Filtrage d'internet et démocratie - Résumé principal

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

http://www.aconite.com/blocking/study

Traduction « Framalang » et « La Quadrature du Net ».

22 Octobre 2009
(traduction 15 Décembre 2009)

Table des matières

0.1 Introduction

Ce rapport explique ce qu'est le filtrage d'Internet, quelles sont les motivations poussant à ce ce filtrage dans la société, quelles sont les options techniques disponibles et quelles sont les questions légales qui affectent les stratégies de fitrage d'Internet.

Note : Les citations se trouvant dans ce sommaire principal ne sont pas directement attribuées à l'auteur. Ces citations sont clairement présentées entre guillemets et peuvent être retrouvées dans le texte principal de l'étude, avec la référence détaillée de l'auteur et de la source. Aucune reproduction de ces citations n'est autorisée depuis ce document sans l'accord de l'auteur de cette citation ET la mention de la page et du chapitre de la citation dans cette étude, où le nom de l'auteur original est indiqué.

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

Cette étude présente une analyse complète de l'état du filtrage d'Internet, un inventaire des régulations et cadres juridiques en relation avec le filtrage d'Internet et un commentaire sur l'efficacité de ce filtrage et de son impact sur la lutte contre le cybercrime et sur le maintien de la démocratie et de la sécurité des individus.

Trouver l'équilibre le plus approprié entre protection de l'enfance et libertés démocratiques est une question très complexe, qui nécessite en définitive une réponse au niveau national, par d'importants débats entre les différentes parties prenantes dans chaque pays et en prenant en considération les engagements internationaux tels que la Convention européenne des droits de l'Homme.

Selon les membres du Parlement européen (euro-députés), un accès sans entraves à Internet, sans aucune interférence, est un droit d'une importance considérable. 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 il est protégé par le droit à la liberté d'expression, quand bien même il n'est pas encore lui-même, considéré comme un droit fondamental[1].

Ces dernières années, certains états démocratiques ont promu l'usage de techniques de filtrage d'Internet ciblant différents types de contenu. Ils ont invoqué l'intérêt général pour exiger la mise en œuvre de filtrages spécifiques, dans le but de faire respecter divers points de politiques publiques pour lesquels les caractéristiques d'Internet engendraient des difficultés à faire appliquer le droit (notamment au niveau international). Ces points spécifiques vont de la disponibilité de reliques nazies sur des sites de ventes en ligne, à des sites de jeux d'argent hébergés dans des états aux législations plus laxistes sur les casinos en ligne. De même, des états aux régimes moins ouverts sur l'information se sont mis au filtrage, en tant que ressource technique pour étendre leur pratique du contrôle de l'information au monde des réseaux.

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

Le filtrage d'Internet (parfois nommé blocage d'Internet) n'est pas une activité récente. Voilà des années qu'il est utilisé. Cependant, ce terme recouvre une gamme si large de pratiques, de matériels, de logiciels et de services qu'il serait erroné de penser que tous les types de filtrage d'Internet se ressemblent ou sont aussi efficaces ou équivalents devant la loi ; ou même, qu'un système de filtrage puisse être utilisé aisément contre plus d'un type de contenu.

L'objectif premier du filtrage d'Internet est d'empêcher le contenu d'atteindre un ordinateur personnel ou un moniteur informatique en utilisant un produit logiciel ou materiel qui scrute toutes les communications Internet et détermine s'il doit empêcher la réception et/ou l'affichage du contenu spécifiquement ciblé.

[1] Parlement Européen, résolution 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 la section 6.3.2.2.

Par exemple, un courriel peut être filtré parce qu'il est suspecté d'être un pourriel, un site web peut être filtré parce qu'il est suspecté de contenir un logiciel malveillant ou une session de pair-à-pair peut être interrompue parce qu'elle est suspectée de véhiculer de la pédopornographie.

Le terme anglais Internet Blocking , littéralement blocage d'Internet , est lui-même quelque peu inapproprié puisqu'il suggère que c'est un mécanisme facile à mettre en œuvre et qu'il s'agit juste de décider si on ouvre ou ferme un interrupteur. C'est on ne peut plus éloigné de la réalité puisque les capacités des techniques de filtrage sont plutôt complexes et peuvent souvent être facilement contournées. Il y a plusieurs raisons à cela, la plus fondamentale étant qu'Internet a été conu pour être décentralisé, avec une capacité intrinsèque à s'assurer que les données puissent circuler en contournant tout obstacle qu'on pourrait poser sur leur route[2]

Essayer de filtrer les contenus d'Internet qui sont mis à disposition légalement hors d'un pays alors qu'à l'intérieur de celui-ci ces contenus sont considérés comme illégaux, voilà qui peut être un choix possible pour les pays qui voudraient conserver leurs critères de culture nationale à une époque d'accès global.

On peut dire que le filtrage d'Internet commena il y a vingt ans, avec le filtrage des courriels non sollicités (pourriels, spam). Cela commena pour plusieurs raisons, mais ce fut initialement pour éviter la saturation des réseaux. Cela a représenté un sujet constant de recherche et développement et une concurrence continuelle entre les initiatives anti-pourriels et l'activité des arroseurs. Malgré ces initiatives approfondies durant une longue période de temps, tous les utilisateurs de messagerie électronique savent aujourd'hui que le blocage des pourriels n'est pas un problème complètement résolu, puisqu'il n'a pas été éradiqué d'Internet.

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] et que, dans les systèmes avancés, ceux-ci sont minimisés lors de la conception des techniques de filtrage en service.

Cependant, ces problèmes peuvent devenir plus prononcés et avoir des conséquences plus importantes lorsque les systèmes de filtrage sont appliqués à l'Internet public et imposés à tous les utilisateurs d'Internet dans une région. Ils constituent donc un enjeu important pour la société dans son ensemble. Étant donné que ces systèmes sont souvent mis en œuvre avec un contrôle public ou des débats minimums et souvent insuffisants et qu'ils sont appliqués sans l'accord expresse des utilisateurs de ces services Internet, ils doivent être conus, développés, gérés, mis en œuvre et vérifiés d'une manière bien plus transparente et responsable.

Il existe différents types de filtrages d'Internet. Le filtrage personnel et le filtrage en réseau sont les deux principaux types d'usage courant. Il existe aussi des systèmes qui combinent les deux faons de procéder.

