu'il s'agit de préserver dans le cadre de chaque situation factuelle, de l'utilité de la mesure pour atteindre ce but dans des circonstances particulières, et des caractéristiques du mécanisme de filtrage et de leur impact sur les autres droits et libertés. Par exemple, une mesure spécifique de blocage visant un site web illégal qui ne conduirait qu'à filtrer des contenus illégaux déclarés tels par un juge sans que ne soient parallèlement filtrés de contenus légaux ou un domaine de messagerie électronique, tandis que les ingérences que constitueraient cette mesure seraient compensées par son utilité, pourrait être considérée par un juge comme étant la réponse appropriée à apporter à une situation d'illégalité donnée. Inversement, l'absence de l'un ou de plusieurs de ces éléments pourrait conduire à évaluer la mesure de filtrage comme étant non proportionnée. Puisque le juge est la seule autorité à avoir, à un niveau professionnel, les compétences et les aptitudes nécessaires à l'évaluation de la proportionnalité d'une mesure lorsqu'il s'agit d'établir un équilibre entre les libertés[631], seul le juge devrait être habilité à apprécier la proportionnalité d'une mesure de filtrage en réponse à un crime, un délit ou une contravention.

L'existence d'une disposition imposant le recours au juge est parfois une exigence de la Cour européenne des droits de l'Homme, dans le cadre de son examen de la proportionnalité d'une ingérence. Elle prête en effet « *une attention particulière (...) à l'étendue des pouvoirs par lesquels des restrictions sont imposées aux droits et libertés* ». « *Des objections doivent probablement être soulevées lorsque (ces pouvoirs) ne sont pas l'objet d'un étroit contrôle et qu'il y a, dès lors, plus de place pour de potentiels abus* ». Par exemple, la Cour européenne des droits de l'Homme condamna des pouvoirs d'enquête « *pouvant être exercés sans mandat judiciaire et étant soumis à des limitations qui apparaissaient trop lâches et lacunaires ; la police avait compétence pour apprécier seule l'opportunité, le nombre, la durée et l'ampleur des opérations de recherches et de saisies, et l'ingérence dans le droit du requérant au respect de sa vie privée ne pouvait être vue comme étroitement proportionnée au but légitime de lutte contre l'évasion fiscale* »[632].

En conséquence, puisque le filtrage pourrait limiter de manière significative l'exercice du droit à la liberté d'expression et l'exercice du droit à la vie privée, la Cour européenne des droits de l'Homme pourrait considérer le recours au juge, aux fins de décider de la mise en place et de l'étendue d'une mesure de filtrage, comme une exigence.

S'agissant d'une mesure de filtrage qui ne serait pas dirigée contre un contenu électronique mais contre un internaute, en sanction de l'un de ses actes qui tomberait sous le coup de la loi pénale, une conclusion analogue semble pouvoir être apportée. Une telle mesure serait une sanction très sévère, puisqu'elle aurait pour effet de priver l'internaute de son droit entier de communiquer en ligne et d'exercer sa vie privée dans le monde électronique, alors même que le droit d'accéder à Internet est considéré comme fondamental en démocratie[633]. Dès lors, dans une telle situation également, seul le juge a l'aptitude professionnelle et devrait avoir la légitimité de prononcer une telle sanction, après avoir vérifié qu'elle se trouve proportionnée à l'infraction ainsi réprimée. Le Parlement européen lui-même a déjà eu

---

[631] Voir par exemple Véra Morales, « La protection juridictionnelle des droits fondamentaux : révélation d'une entente conceptuelle », VI° Congrès français de droit constitutionnel, Atelier n°2 : « Le renouveau du droit constitutionnel par les droits fondamentaux », Montpellier, 9, 10 et 11 juin 2005, disponible à l'adresse suivante : http://www.droitconstitutionnel.org/congresmtp/textes2/MORALES.

[632] Traduit de l'anglais. Jeremy McBride, « Proportionality and the European Convention on Human Rights » (« La proportionnalité et la Convention européenne des droits de l'Homme »), in *The principle of Proportionality in the Laws of Europe* (*Le principe de proportionnalité dans les lois d'Europe*), édité par Evelyn Ellis, Hart Publishing, 197 p., 1999, p. 23 et s., citations p. 27.

[633] Voir supra, sous-section 6.6.3.2.

l'occasion de se prononcer en ce sens[634], de même que le Comité des ministres du Conseil de l'Europe[635] et, s'agissant du « *but de protéger les droits des titulaires du droit d'auteur et de droits voisins* », le Conseil constitutionnel français[636].

[634] Voir par exemple « Pas d'accord sur le "Paquet Télécom" », Société de l'information, communiqué de presse, 6 mai 2009, disponible à cette adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20090505IPR55085+0+DOC+XML+V0//FR : « *L'accès à Internet ne peut pas être restreint sans décision préalable des autorités judiciaires, insiste le Parlement en rétablissant l'un de ses amendements de première lecture* ».