Le filtrage mis en œuvre par l'utilisateur final permet de décider du type de contenu à filtrer en fonction de critères propres à chaque utilisateur d'un ordinateur. Ce filtrage personnel sur mesure peut être configuré au plus juste suivant les catégories d'utilisateurs (parents, enfants, enseignants, étudiants, etc.). Ce type de filtrage est le plus granulaire mais ne permet pas d'empêcher les utilisateurs d'accéder à des contenus illégaux qu'ils auraient pourtant choisi de parcourir et télécharger.

Dans le système de filtrage d'Internet basé sur le réseau, le fournisseur de services (fournisseur d'accès Internet, employeur, association, etc.) peut déterminer quel type de contenu ou d'activité sera filtré pour TOUS les utilisateurs du service, du moins pour les contenus qui sont accessibles directement via les serveurs réseaux sur lesquels le fournisseur a mis en œuvre le filtrage (parfois le système peut être adapté sur mesure, pour décider des critères de filtrage en fonction des utilisateurs identifiés)

Il existe deux points clés à discuter à propos du filtrage d'Internet :

[2]La gamme complexe des problèmes technologiques est résumée au chapitre 5.

[3]Un faux-négatif survient lorsqu'un courriel est autorisé à passer outre le filtre de pourriel, il est considéré comme ne contenant aucun spam, alors qu'il est pourtant porteur. D'où l'expression faux-négatif.

[4]Un faux-positif survient lorsqu'un élément qui ne devrait pas être bloqué par le filtre l'est cependant, car le filtre renvoie un résultat positif. Ce dernier est incorrect, d'où l'appellation faux-positif.

Comment pouvons-nous préciser techniquement ce qu'il faut filtrer ?

Pour collecter les contenus, les passer en revue, les évaluer, les classer, identifier ceux qui doivent être bloqués, les processus utilisés sont complexes et gourmands en ressources. Ils doivent être développés, testés et mis en œuvre, il faut identifier et former le personnel compétent.

- Les listes noires constituent la stratégie de filtrage la plus courante
- L'identification automatique est à l'étude mais ses résultats sont limités
- Les systèmes d'évaluation sont disponibles depuis des années mais n'ont pas eu le succès escompté

Qui devrait choisir ce qu'il faut bloquer 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 démocracies libérales, seul un juge devrait avoir la compétence de déclarer illégal un contenu, une situation ou une action. Ce point crée un des défis majeurs pour les systèmes de filtrage d'Internet.
- Les procédures juridiques nationales et internationales actuelles sont rarement appropriées aux développements sans frontières d'Internet ou à la vitesse des communications des services Internet. Il en résulte que les autorités judiciaires participent rarement de faqn suffisante aux décisions de filtrage d'Internet.

L'association International Network of Internet Hotlines (réseau international des services d'assistance téléphonique Internet) coordonne un réseau de services d'assistance téléphonique dans plus de trente pays qui traitent des signalements de pédopornographie sur Internet. Les services d'assistance téléphonique ont reu plus de 500 000 rapports en 2005, 850 000 en 2006, plus d'un million en 2007 et leur nombre ne cesse de s'accroître chaque année. Les chiffres exacts pour 2008 n'ont pas encore été publiés. Sur le total des rapports reus entre septembre 2004 et décembre 2006, moins de 20% des cas ont été considérés comme illégaux OU dangereux et seulement 10% ont été considérés comme illégaux par les services d'assistance téléphonique.

Un problème crucial autour des listes noires et celui de leur sécurité et leur intégrité. Une liste de contenus tels que ceux-là est extrêmement recherchée par ceux qui sont enclins à tirer parti d'une telle ressource. Sans même mentionner les fuites de listes noires directement sur Internet, des recherches indiquent qu'il serait possible de faire de la rétro-ingénierie des listes utilisées par n'importe quel fournisseur de services.

Le blocage de la pédo-pornographie sur Internet ne mettra pas un terme aux sévices sur les enfants. Il ne fera pas disparaître les images ou ne les supprimera pas d'Internet. La réponse la plus efficace à la pédo-pornographie et aux images d'enfants maltraités est d'ordonner leur suppression d'Internet, d'engager des poursuites pénales contre le pourvoyeur des images et de mettre en sûreté les enfants victimes d'abus afin qu'ils soient dans un environnement favorable à une thérapie réparatrice.

Le filtrage d'Internet rend parfois plus difficile l'accès à certains contenus (cela dépend du système de filtrage adopté) de telle sorte que seules les personnes les plus déterminées et les plus capables techniquement les découvriront (en fonction du logiciel qu'elles utiliseront). Lorsque les images contiennent des informations personnelles identifiables sur les victimes, bloquer de telles images peut les protéger de la crainte d'être à nouveau exploitées[5].

Malheureusement, certains contenus illégaux relatifs à la pédo-pornographie sur les sites Web sont hébergés actuellement dans des pays et par des hébergeurs pour lesquels la législation nationale, la conscience et l'intervention politiques sont sans comparaison aucune avec les meilleures pratiques actuelles suivant les critères internationaux et les procédures de notification et de retrait (notice and take down) sont sous-développées ou ne fonctionnent pas. Toute initiative visant à résoudre ce problème doit être encouragée.

Il est important de noter qu'un grand nombre de stratégies de filtrage sont de nature intrusive. C'est particulièrement vrai pour les mécanismes de filtrage les plus pointus qui nécessitent une analyse précise des contenus échangés entre les utilisateurs. Ce n'est pas seulement un problème du point de vue des moyens à investir (invariablement, ils sont très importants pour ce genre de scénario), mais aussi plus largement au plan sociétal.

[5]Ce point est abordé au chapitre 6

Il est généralement difficile d'évaluer si une mesure de filtrage d'Internet est une réponse proportionnée, parce que cela dépend essentiellement de l'objectif légitime [6] qu'on veut atteindre dans chaque cas, de l'utilité de la mesure mise en œuvre pour atteindre cet objectif légitime dans une circonstance particulière, des caractéristiques du filtrage et de leurs conséquences sur les droits et les libertés.

Les conséquences des mesures de filtrage d'Internet en termes d'interférence avec les libertés fondamentales sont mises en évidence aux chapitres 6 et 7. Toutefois, plusieurs processus de filtrage d'Internet entrainent d'autres interférences possibles, en raison de la nature des mécanismes mis en œuvre pour filtrer.