[635] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, III, disponible à l'adresse suivante : https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 : « *Sans préjudice de l'importance de la responsabilisation et l'autonomisation des utilisateurs au fonctionnement et au contrôle des filtres, comme expliqué plus haut, et compte tenu de la large valeur de service public revêtue par Internet pour le grand public, les entités publiques de tous les niveaux (telles que les administrations, les bibliothèques ou les établissements d'enseignement publics) qui introduisent des filtres ou les utilisent dans leurs prestations de services devraient veiller au plein respect de la liberté d'expression et d'information, du droit de chacun à la vie privée et au respect de la correspondance de chaque utilisateur* » ; « *Dans ce contexte, les Etats membres devraient (…) : ii. Garantir que les mesures générales de blocage ou de filtrage sur tout le territoire ne sont introduites par l'Etat que si les conditions énoncées à l'article 10, paragraphe 2, de la Convention européenne des Droits de l'Homme sont remplies. De telles mesures étatiques ne devraient être prises que si le filtrage concerne un contenu spécifique et clairement identifiable, une autorité nationale compétente a pris une décision au sujet de l'illégalité de ce contenu et la décision peut être réétudiée par un tribunal ou entité de régulation indépendant et impartial, en accord avec les dispositions de l'article 6 de la Convention européenne des Droits de l'Homme* ».

[636] Voir la décision n° 2009-580 DC du 10 juin 2009, J.O.R.F. du 13 juin 2009, p. 9675, § 16, décision disponible à l'adresse suivante : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html : « *Considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins* ».

7.8.3 Le rôle des prestataires de services Internet

Dans le cadre du Conseil de l'Europe, les ministres responsables des médias et des nouveaux services de communication se prononcèrent eux-aussi en ce sens, s'agissant de l'interruption d'un accès à Internet mais également s'agissant de toute action sur Internet pouvant remettre en question les droits fondamentaux, en déclarant que « *la participation active des fournisseurs de services Internet à l'instauration d'un contrôle du contenu, dans le domaine de l'application des droits d'auteur ou dans d'autres domaines, pose un certain nombre de problèmes en termes de respect de la liberté d'expression et d'accès à l'information. Seul un juge devrait être habilité à trancher en matière de suspension d'abonnements Internet ou à prendre des mesures spécifiques relatives à l'utilisation d'Internet, dans le plein respect des droits et libertés fondamentaux* »[637].

[637] 1ère Conférence du Conseil de l'Europe des Ministres responsables des médias et des nouveaux services de communication, « Une nouvelle conception des médias ? », 21 avril 2009, MCM(2009)021, p.5, disponible à l'adresse suivante : http://www.coe.int/t/dghl/standardsetting/media/doc/MCM(2009)021ENPA_fr.pdf.

7.8.4 Conclusion

En conséquence de nos développements, il semble que les seules mesures de filtrage pouvant être mises en place sans l'obtention d'une décision de justice soient les mesures de filtrage du spam et de filtrage dans un but de protection de la morale.

Ce dernier type de filtrage relève toutefois du choix de chaque pays, même si nous avons vu que le filtrage pour des considérations morales ne semble pas être acceptable dans une démocratie libérale[638].

Le filtrage du spam a un statut particulier, en ce que sa proportionnalité est généralement acceptée et en ce qu'il répond à une demande formulée par les personnes mêmes qui sont impactées par la mesure, en d'autres termes les utilisateurs des services de messagerie électronique.

[638] Voir supra, sous-section 7.4.3.

7.9 Les conditions dans lesquelles le filtrage d'Internet pourrait être acceptable

Les initiatives de filtrage limitent l'exercice de certains droits et libertés. La légitimité du filtrage est en conséquence liée au respect de certaines conditions, à tout le moins dans les démocraties libérales, puisque celles-ci garantissent le respect des droits de l'Homme et des libertés fondamentales.

7.9.1 Les conditions de la limitation des libertés fondamentales

Les démocraties libérales doivent respecter les libertés fondamentales et les conditions de leur limitation que pose la Cour européenne des droits de l'Homme.

Les conditions devant être respectées dans le cadre d'une limitation de libertés sont essentiellement explicitées par la Cour européenne des droits de l'Homme, qui en contrôle par ailleurs le respect. Toutefois, les pays qui n'adhèrent qu'au PIDCP devraient également suivre l'interprétation de cette Cour, au moins dans le cadre d'une limitation du droit à la liberté d'expression, afin de contribuer à l'harmonisation des notions de droit international relatives aux droits de l'Homme.

Ces conditions, que nous avons décrites en détail dans notre chapitre 7, sont reprises ci-dessous sous la forme de différentes étapes, qui peuvent être suivies aux fins de déterminer la légitimité d'une mesure de filtrage dans une démocratie qui respecte les droits de l'Homme et les libertés fondamentales.