Pour savoir si chaque mesure qui interfère avec des libertés est une réponse proportionnée, il faut d'abord l'évaluer en fonction de son objectif légitime déclaré et ensuite selon son impact plus large, qui ne doit pas aller au-delà de ce qui est nécessaire pour atteindre l'objectif légitime et, en tout état de cause, conserver une certaine marge nécessaire à l'exercice de la liberté ainsi restreinte sans annihiler cette dernière.

à chaque fois qu'une mesure de filtrage est autorisée en raison de sa pertinence pour atteindre un objectif légitime, son fonctionnement basique ne doit pas limiter d'autres libertés de façn disproportionnée et il faut mettre en oeuvre des garde-fous qui empêchent d'utiliser ce dispositif d'une façn qui mettrait davantage les libertés en péril.

En tout état de cause, il faut souligner qu'aucune stratégie identifiée dans le présent rapport ne semble capable d'empêcher complètement le filtrage abusif. Ceci est d'une importance décisive lorsqu'on met en balance la nécessité de bloquer la pédo-pornographie et les exigences des droits de l'Homme et de la liberté d'expression. Il semble inévitable que des contenus légaux soient aussi bloqués lorsque le filtrage sera mis en œuvre.

Dans la mesure où les contenus présents sur Internet peuvent être échangés en utilisant diverses techniques, la pratique du filtrage limité à certaines d'entre elles (comme filtrer seulement le trafic de serveurs Web) peut facilement entraîner le recours à des procédés alternatifs de distribution du contenu. Ceux qui ont en tête de diffuser du matériel illégal sur Internet ont une myriade de possibilités pour le faire, en dépit des mesures de filtrage du réseau mises en place. D'un point de vue technique, les tentatives de filtrage peuvent, par conséquent, se borner à assurer une protection efficace aux usagers qui ne veulent pas accéder à ces contenus par inadvertance. Il semble peu probable que ces stratégies de filtrage, telles que le présent document les examine, soient capables de prévenir efficacement ou de façn substantielle la cyberdélinquance ni d'empêcher ceux qui en sont victimes de l'être à nouveau.

Les tentatives de filtrage d'Internet peuvent être caractérisées comme une action de re-localisation par laquelle un pays vise à s'assurer que ses critères nationaux s'appliquent au contenu globalisé disponible sur Internet, pour les usagers de ce pays.

Toutes les tentatives de filtrage ne sont pas du même ordre, tous les contenus ne sont pas du même type, et tous les types de crimes ou délits sont différents.

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

Le débat autour du filtrage d'Internet ne peut être limité à un problème particulier. Le débat est aussi complexe que le sujet lui-même. Les domaines concernés sont extrêmement divers et les défis auxquels les politiciens doivent faire face pour répondre aux problèmes posés par les contenus d'Internet sont complexes.

Il existe beaucoup de raisons pour lesquelles la société croit (et dans certains cas espère) que les tentatives de filtrage d'Internet pourraient résoudre des problèmes de société majeurs là où d'autres moyens ne se sont pas avérés très efficaces. Il existe de nombreuses institutions qui ont mis en œuvre le filtrage. Il existe une large gamme de matériels qui sont la cible de telles tentatives de filtrage. Celles-ci peuvent être entreprises de nombreuses façns différentes en fonction de ceux que l'on vise comme cibles de filtrage. Plusieurs pays ont déjà adopté des systèmes de filtrage d'Internet.

[6] Voir section 1.6

Internet est un réseau de réseaux immense et complexe, comprenant une myriade de matériels, de protocoles et de services mis en œuvre. La première étape d'une décision de filtrage d'Internet consiste à choisir à quel endroit on peut essayer de filtrer Internet. Un deuxième point clé est de déterminer qui doit choisir quoi filtrer et quels doivent être les différents niveaux de connaissance et de capacité des différents utilisateurs et organisations qui veulent filtrer les contenus d'Internet. Un large éventail de contenus peut causer différents problèmes dans différents environnements sociaux ; toute mesure de filtrage doit décrire la variété de contenus qu'elle vise et comment certains pouvoirs publiques ont considéré le filtrage d'Internet comme une solution possible à certains de ces problèmes. Il est important d'exposer les motivations primordiales qui incitent les décideurs politiques à envisager le filtrage d'Internet, ainsi que les raisons pour lesquelles les solutions alternatives semblent avoir échoué. Une mesure de filtrage d'Internet cible généralement soit les producteurs, soit les consommateurs de contenus illégaux et comprend différents niveaux d'efficacité suivant ce choix.

La gamme très complexe des approches et des motivations du filtrage d'Internet doit être clairement différenciée si l'on veut pouvoir établir une comparaison entre ces différentes approches.

Le premier critère qui peut être utilisé pour se repérer parmi les différentes approches de filtrage est la cible des outils de filtrage. En général, il y a quatre cibles différentes sur lesquelles peut se focaliser le filtrage :

- l'approche basée sur le service, par exemple l'e-mail ;
- l'approche basée sur le contenu, par exemple les discours de haine, la pédo-pornographie, les sites de casinos ;
- l'approche basée sur les utilisateurs, par exemple ceux qui téléchargent illégalement de la musique, envoient des courriers indésirables ; ou
- l'approche basée sur les moteurs de recherches, pour empêcher des sites illégaux d'apparaître dans les résultats de recherche.

Un second critère qui peut être utilisé pour différencier les approches du filtrage d'Internet est de se focaliser sur le rôle du décideur à propos des contenus illégaux. Le décideur est la personne ou l'institution qui décide de **ce qui doit** être filtré :

- choix individuel ;
- choix institutionnel ; ou
- législateur / tribunal.

On parle du filtrage d'Internet comme d'une solution technique au regard d'un large éventail d'activités illégales. Dans une certaine mesure mais pas nécessairement ces activités sont considérées comme des crimes ou délits dans les pays qui tentent de mettre en place ou ont déjà mis en place une technique de filtrage, mais ne tombent pas sous le coup de la loi de la même faqn dans les pays où le contenu est hébergé. La pédo-pornographie fait partie des catégories de contenus filtrés qui tombent sous le coup de dispositions du droit pénal.

Faire respecter le droit est difficile sur Internet, où les contenus sont souvent légalement mis à disposition sur des serveurs en dehors du pays. C'est une conséquence directe des différents standards nationaux mis en œuvre pour la publication des contenus. Tenter de filtrer les contenus qui sont légalement mis à disposition en dehors du pays mais qui sont considérés comme illégaux à l'intérieur du pays, peut être considéré comme une possibilité pour les états de préservers leurs propres normes culturelles nationales en cette période d'accès global.