7.9.2 La détermination de la légitimité du filtrage dans une démocratie libérale

Etape n°1 Mettre en œuvre le filtrage de manière à ne pas entraîner une violation d'autres droits et libertés

La mesure de filtrage doit être mise en œuvre pour préserver un ou plusieurs intérêts légitimes particuliers, de manière à répondre à un besoin social impérieux avec proportionnalité, sur le fondement d'une loi tenant compte des autres dispositions de droit international que l'Etat en question s'est engagé à respecter.

Etape n°2 Identifier les droits et libertés qui se trouveront limités

Une mesure de filtrage d'Internet constituera toujours une ingérence dans le droit à la liberté d'expression, puisqu'elle a vocation à réduire l'accessibilité de certains contenus ou la capacité à se connecter de certains individus[639], et peut également constituer une ingérence dans le droit au respect de la vie privée[640]. La mesure peut encore limiter, de manière plus sévère qu'à l'égard des autres personnes, certaines libertés que

Etape n°3 – Exemple :
Déterminer l'ampleur de la limitation

Dans le cadre d'une mesure de filtrage qui aurait pour but de prévenir les accès à un type particulier de contenus illégaux, comme ceux de pédopornographie, il s'agirait de déterminer la mesure dans laquelle des contenus légaux ou des domaines de messagerie électronique pourraient également être bloqués, cette dernière situation pouvant conduire à limiter le droit à la protection de la liberté et du secret de la vie privée, de la vie familiale et des correspondances[640]. Il apparaît dès lors que les effets de bord de la mesure peuvent varier selon les caractéristiques des serveurs ou des domaines qui hébergent les contenus à filtrer.

Devraient encore être évalués le coût de la mesure et son impact sur la qualité, la stabilité et le calendrier de développement du réseau sur lequel il est prévu de l'implémenter. La mesure pourrait en effet avoir un impact sur le droit à la vie privée et le droit à la liberté d'expression, impact qu'il conviendrait de déterminer, si elle entraînait par exemple un coût plus élevé de l'accès à Internet, une moindre qualité du réseau pour aujourd'hui ou pour demain, ou une moindre possibilité de choix entre les prestataires et les services Internet, en raison de la disparition de certains d'entre eux.

[639] Voir supra, sous-section 6.6.2.2.
[640] Voir supra, sous-section 6.6.1.

les personnes handicapées ne peuvent exercer que par l'intermédiaire de leur accès aux technologies et aux services Internet[641]. Il est dès lors nécessaire de déterminer précisément les droits dans l'exercice desquels la mesure de filtrage projetée constituera une ingérence.

Etape n° 3 Déterminer l'ampleur de l'ingérence

L'ampleur d'une ingérence doit être déterminée en tenant compte des éléments ci-dessous :

- Les caractéristiques, inhérentes à la mesure, qui pourraient conduire à la limitation de certaines libertés ;
- Les caractéristiques, inhérentes à la mesure, qui pourraient permettre d'implémenter d'autres fonctionnalités pouvant elles aussi conduire à la limitation de libertés, même si le but poursuivi par la mesure n'inclut pas l'implémentation et l'utilisation de ces dernières fonctionnalités ;
- Les caractéristiques et fonctionnalités qui sont attendues de la mesure de filtrage afin d'atteindre un objectif particulier.

Etape n°3 – Exemple :
Impact des autres fonctionnalités - preuve de responsabilité

L'impact des autres fonctionnalités qu'un Etat ou un acteur souhaiterait ajouter à la mesure de filtrage doit également être apprécié. La conservation généralisée des adresses IP des utilisateurs tentant d'accéder aux sites web bloqués constituerait par exemple une limitation sévère du droit à la protection des données personnelles, limitation qui pourrait au demeurant ne pas être admise[642], excepté dans le cadre d'une investigation prévue par la loi, éventuellement placée sous le contrôle du juge[643]. Une telle conservation serait d'autant plus dangereuse qu'une adresse IP ne permet pas d'identifier la personne qui a utilisé un accès à Internet donné pour consulter un site web[644], alors même que certains pays commencent à faire tomber sous le coup de la loi pénale l'accès régulier à de la pédopornographie en ligne[645]. La conservation de telles données et la possibilité de les transmettre aux autorités pourrait conduire à des investigations injustifiées, qui pourraient priver une personne de ses libertés pour quelques jours, conduire à la saisie de son matériel informatique[646] et porter atteinte à son honneur et à sa réputation à l'occasion de son arrestation sous le regard de ses voisins, l'ensemble sans aucune preuve sérieuse de responsabilité[647].

[641] Voir supra, sous-section 6.6.3.
[642] Voir supra, sous-section 6.6.1.3.
[643] Voir supra, sous-section 7.8.2.
[644] Voir supra, sous-section 6.6.1.3.
[645] Voir par exemple l'article 227-23 du Code pénal français. De telles dispositions, considérées comme utiles aux investigateurs qui ressentent le besoin de disposer de plus d'outils juridiques dans le cadre de leur lutte contre la pédopornographie en ligne, semblent toutefois s'aventurer dangereusement au delà des principes généraux du droit pénal dans une démocratie, lesquels impliquent qu'une action ne peut être sanctionnée que lorsqu'elle est commise volontairement, et que la loi pénale n'incrimine que des actions ou omissions caractérisées heurtant les valeurs principales de la société. Généralement, voir un crime n'est donc pas une infraction, tandis que ne pas aider à stopper la commission de ce crime ou à en limiter les effets, lorsque cela s'avère possible, peut en être un.
[646] Sans garantie aucune de récupérer ce matériel, même en cas d'innocence.
[647] Parallèlement à l'impossibilité qu'il y a à déduire, d'une adresse IP, la responsabilité d'un individu pour une action commise sur Internet, un expert informatique semble avoir la possibilité de faire croire qu'une adresse IP est à l'origine d'une action, sans que cette adresse ne l'ait été en pratique. Voir par exemple Michael Piatek, Tadayoshi Kohno, Arvind Krishnamurthy, « Challenges and Directions for Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown Notice » (« Défis et instructions pour la surveillance des réseaux de partage de fichiers P2P – ou – pourquoi mon imprimante reçut une demande de retrait fondée sur le DMCA »), technical report (rapport technique), University of Washington Department of Computer Science and Engineering (Département de science informatique et d'ingénierie de l'Université de Washington), http://dmca.cs.washington.edu/dmca_hotsec08.pdf, p. 3 (index du site : http://dmca.cs.washington.edu/).

Etape n° 4 Identifier précisément le ou les buts poursuivis

Une mesure de filtrage qui constitue une ingérence dans l'exercice de certaines libertés conditionnelles doit poursuivre l'un des buts légitimes énumérés restrictivement par la Convention européenne des droits de l'Homme ou le PIDCP, au sein de l'article qui garantit la liberté concernée. Plus de détails sont disponibles en notre section 7.4.

Une mesure de filtrage poursuit généralement un ou plusieurs des buts suivants :

- La protection des droits d'autrui ;
- La protection de la morale ;
- La protection de la santé ;
- La prévention des infractions ;
- La répression des infractions.

L'identification précise du ou des buts poursuivis est extrêmement importante, car le respect des autres conditions de la légitimité d'une mesure de filtrage devra être contrôlé à sa ou leur lumière.

Etape n° 5 S'assurer que le but assigné à la mesure de filtrage corresponde à une réalité

Les buts énumérés ci-dessus sont tous des buts légitimes à la lumière des textes internationaux qui garantissent les libertés. Toutefois, reste la question de la possibilité effective, pour une mesure de filtrage d'Internet, de poursuivre le but qui lui a été assigné.

Etape n° 6 Déterminer si la mise en place d'une mesure de filtrage dans le but qui lui a été assigné répond à un besoin social impérieux

Dès lors que le but poursuivi par une mesure de filtrage est identifié, une autre question est celle de savoir s'il existe un besoin social impérieux d'atteindre ce but par la mise en œuvre d'une mesure de filtrage qui provoquera les ingérences que nous avons analysées dans notre section 7.6. Une réponse positive implique que la mesure de filtrage soit capable de répondre à ce besoin de manière adéquate.

- Le filtrage répond-il à un besoin social impérieux lorsqu'il a pour but de prévenir le crime ?
- Le filtrage répond-il à un besoin social impérieux lorsqu'il a pour but de protéger la morale ou la santé des personnes sensibles (enfants inclus) ?
- Le filtrage répond-il à un besoin social impérieux lorsqu'il a pour but de protéger les droits d'autrui ?

Etape n° 7 Apprécier la proportionnalité de l'ingérence au but poursuivi

L'ingérence dans les libertés que constitue une mesure de filtrage d'Internet doit être proportionnée au but poursuivi.

- L'effet général d'une restriction donnée doit être notamment évalué au regard des limitations apportées par la mesure aux autres libertés et au regard de l'efficacité de la mesure pour atteindre le but qu'elle poursuit.
- Une mesure qui présente un faible degré d'efficacité ne peut pas conduire à limiter, dans une proportion plus grande, les libertés avec lesquelles elle se trouve en interférence.
- Il doit exister des raisons suffisantes de croire que l'intérêt qui se trouve protégé par la mesure de filtrage d'Internet est en péril.
- La proportionnalité du comportement précis qui se trouve limité dans son exercice doit également être évaluée. En d'autres termes, une limitation

sera plus ou moins acceptable selon la légitimité des personnes à entretenir un tel comportement, à la lumière de l'intérêt qui se trouve en péril.