Parmi les autres contenus ciblés par des tentatives de filtrage d'Internet on trouve :

- les pourriels (spams) les services prestataires de courrier électronique signalent qu'en ce moment, 85 à 90 pourcents des courriels sont des pourriels. La plupart des filtrages de pourriels sont effectués avec le consentement des clients ;
- le matériel érotique et pornographiques il est souvent considéré par les décideurs politiques comme devant être inaccessible aux mineurs au motif qu'il est dangereux. Dans certains pays, des *systèmes de vérification de l'âge adulte* ont été développés pour empêcher les mineurs d'accéder au contenu adulte . D'autres pays pénalisent tout échange de matériel pronographique même entre adultes ;
- La pédo-pornographie elle est universellement condamnée et les dérives associées à la pédo-pornographie sont largement reconnues comme des actes criminels. Malgré des efforts financiers conséquents, ces initiatives cherchant à contrôler la distribution en réseau de pédo-pornographie ont prouvé qu'elles ne dissuadaient que médiocrement les auteurs de tels actes ;

- les sujets politiques controversés / l'incitation à la haine et à la xénophobie certains pays pénalisent l'incitation à la haine raciale, à la violence et à la xénophobie, tandis que de tels contenus peuvent être publiés légalement dans d'autres pays qui disposent d'un niveau ęllcolorred Élevé de protection de la liberté d'expression, tels que les états-Unis ;
- les jeux d'argent illégaux Internet permet aux gens de contourner les interdictions concernant certains jeux. Les casinos en ligne sont largement accessibles et la plupart sont hébergés dans des pays ayant des lois libérales voire pas de loi du tout sur les jeux en ligne ;
- la diffamation et la publication de fausses informations les sites Web peuvent présenter des informations erronées ou diffamatoires, particulièrement dans les forums ou les chats, où des utilisateurs peuvent poster des messages qui ne sont pas vérifiés par des modérateurs ;
- les contenus publiés par des organisations terroristes la publication de propagande et d'informations liées à l'incitation au crime sont monnaie courante ;
- la violation de droits d'auteur elle comprend l'échange de chansons protégées par des droits d'auteur, de fichiers et de logiciels par des systèmes de partage de fichiers et le contournement des systèmes de gestion des droits numériques (en anglais, Digital Rights Management ou DRM). La technique Pair-à-Pair (P2P pour Peer to Peer) joue un rôle vital sur Internet.

Pourquoi envisager de filtrer Internet ?

- Le manque d'outils de contrôle sur Internet
  Puisque Internet a été conu à l'origine en s'appuyant sur une architecture en réseau décentralisé, résistante aux pannes et aux dysfonctionnements, Internet résiste aux tentatives de prise de contrôle par une entité externe. Les tentatives de filtrage peuvent être considérées comme un moyen de mettre en œuvre de tels instruments de contrôle qui n'étaient pas prévus dans la phase de développement du réseau.
- La dimension internationale
  La coopération internationale basée sur des principes traditionnels d'entraide judiciaire est souvent très lente et consommatrice de temps. Les exigences formelles et le temps nécessaire à une collaboration entre les différentes institutions de poursuites judiciaires à l'étranger ralentissent souvent les enquêtes. Les tentatives de filtrage pourraient par conséquent être considérées comme des moyens d'agir même dans les cas où les limites de la coopération internationale empêchent les mesures d'être prises en temps utile.
- L'importance décroissante de l'hébergement structuré par pays
  La publication d'un contenu qui est parfaitement légal dans un pays peut se révéler être un acte criminel ou délictuel dans un autre. Les tentatives de filtrage peuvent donc être considérées comme une volonté de re-localisation par laquelle un pays tente de s'assurer que ses critères nationaux s'appliquent sur un contenu global disponible pour les utilisateurs d'Internet dans ce même pays.

Qui doit-on filtrer ?

Le filtrage des contenus illégaux sur Internet peut être vu non seulement comme un moyen d'agir sur ceux qui transgressent la loi en rendant disponibles des contenus (les producteurs), mais aussi comme un outil de prévention pour empêcher les utilisateurs de télécharger des contenus illégaux (les consommateurs).

- Le producteur de contenu illégal le fournisseur de contenu illégal
  Internet est devenu un outil majeur de distribution de pédo-pornographie car il offre un grand nombre d'avantages aux auteurs de tels actes, faisant des enquêtes une véritable gageure. De faǫn comparable, les appareils photos numériques et les caméscopes sont devenus les principaux moyens de production de pédo-pornographie. Les raisons de la mise en œuvre de techniques de filtrage sont donc similaires à celles qui criminalisent l'échange de pédo-pornographie, c'est-à-dire la volonté de réduire le crime et de protéger les enfants.
- Le consommateur de contenu illégal
  Au-delà de la production, de la publication et de la mise à disposition de pédo-pornographie, un nombre significatif de pays rendent illégale la possession de matériel pédo-pornographique. La demande pour de tels matériels pourrait en accroître la production. Plus encore, beaucoup de pays ne se contentent pas de rendre illégale la possession de matériel pédo-pornographique, ils rendent aussi illégal l'acte ***d'obtenir un accès*** à la pédo-pornographie.

Alors que le fait que le filtrage d'Internet ne supprime pas le contenu à la source diminue les capacités de cet instrument à empêcher le délit de mise à disposition du contenu, il permet pourtant, s'il est techniquement efficace, de **potentiellement empêcher les délits commis par certains utilisateurs, qui essaient d'accéder à un site Web soit pour regarder, soit pour télécharger de la pédo-pornographie**. Le succès de l'opération dépend de l'efficacité des techniques de filtrage en place et du niveau de motivation et de connaissance de l'utilisateur.

Les principaux problèmes concernant le filtrage sont l'impossibilité de supprimer le contenu à sa source et les nombreuses possibilités de contourner le dispositif. Ces aspects ont plusieurs conséquences :

- le contenu peut encore être accessible en utilisant une connexion qui ne bloque pas l'accès ;
- une fois que les techniques de filtrage sont développées et mises en œuvre, on peut les utiliser pour une toute autre fin. Une des raisons majeures de ce problème vient de l'opacité de la mise en œuvre de ces techniques ;
- le fait que le contenu ne soit pas supprimé permet aux utilisateurs de chercher un moyen d'y accéder en contournant les solutions techniques de protection ;
- il existe plusieurs façons de contourner les différents systèmes de filtrage faisant actuellement l'objet de discussions ;
- le fait que le contenu ne puisse être supprimé suggère aux utilisateurs que ce sont des sites Web de confiance puisque les autorités ont clairement échoué à les éradiquer et à les poursuivre ;
- les échanges de pédo-pornographie via les systèmes de partage de fichiers ou les courriels chiffrés ne sont pas pris en compte par les solutions en ligne actuelles ;
- le fait de rendre invisibles de tels matériels pourrait fausser le débat politique en laissant croire que le problème de la pédo-pornographie en ligne a été efficacement traité, ce qui diminuerait ainsi la prise de conscience de la société dans ce domaine.