- Il est nécessaire de choisir la manière la moins restrictive de droits, parmi celles qui sont à même d'atteindre de manière satisfaisante le but poursuivi.

Etape n° 8 Tenir compte du principe qui doit gouverner le filtrage, déduit de la lecture des critères de légitimité posés par la Cour européenne des droits de l'Homme

S'agissant du filtrage d'Internet, les critères posés par la Cour permettent de dire que « l'utilité » de la mesure, pour atteindre un but particulier, doit être d'ampleur équivalente ou supérieure à celle de la limitation apportée à d'autres libertés.

- L' « utilité » de la mesure doit en premier lieu être évaluée au regard du degré de péril souffert par l'intérêt à préserver, et de l'importance qu'il y a à apporter une réponse à ce péril. L'utilité de la mesure doit en second lieu être évaluée au regard du niveau d'efficacité de cette dernière pour prévenir l'intérêt en cause de ce péril particulier, une telle prévention ayant été préalablement reconnue comme étant un besoin social impérieux.
- L'ampleur de la limitation apportée aux libertés doit être évaluée à la lumière de l'importance des libertés qui se trouveront limitées, et à la lumière de la proportionnalité du comportement précis qui se trouvera limité, compte tenu des limites que ce comportement apporte lui-même à l'intérêt qui doit être protégé par le filtrage. Cette ampleur doit encore être évaluée en tenant compte des limitations qui ne sont pas nécessaires au but poursuivi mais qui pourraient néanmoins être apportées aux libertés parce qu'elles sont rendues possibles par la technologie utilisée pour mettre en place le filtrage.

Etape n° 8 – Exemple :

Une mesure de filtrage ne peut pas être mise en place sans une loi qui en assure la proportionnalité en prévoyant des dispositions de nature à prévenir l'utilisation de certaines fonctionnalités du mécanisme ou à en corriger certains effets, lorsqu'ils peuvent l'être.

Par exemple, l'un des effets négatifs d'une mesure de filtrage des contenus à caractère pédopornographique sur les droits des citoyens serait la limitation du droit de ces derniers à être informés de l'existence et du volume de cette catégorie d'infractions sur Internet.

Une mesure corrective possible serait une information régulière des citoyens sur le volume des contenus de cette nature qui sont toujours en ligne, sur les moyens alloués aux enquêteurs et sur le taux de réussite que rencontrent les investigations.

Ces principes doivent être pris en compte en conjonction avec les critères suivants :

- Une limitation ne peut être apportée à une liberté qu'aux fins de protéger l'intérêt particulier qui se trouve en péril et qui justifie une mesure de filtrage.
- La limitation apportée à une liberté ne peut pas aller jusqu'à « provoquer (l')extinction » de cette dernière ; elle doit « ménager un certain périmètre » à son exercice, même lorsque l'« utilité » de la mesure de filtrage est évaluée comme étant très élevée.
- La limitation apportée aux libertés doit être la plus faible possible, afin d'atteindre le but recherché de manière satisfaisante, et ne peut jamais être plus importante que ne l'est l'« utilité » de la mesure.

Etape n° 9 Déterminer si une loi est nécessaire aux fins de prévenir l'utilisation de certaines fonctionnalités du mécanisme de filtrage

Une telle loi devra également être adoptée, dans la plupart des cas, en vue de prévoir l'intervention du juge dans le dispositif de filtrage. Nous avons en effet vu qu'un juge était nécessaire dans au moins deux situations :

- La décision de filtrer un contenu particulier peut être vue comme une déclaration d'illégalité, laquelle peut constituer la première étape d'un processus pouvant aboutir à une accusation pénale, et laquelle pourrait être utilisée dans le cadre d'un procès ultérieur pour établir partiellement la responsabilité du propriétaire du contenu en cause. La décision de filtrer un contenu peut également être vue comme une décision de priver une personne du droit de distribuer ce contenu, décision dont la possibilité doit être prévue par la loi, et, dans les démocraties libérales, qui doit être prise par le juge.
- La proportionnalité de la mesure devra être évaluée dans chaque cas particulier. Le filtrage d'un contenu particulier, qui se trouve sur un serveur particulier, par une mesure particulière, peut provoquer ou non des limitations étendues de libertés. Bloquer une personne en réponse à la commission d'une infraction est également une sanction très sévère, dont l'opportunité doit être appréciée par un juge.

Etape n° 10 Prévoir la mesure de filtrage au sein d'une loi

Une mesure de filtrage qui répondrait à l'ensemble des critères exigés doit être prévue par la loi. La définition de loi inclut ici « *le droit non écrit* », « *les textes de rang infralégislatif* » et parfois la jurisprudence[648]. Quelle que soit sa nature, cette loi doit être « *suffisamment accessible* », ce qui signifie que « *le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné* », et doit être « *énoncée avec assez de précision pour permettre au citoyen de régler sa conduite* »[649].