Outre les limitations systémiques des procédures de filtrage, des problèmes techniques et juridiques doivent être pris en considération.

Autres possibilités ne faisant pas appel au filtrage :

- améliorer les moyens de coopération internationale de façon à réduire le délai entre l'identification du contenu illégal hébergé à l'étranger et sa suppression ;
- travailler à l'éradication de tels contenus pour empêcher les délinquants sérieux d'y avoir accès ;
- mener des enquêtes judiciaires sur les images de pédo-pornographie pour s'assurer que les victimes de ces images soient identifiées et mises à l'abri de situations de maltraitance.

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 comme l'Australie, la Chine, l'Iran et la Thalande pratiquent le filtrage d'Internet. Les approches techniques, les objectifs du filtrage, ainsi que la participation de l'industrie sont variables.

En Australie par exemple, une liste noire élaborée par l'ACMA (l'autorité australienne des communications et médias) sera probablement obligatoire à l'avenir pour tous les fournisseurs de services Internet. Au Royaume-Uni, la liste noire est créée par l'IWF (Internet Watch foundation, observatoire d'Internet). La technique utilisée est le BT Cleanfeed ou le filtrage des adresses URL. Au Danemark, la liste noire est maintenue par le National High Tech Crime Center (centre national pénal des technologies de pointe) de la police nationale danoise et par l'ONG Save the Children Danemark (Sauver les enfants). En Finlande, le filtrage se basait initialement sur une liste de domaines fournie par la police finlandaise. Aujourd'hui, la plupart des fournisseurs de services Internet participent à cette démarche, mais en se basant sur le filtrage des DNS (Domain Name System, système de noms de domaine).

0.4 Les aspects techniques du filtrage d'Internet

La multiplication et la mise en œuvre de divers types de techniques de filtrage d'Internet ne constituent pas un développement récent. Pendant longtemps, le pourriel, les virus basés sur Internet, les logiciels malveillants et beaucoup d'autres types de contenus qui ne sont ni voulus ni demandés par l'utilisateur final ont été la cible des efforts de filtrage menés par les entreprises pour des raisons de sécurité et d'utilisabilité ou par l'état dans son rôle consistant à développer et faire respecter les lois et les politiques.

Une vue d'ensemble technique des principaux systèmes de filtrage d'Internet en service aujourd'hui est essentielle, ainsi qu'une explication sur la faqn dont ils sont appliqués aux différents services Internet. Outre les questions sur l'efficacité de tels systèmes de filtrage, ces systèmes engendrent des conséquences et des défis techniques significatifs. Il existe également plusieurs faqns d'échapper à ces systèmes de filtrage et il convient d'intégrer une analyse de l'efficacité de ces systèmes.

Des états démocratiques ont promu l'utilisation de techniques de filtrage d'Internet dans différents domaines politiques, invoquant l'intérêt public pour exiger que certains filtres soient mis en œuvre dans le but de faire respecter divers points de politique publique pour lesquels les caractéristiques d'Internet engendraient des difficultés à faire appliquer le droit (notamment au niveau international). De même, des états aux régimes moins ouverts sur l'information se sont mis au filtrage, en tant que ressource technique pour étendre leur pratique du contrôle de l'information au monde des réseaux.

Tous ces développements s'articulent sur la capacité des techniques de filtrage d'internet. Selon leurs caractéristiques techniques, ils diffèrent dans leur efficacité et leur chance d'être contournés. On se concentre principalement sur les techniques pour filtrer les contenus pédo-pornographiques, mais il est important de noter que beaucoup de techniques de filtrage peuvent être déployées pour d'autres types de contenus ou d'activités avec peu d'investissements supplémentaires.

Déterminer les contenus

Pour tenter de filtrer les contenus, des identifiants sont nécessaires pour qu'une décision de filtrage puisse être mise en œuvre. Les contenus sur lesquels ce rapport se concentre sont habituellement de nature visuelle, c'est-à-dire qu'ils contiennent soit des clichés photographiques, soit des images vidéos de sévices sexuels sur des enfants.

- Adresses IP ;
- nom de domaine et DNS ;
- URL ;
- contenu et nom de fichier ;
- mots clés ;
- Contenu des signatures (valeurs de hachage).

Mesurer l'efficacité

1. Il n'est pas possible d'exprimer l'efficacité comme la **quantité de contenus correctement filtrés comparée à la quantité totale de contenus disponibles illégalement** puisque le volume total de contenus disponibles illégalement est inconnu.
2. Puisqu'on ne sait souvent pas très bien d'où viennent les visites sur un site Web, **les chiffres mentionnant le volume de visites sur une liste existante sont au mieux un indicateur très approximatif**.
3. L'analyse du **potentiel de sur-filtrage et de sous-filtrage** peut être utilisée comme indicateur de l'efficacité des techniques de filtrage d'Internet.
4. Un autre indicateur pour l'efficacité est la **facilité de contourner un filtrage**. S'il est facile de contourner ou de désactiver un filtrage, il est probable que la disponibilité du matériel filtré restera inchangée.
5. **La disponibilité de méthodes alternatives pour accéder au même contenu**, par n'importe quel moyen, peut être vue comme une mesure de l'efficacité du filtrage en l'absence de données précises.
6. **La possibilité d'utiliser d'autres moyens d'action** qui procurent d'autres méthodes plus efficaces pour empêcher l'accès aux contenus, peut aussi être prise en compte particulièrement s'ils sont moins chers, moins intrusifs et plus efficaces pour la disponibilité au contenu.

Caractéristiques des stratégies de filtrage

- **Liste blanche contre liste noire** Les filtres qui sont configurés par défaut pour autoriser les contenus à passer sans entraves mais qui ont des listes spécifiques de contenus à filtrer sont habituellement appelés listes noires, tandis que les filtres qui sont configurés par défaut pour filtrer tous les contenus exceptés une liste de contenus spécifiques sont appelés *listes blanches*.