Une loi est nécessaire

Une loi est nécessaire pour deux raisons principales.

La première de ces raisons est l'exigence de la clause d'ordre public prévue par la Convention européenne des droits de l'Homme. La Cour éponyme commence son analyse de toute ingérence dans une liberté conditionnelle[1] en vérifiant si l'ingérence était « *prévue par la loi* »[2].

La seconde de ces raisons est la nécessité, pour un pays qui prévoit d'implémenter le filtrage :

- De s'assurer que la mesure de filtrage n'entrera pas en contradiction avec d'autres droits et obligations prévus par certaines dispositions internationales que ce pays a pris l'engagement de respecter ;
- De combiner ces droits et obligations avec les effets de la mesure de filtrage qui pourraient leur être contradictoires.

(1) Voir supra, section 7.2.
(2) Voir supra, section 7.3.

[648] Arrêt *Kruslin c/ France* de la Cour européenne des droits de l'Homme, arrêt du 24 avril 1990, séries A, n° 176 A, p. 20, § 29. Voir supra, notre section 7.3.
[649] Toutes les citations sont extraites de l'arrêt de la Cour européenne des droits de l'Homme *Sunday Times c/ Royaume-Uni*, précité, § 49.

7.10 Les études requises

Au cours de notre analyse de la manière d'équilibrer les libertés fondamentales, plusieurs études ont été identifiées comme nécessaires, pour permettre une évaluation adéquate de certaines mesures de filtrage au regard des critères posés par la Cour européenne des droits de l'Homme. Diligenter ces études n'écarte toutefois pas la nécessité d'évaluer la mesure de filtrage dans ses autres éléments. Cette liste d'études n'est en outre pas exhaustive, en ce que chaque mesure particulière doit être évaluée dans son propre contexte. Dès lors, d'autres études pourraient s'avérer nécessaires. Les études proposées portent sur les mesures suivantes :

7.10.1 Le filtrage d'Internet visant à prévenir la pédophilie

Afin de s'assurer de la réalité d'un tel but, assigné à une mesure de filtrage, il serait nécessaire de diligenter une étude relative à la prévention de la pédophilie, qui aurait pour objectif de démontrer que certaines personnes peuvent devenir des criminels après avoir accédé à certains contenus. Elle expliquerait le processus de « passage à l'acte » et mettrait en lumière le pourcentage que représente la population concernée. Afin de déterminer l'utilité de la mesure et sa réponse à un besoin social impérieux, une telle étude démontrerait encore que le filtrage empêche effectivement les personnes concernées d'accéder à des images illégales, tandis que leur accès à ces images est effectivement le facteur déterminant qui les pousse à commettre un acte illégal.

Cette dernière étude pourrait, dans ce cadre, identifier les différents protocoles Internet utilisés par la population à préserver d'un passage à l'acte pour accéder à des contenus à caractère pédopornographique, ainsi que le comportement prévisible qu'auraient, en cas de blocage, les individus qui composent cette population, afin de savoir par exemple s'ils renonceraient ou, inversement, s'ils trouveraient la manière d'accéder à ces contenus d'une autre façon. Cette étude pourrait également évaluer le risque de passage à l'acte chez les éventuelles personnes qui n'accéderaient plus du tout aux contenus illégaux, si un tel effet apparaissait comme pouvant être obtenu.

7.10.2 Le filtrage d'Internet visant à entraver le modèle économique du commerce de la pédopornographie

Afin de s'assurer de l'utilité d'une mesure visant un tel objectif, et donc de s'assurer que cette mesure répond à un besoin social impérieux, une étude relative à la manière d'entraver le modèle économique du commerce de la pédopornographie devrait par exemple mettre en lumière le pourcentage que représentent les activités commerciales ayant lieu par l'intermédiaire des sites web qui sont ou pourraient être bloqués. Cette étude pourrait analyser les différents moyens qui permettent d'accéder à ces sites web et l'impact qu'auraient ces moyens sur une mesure de filtrage, en termes, par exemple, de contournement de la mesure. Elle devrait étudier les autres protocoles de communication utilisés pour vendre les contenus litigieux, ainsi que le taux potentiel de transfert de ces contenus comme de leurs clients entre le web et ces autres protocoles, en cas de mise en place d'une mesure de filtrage.

7.10.3 Le filtrage d'Internet visant à réduire les échanges de pédopornographie

Afin de s'assurer qu'une mesure de filtrage visant un tel objectif répond effectivement à un besoin social impérieux, une étude relative à l'utilité du filtrage pour réduire les échanges de ressources à caractère pédopornographique devrait par exemple examiner la proportion des ressources de cette nature qui sont accessibles via le protocole dont le filtrage est planifié, au regard de la proportion approximative des contenus de même nature qui se voient distribués par les délinquants via d'autres protocoles. Cette étude devrait encore analyser l'impact qu'aurait l'opération projetée sur le comportement des personnes qui distribuent des contenus à caractère pédopornographique ou qui y accèdent via le protocole filtré, afin de prendre la

mesure du taux potentiel de transfert de ces contenus et de leurs amateurs entre ce dernier protocole et les autres.