- **Intervention humaine (filtrage dynamique ou statique)** Typiquement, les filtres sur la pédo-pornographie sont basés sur des plaintes des consommateurs et des enquêtes visant à faire respecter le droit. Le contenu du filtre sera habituellement sélectionné manuellement, puisque l'administrateur de la liste de filtrage analyse personnellement les contenus et les fait personnellement correspondre aux critères de la liste. D'un autre côté, de nombreux filtres, comme les filtres de courriels et certains anti-virus seront souvent utilisés avec les critères prédéfinis pour filtrer les contenus sans intervention humaine. Ces critères peuvent avoir des facettes multiples et complexes.
- **Point de filtrage** On peut distinguer les stratégies de filtrage par le niveau auquel elles sont exécutées. Les filtres au niveau des utilisateurs autorisent les parents et les administrateurs informatiques à sélectionner et à bloquer certains types de contenus. D'autres techniques de filtrage sont employées par les associations, les FAI ou même au niveau de l'état. Ils exigent typiquement l'envoi de tout le trafic à travers des machines centrales qui analysent le trafic entrant.

Niveau de détails ou particularités

- **Adresses IP** Filtrer une *adresse IP* signifie que d'autres services Internet et utilisateurs qui utilisent la même adresse seront aussi filtrés.
- **Noms de domaines** Filtrer par noms de domaines filtrera ***tout*** le contenu présent sur ce domaine.
- **Localisateur uniforme de ressources (URL)** De meilleurs résultats en termes de spécificités seront obtenus en filtrant sur la base d'URL. Cela est dû à la facilité d'échapper à ces filtres, en filtrant par identifiant, on peut introduire un risque significatif de sous-filtrage.
- **Signatures des contenus** Les contenus peuvent être filtrés en utilisant les signatures qui ont déjà servi à classer des contenus comme illégaux. Les nouveaux contenus échappent facilement aux filtres. Le chiffrement des contenus rend cette méthode inutile.
- **Mots clés** Il s'agit du filtrage sur la base de mots clés trouvés soit dans le nom de fichier, soit dans l'URL, soit dans le texte à l'endroit où le contenu est accessible. Il convient de réaliser une analyse complexe des mots clés reconnus dans leur contexte d'utilisation.

Les méthodes de diffusion sur Internet de la pédo-pornographie.

La pédo-pornographie peut être diffusée sur Internet par des méthodes diverses *via* les connexions Internet à haut débit. Outre la distribution de contenus statiques (matériels photos et vidéos), elles servent également de rampes de lancement à d'autres activités voisines, comme la *manipulation* ou le *cyber-harcèlement*. L'augmentation de l'utilisation des réseaux sociaux est très importante dans ce dernier secteur.

- Sites Web
  Les sites Web sont le moyen de diffusion de contenus le plus employé sur Internet. Habituellement, les contenus du Web se trouvent sur un serveur, mais ils peuvent aussi être récupérés ou créés dynamiquement, là où une base de données est souvent utilisée pour conserver des données pertinentes. Beaucoup de serveurs Web différents gérés par différentes personnes sont fréquemment reliés à une seule adresse IP.
- Courriels et pourriels (courriels non sollicités)
  Le courriel est encore largement le service le plus utilisé sur Internet, même plus que les sites Web ou les réseaux sociaux.
- Listes de diffusion
  La différence capitale entre les listes de diffusion et les courriels est que les flux de messages échangés entre serveurs Usenet (souvent appelés flux de nouvelles) sont organisés à l'intérieur des groupes qui suggèrent des références au contenu des messages échangés.
- Réseau de pair à pair (P2P)
  Le partage de fichiers de pair-à-pair est basé sur l'échange de fichiers directement entre les ordinateurs des utilisateurs finaux, sans passer par des serveurs intermédiaires. Bien qu'il y ait des utilisations légitimes de cette technique, l'usage se prête au partage de fichiers de musique et de films, causant des défis majeurs pour les ayants droit.
- Moteurs de recherche
  En indexant les contenus des sites Web, les moteurs de recherche sont capables d'identifier les contenus pertinents par le biais de recherches par mots clés et d'algorithmes complexes de recherche.

– Messagerie instantanée et autres
Un autre outil important pour l'échange de contenu pédo-pornographique est la messagerie instantanée. Les canaux de messagerie instantanée servent plus comme mécanisme de contrôle et de mise en relation, alors que les contenus sont échangés directement avec d'autres techniques.

Stratégies de filtrage et efficacité

– Filtrage de site web
Filtrer les sites web est habituellement mis en place en utilisant un de ces deux identifiants :
  – le serveur qui contient le site Web peut être filtré au niveau de son adresse IP, empêchant quiconque utilisant le filtre d'accéder à cette adresse. Une liste noire ne contiendrait dans ce cas que des adresses IP de contenus illégaux connus ;
  – une mesure de filtrage peut également être adoptée en se basant sur le nom de domaine ou même sur l'URL d'une page ou d'un fichier page particlier du site hôte.

  Si ce type de tentative de filtrage s'effectue sur le réseau d'accès plutôt que sur l'équipement de l'utilisateur, son contournement représentera un défit plus important, toute proportion gardée, pour l'utilisateur, puisque ce dernier aura besoin de connaissances élémentaires sur le fonctionnement d'Internet.
– Filtrage des courriels
La plupart des filtres de courriels opèrent sur le serveur de mail **récepteur** qui récupère les courriels envoyés à l'utilisateur sur un réseau, ou juste avant ce serveur. Il exite deux faǫns de filtrer les courriels :
  – des filtres basés sur la connexion qui vérifient l'origine de l'adresse IP du serveur de courriel expéditeur à travers un certain nombre de listes noires ;
  – les filtres peuvent utiliser les contenus des messages pour bloquer les contenus indésirables. Une possibilité de sur-filtrage existe lorsque l'adresse IP, voire des serveurs de mails expéditeurs entiers, sont bloqués à cause d'incidents portant sur de la pornographie enfantine.
– Filtrage des listes de diffusion
Les tentatives de filtrages des contenus des listes de diffusion est habituellement réalisé en bloquant l'accès d'une partie de la hiérarchie du groupe ou en refusant d'héberger un groupe particulier. Les fournisseurs d'accès à Internet ont observé que, lorsqu'ils privent les utilisateurs de l'accès à des hiérarchies douteuses, ceux-ci seraient enclins à déplacer leurs contenus illégaux sous des noms moins voyants, entraînant potentiellement plus d'incidents d'accès fortuit au matériel illégal.
– Filtrage des résultats des moteurs de recherche
Il est possible d'empêcher l'accès aux résultats de recherche au niveau des fournisseurs de moteur de recherche. Une question importante réside dans la visibilité du filtrage, tel qu'affiché dans les pages de résultats des moteurs de recherche. Certains fournisseurs exposent clairement leur politique à propos du filtrage des résultats, d'autres non. Il est facile de contourner ces filtres : simplement en en accédant directement aux contenus.
– Pair-à-pair et filtrage de messagerie instantanée
Tenter de filtrer le trafic de pair-à-pair est une tâche considérable. Beaucoup de protocoles de p2p sont distribués c'est-à-dire que les fichiers en train d'être téléchargés sont fabriqués depuis plusieurs sources et, par conséquent, aucun flux de données ne contient l'intégralité du fichier.
  – La première option pour essayer de filtrer l'accès au contenu du P2P est d'analyser ce que les contenus du réseau P2P en agissant comme un utilisateur de ce service. En demandant certains fichiers ou en surveillant les demandes et les réponses des autres utilisateurs, il est possible de trouver les utilisateurs qui ont des parties d'un fichier sur leur disque dur. Bloquer l'accès à leur adresse IP ou déconnecter ces utilisateurs, si cela est possible juridiquement et techniquement, est dans ce cas le seul recours extrême disponible.
  – La seconde option avec une efficacité maximale pour essayer de filtrer les contenus sur ces réseaux est d'utiliser des techniques apparentée à de l'inspection approfondie des paquets (Deep Packet Inspection ou DPI) dans le but de reconnaître les fichiers au moment où ils sont échangés.

Résumé

Ce tableau liste les caractéristiques de chaque stratégie de filtrage évoquée. Il montre les probabilités du sur- et du sous-filtrage selon nos estimations. Il énumère les ressources nécessaires pour mettre en place la stratégie de filtrage, le type de liste noire et l'effort de maintenance exigé pour une telle liste. Et, dans la

dernière colonne, il indique si le contenu des communications nécessite d'être énormément analysé pour cette stratégie (technique DPI ou assimilée) pour que le filtrage soit effectif.

Alors que les méthodes de distribution peuvent varier, chaque méthode peut raisonnablement se substituer à chacune des autres méthodes. Sans se soucier de l'efficacité du filtrage de contenu sur un de ces médias, tout défaut dans le filtrage d'un même contenu sur l'un des autres médias amènera à changer la méthode de distribution.

La plupart des activités de pornographie enfantine sur Internet impliquent aujourd'hui l'utilisation de plusieurs services et systèmes Internet. Il existe plusieurs cas étudiés pour lesquels le contact entre un adulte et un enfant a commencé dans des salles de discussion publique, s'est déplacé vers des salons de discussion privés, puis a progressé vers des courriels personnels et des messages textuels SMS (Short Messaging Service, service de messages textuels courts) privés sur le réseau téléphonique portable avec une rencontre finale face-à-face planifiée *via* des appels personnels sur les téléphones portables.

Enquêter sur de telles activités est un véritable défi et requiert de larges connaissances de la part des enquêteurs sur tous les aspects des technologies d'Internet et des télécommunications.

Échapper au filtrage d'Internet

- Serveurs mandataires (proxy)
  Contourner ce type de filtre est assez aisé. Pour contourner un filtre bloquant l'accès direct, un utilisateur peut demander à un serveur mandataire étranger d'accéder pour son compte aux contenus filtrés et, tant que le serveur proxy étranger n'a pas lui-même été bloqué, l'utilisateur peut ainsi avoir accès aux contenus en évitant le filtre local.
- Tunnel
  Les tunnels logiciels permettent à l'utilisateur de créer un 'tunnel' chiffré vers une machine différente sur Internet qui empêche le logiciel de filtrage de voir leurs requêtes Web. Une fois que le tunnel est créé vers l'autre machine, toutes les requêtes Internet passent par ce tunnel, à travers la machine à l'autre bout, et vers Internet.
- Hébergement ou rotation des URL
  Du point de vue de l'éditeur de contenu, il est tout aussi banal de changer la configuration du site Web vers une adresse différente (nom de domaine, URL, voire adresse IP) est aussi banal et cela pourrait contourner efficacement les filtres d'IP, d'URL ou de noms de domaine.
- Machines zombies (Botnets)
  La rotation des noms de domaines ou le masquage d'adresse IP sont souvent réalisés en utilisant des techniques de machines zombies dans lesquelles des machines infectées d'utilisateurs finaux innocents sont utilisées pour agir comme portails d'accès aux contenus du serveur Web. En substance, l'ordinateur de l'utilisateur est utilisé en tant que serveur mandataire sans mémoire tampon (non-cache proxy).
- Échapper aux filtres de DNS
  Le filtrage au niveau des requêtes DNS est encore plus facile à contourner. Il suffit de changer le serveur DNS de fournisseur pour un autre (qui n'a pas de système de filtrage) pour contourner totalement cette méthode de filtrage.

Quand un filtrage est en place sur autre chose qu'une URL complète (un nom de chemin) ou qu'une signature de contenu, la potentialité de sur-filtrage est significative. Cependant, inversement, le filtrage par l'url ou par signature de contenu offre un potentiel significatif de sous-filtrage.

Filtrer le trafic Web efficacement, (c'est-à dire filtrer l'accès des utilisateurs aux contenus et pas simplement utiliser des filtres de DNS) nécessite d'investir significativement en infrastructures pour inspecter en profondeur ce qui circule par les proxies et d'intercepter de manière substantielle toutes les communications Internet.