7.10.4 Le filtrage d'Internet visant à protéger les personnes sensibles ou la morale

Aux fins de savoir si une mesure de filtrage visant de tels objectifs serait en mesure de répondre à un besoin social impérieux, deux types d'études sont nécessaires :

Une étude sur l'efficacité du filtrage pour protéger les personnes sensibles des contenus qui pourraient leur porter préjudice ou pour protéger tout un chacun des contenus qui se voient opposés à la notion de morale (gardant à l'esprit qu'empêcher les personnes d'accéder à certains contenus déterminés pour des considérations morales pourrait ne pas correspondre à la conception démocratique de la liberté d'accès à l'information, à tout le moins dans les démocraties libérales). La question principale est de déterminer le volume de la population à protéger, en d'autres termes le pourcentage de la population qui accède accidentellement aux contenus choquants ou immoraux qui se trouvent visés, ainsi que l'efficacité de la mesure à assurer la protection de ces personnes. Déterminer le volume de la population qu'il s'agit de protéger implique en premier lieu de connaître le pourcentage des tentatives d'accès aux contenus litigieux dont sont à l'origine des robots ou d'autres machines présentes sur le réseau. Il est également nécessaire de déterminer les caractéristiques de cette population, et l'impact de la mesure de filtrage sur les sites web bloqués (pour savoir si certains d'entre eux réapparaissent, dans quelle mesure et sous quel délai général, et si les nouveaux sites web présentent les mêmes caractéristiques d'accessibilité que les premiers).

Une étude permettant de déterminer si la mesure de filtrage pourrait être considérée comme répondant réellement à un **besoin social impérieux** de protéger la santé ou la morale, alors qu'elle ne filtrerait que *certains* types de contenus choquants ou immoraux, mais non *l'ensemble* des contenus choquants ou immoraux disponibles. Il semble que, dans une telle situation, la mesure pourrait être considérée comme inappropriée pour atteindre ses objectifs.

Une analyse du pourcentage que représente chaque type de contenus choquants facilement accessibles sur Internet serait la bienvenue sur cette question. Cette analyse pourrait mettre l'accent sur les principales catégories identifiées de contenus choquants (pédopornographie, meurtres, viols, autres types de violences ou de tortures), mais également s'attacher à l'étude de chacun des contenus pouvant heurter une population spécifique, en s'appuyant par exemple sur les règles généralement mises en place par les utilisateurs de filtres sur postes clients.

7.10.5 Le filtrage d'Internet visant à protéger les intérêts des victimes

Pour s'assurer de la **réalité d'un tel but assigné au filtrage**, il est nécessaire de conduire une étude sur les intérêts des victimes. Cette étude démontrerait que la protection de ces intérêts implique que, parmi les catégories d'individus susceptibles d'accéder aux images des victimes dans le cadre d'une scène de crime, l'une de de ces catégories ou chacune de ces catégories en soient empêchées.

Cette étude pourrait également évaluer la capacité du filtrage à répondre de manière appropriée à un **besoin social impérieux**. Elle pourrait par exemple identifier le pourcentage de délinquants qui ne contourneraient pas la mesure, ainsi que le pourcentage de personnes qui ne souhaitent pas accéder à de telles images mais qui y accéderaient malgré tout, soit que le contenu ait réapparu à une autre adresse, soit que le contenu n'ait pas été inscrit sur la liste des sites à bloquer, soit que ces personnes contournent généralement les mesures de filtrage, non pour accéder à des images illégales, mais simplement pour ne pas être bloquées à l'occasion de leur surf.

7.10.6 Le filtrage d'Internet visant à protéger les droits de propriété intellectuelle

S'agissant de la protection des droits de propriété intellectuelle, l'existence d'un besoin social pourrait être déterminée par une étude de la réalité de la menace qu'Internet représente pour les titulaires de droits, étude qui pourrait notamment inclure une analyse du modèle économique des industries de la musique et du film sur Internet, spécialement en ce qui concerne le manque de disponibilité en ligne de contenus légaux et le faible niveau de rémunération des artistes. Cette étude pourrait encore inclure une analyse de la perception de ce modèle économique par le grand public et par les artistes, et une analyse de la possible évolution de ce modèle. Si une telle étude conduisait à montrer que la protection des droits de propriété intellectuelle par une mesure de filtrage constitue un besoin social impérieux, une autre étude devrait examiner l'efficacité du filtrage des violations en ligne de droits de propriété intellectuelle. Une telle étude pourrait notamment inclure une analyse du comportement prévisible des internautes qui rencontreraient la mesure de filtrage, cette dernière pouvant les conduire soit à chiffrer leurs échanges, soit à échanger leurs fichiers par la voie d'autres protocoles, soit à échanger leurs fichiers via le protocole sur lequel est mise en œuvre la mesure de filtrage, mais à d'autres adresses ou par d'autres moyens. Cette étude pourrait, plus loin, inclure une analyse des conséquences de tels comportements sur l'efficacité de la mesure.

Chapitre 8 CONCLUSION

Le présent rapport a couvert quatre sujets importants relatifs au filtrage d'Internet.

Le chapitre 3 s'est intéressé à la signification de la notion de filtrage d'Internet et en a examiné différentes appréhensions.

Le chapitre 4 s'est attaché aux raisons pour lesquelles la société croit que les tentatives de filtrage pourraient résoudre certaines problématiques sociétales majeures, et aux raisons pour lesquelles d'autres approches n'apparaissent pas être très efficaces. Il s'est intéressé à la qualité des personnes ou entités qui mettent en œuvre le filtrage, à ce qui peut être filtré, à la manière dont la question du filtrage peut être approchée et aux personnes visées par les initiatives de filtrage d'Internet. Il a également proposé une liste de pays qui ont déjà adopté des systèmes de filtrage d'Internet. La conclusion de ce chapitre est que certains pays connaissent d'importantes frustrations tenant au manque d'efficacité de la coopération internationale actuelle en matière de cybercriminalité et au manque de réponses, de la part de certains pays, à des problématiques juridiques significatives que sont par exemple la pédopornographie, les discours de haine ou le terrorisme.

Le chapitre 5 a dressé le panorama, sous une approche technique, des principaux systèmes de filtrage d'Internet qui sont aujourd'hui utilisés. Il a montré la manière dont ces systèmes sont appliqués à différents services Internet, et engagé une discussion sur l'impact de ces systèmes et sur les défis techniques que ces derniers posent. Il a inclu une présentation des méthodes utilisées pour contourner ces systèmes de filtrage et une analyse de l'efficacité de ces systèmes. La conclusion de ce chapitre est que la mise en œuvre d'un système de filtrage d'Internet implique des ressources substantielles en termes humain et financier. Etonnamment, l'un des systèmes les plus simples à contourner est celui qui recourt au filtrage DNS et qui est pourtant aujourd'hui mis en œuvre dans de nombreux pays au niveau national. Quasiment tous les systèmes ont un impact technique au regard de la résilience d'Internet, et ajoutent une couche supplémentaire de complexité au sein d'un réseau déjà complexe. Tous les systèmes peuvent être contournés, avec un niveau de connaissances techniques parfois faible, parfois un peu plus poussé. Malgré cela, des solutions logicielles proposant une assistance au contournement des mesures de filtrage d'Internet sont disponibles sur le réseau de manière croissante.

Le chapitre 6 a proposé un panorama détaillé de la question du filtrage d'Internet face à la loi et a passé minutieusement en revue les instruments juridiques qui peuvent avoir une incidence sur un système de filtrage. Le rôle crucial que jouent les démocraties libérales modernes, de par leur respect actif des libertés fondamentales et des libertés publiques, y a été clairement identifié. Cette étude a inclu une analyse des instruments nationaux et internationaux, et s'est attachée à identifier les droits fondamentaux qui se trouvent en opposition avec le filtrage d'Internet, d'une part, et les droits fondamentaux qui sont de nature à soutenir le filtrage d'Internet, d'autre part. Elle a également abordé la question du rôle des prestataires de services Internet et celle des circonstances déroutantes dans lesquelles ces derniers opèrent parfois, en raison d'exigences légales concurrentes, voire contradictoires. Ce chapitre a encore accueilli une discussion relative à la complexité de ces instruments et à la manière dont ils s'appliquent aux services Internet et aux initiatives de filtrage d'Internet.

Le chapitre 7 a développé la question de la mise en équilibre des libertés fondamentales lorsque différents droits sont en opposition, et, au terme d'une analyse détaillée de la méthode retenue par la Cour européenne des droits de l'Homme pour analyser les affaires qui lui sont soumises, a proposé des lignes directrices permettant de guider la mise en place de mesures de filtrage d'Internet. Cette méthode inclut l'application aux cas d'espèce de la stricte « clause d'ordre public », dont l'un des éléments est le principe de nécessité dans une société démocratique. Ces lignes directrices ont alors été appliquées à différentes initiatives de filtrage, notamment différenciées selon leurs objectifs, afin d'analyser la manière dont ces mesures pourraient être jugées par la Cour européenne des droits de l'Homme. Ce chapitre a proposé, dans ce cadre, un examen de la légitimité du but de ces mesures de filtrage, et interrogé la validité de certains systèmes. Il a mis en évidence, en conclusion, une série d'étapes pouvant être suivies aux fins d'évaluer la légitimité, dans une société démocratique, de toute mesure de filtrage d'Internet.