Les filtres offrent la possibilité de fournir des indications utiles aux délinquants qui diffusent illégalement de la pédopornographie sur les sites Web. S'ils gèrent un site Web qui a été placé sur une liste noire de filtrage,

Média	**Filtrage**	**Efficacité**				**Liste noire**		**DPI**
		SURfiltrage	SOUSfiltrage	Ressources nécessaires	Contournement	Effort de maintenance	Identifiant	
Web	DNS	Très probable	Probable	Faible	Facile	Moyen	Nom de domaine	-
	Domaine	Très probable	Probable	Moyen	Moyen	Moyen	Adresse IP au nom de domaine	-
	URL	Peu Probable	Très probable	Moyen	Moyen	Élevé	URL	+
	IP	Très probable	Probable	Faible	Moyen	Moyen	Adresse IP	-
	Dynamique	Très probable	Très probable	Élevé	Moyen	Faible	Mots clés, graphiques, technique de reconnaissance ou autres	+
	Signatures	Peu Probable	Très probable	Élevé	Moyen	Élevé	Hachage	+
	Hybride (IP + signature/URL)	Peu Probable	Très probable	Moyen	Moyen	Élevé	IP et hachage ou URL	+
Courriel	Dynamique	Probable	Probable	Moyen	Difficilement	Faible	Mots clés ou autres	-
	URL	Probable	Probable	Moyen	Difficilement	Élevé	URL	-
	Adresse IP	Très probable	Probable	Moyen	Difficilement	Élevé	Adresse IP	-
	Signatures	Peu Probable	Probable	Élevé	Difficilement	Élevé	Hachage	+
Listes de diffusion	Par groupe	Probable	Probable	Faible	Facile	Faible	Nom du groupe	-
	Par hiérarchie	Très probable	Peu Probable	Faible	Facile	Faible	Hiérarchie du groupe	-
Recherche	Mots clés	Très probable	Très probable	Élevé	Facile	Moyen	Mots clés	-
P2P	Par protocole	Très probable	Peu Probable	Moyen	Difficilement	Faible	Reconnaissance de protocole	+
	Par fichier (signature)	Peu Problable	Très probable	Élevé	Difficilement	Élevé	Hachage	+
	Par fichier (dynamique)	Probable	Très probable	Très Élevé	Difficilement	Faible	Algorithmes avancés	+

alors ils savent qu'il a été identifié par les autorités et qu'il est très probablement la cible d'enquête et de surveillance par les services de police.

- Les délinquants peuvent alors prendre des mesures pour détruire toutes les preuves ET des dispositions pour déménager leurs services vers un nouveau lieu n'importe où ailleurs dans le monde.
- Ils peuvent tester la résistance de leurs techniques de camouflage aux systèmes de détection pour rechercher quelles techniques leur fournissent la plus longue protection contre la détection et le filtrage.
- Les activités de filtrage causent également des perturbations pour ceux qui accèdent à de tels sites, forçant ainsi les opérateurs Web à déplacer leurs contenus plus fréquemment. Ces déplacements peuvent aussi être surveillés, donner des indications précieuses aux enquêteurs qui les pistent et fournir des données de recherche fort utiles.

Les ressources et les efforts exigés pour échapper continuellement aux activités de filtrage tout en restant anonymes ne doivent pas être sous-estimés. Il est probable que cette situation conduira tôt ou tard à commettre des erreurs. Cependant, il est important de noter que les ressources et les efforts pour créer et maintenir un système de filtrage d'Internet sont juste assez importants particulièrement quand il est nécessaire de répondre constamment à des activités de contournement.

Répercussions pour une société démocratique

- Problème de sécurité
  L'infrastructure nécessaire pour appliquer une stratégie de filtrage est capable d'interférer avec de nombreux éléments critiques des connexions Inernet des utilisateurs finaux. De plus, le contenu des listes noires est le premier intérêt des coupables de pédophilie puisqu'ils sont fortement désireux d'utiliser ces listes de filtrage pour la raison inverse à celle pour laquelle elles ont été créées :
- Sur-filtrage et sous-filtrage
  Aucune des stratégies identifiées dans ce rapport ne semble être capable de protéger du sur-filtrage. C'est une des préoccupations majeures dans l'équilibre entre la protection des enfants et les droits de l'homme et de la liberté. Il parait inévitable que le contenu légal soit filtré aux endroits où les filtres sont implémentés. Le sous-filtrage est aussi un phénomène universel spécialement présent dans la plupart des stratégies étudiées.
- Risques de dérives au-delà de l'objectif et re-territorialisation
  De nombreuses stratégies de filtrage sont vraiment intrusives dans les communications par Internet. La plus granulaire, basée sur des mécanismes de filtres du contenu, nécessite une intrusion dans le contenu du matériel échangé entre les utilisateur.

Il est important qu'un débat public ait lieu et que ce débat prenne en compte les différences essentielles techniques et juridiques entre les différents types de contenus et la proportionnalité du filtrage vis-à-vis d'autres méthodes de diminution du préjudice, de lutte contre la délinquance et des enquêtes sur le cyber-crime.

0.5 Le filtrage d'internet et le droit

Essayer de bloquer les contenus illégaux ne revient pas à supprimer définitivement l'accès à des images, vidéos ou pages Web spécifiques. Les inévitables possibilités de contournement, le sous-filtrage, le sur-filtrage, les dérives, le droit international privé et le problème que le filtrage laisse les matériels en ligne, tout cela signifie que la question n'est pas simplement de bloquer ou ne pas bloquer , mais plutôt de savoir quelles mesures de filtrage peuvent être mises en place tout en étant proportionnées et acceptables dans une société démocratique.

Un panorama exhaustif du filtrage d'Internet et du droit nécessite une analyse des instruments juridiques pertinents affectant les systèmes de filtrage d'Internet. Les démocraties libérales modernes jouent un rôle clé de par leur respect actif des libertés fondamentales et des libertés publiques. Les instruments tant nationaux qu'internationaux nécessitent d'être étudiés pour déterminer quels sont les droits fondamentaux sont en

contradiction avec le filtrage d'Internet et lesquels viennent l'étayer. Le rôle des fournisseurs d'accès à Internet est fondamental pour les mesures de filtrage d'Internet et ils agissent dans des circonstances déroutantes vis-à-vis d'obligations légales concurrentes et parfois contradictoires.

Aux yeux de la loi, le filtrage d'Internet est une mesure qui, dans le but de protéger un intérêt particulier, accorderait un droit à filtrer, à choisir les moyens techniques pour y parvenir et à choisir les contenus à filtrer, en étant conscient que cela aurait pour résultat de priver certains citoyens de leur droit à accéder à des contenus ou à rendre disponibles certains contenus.

Par conséquent, le filtrage d'Internet est une mesure qui serait mise en place pour protéger des droits ou des libertés particulières, tout en ayant une incidence directe et immédiate sur d'autres droits et libertés. Puisque les droits et les libertés sont régis par la loi, l'analyse de la légitimité du filtrage d'Internet nécessite (par conséquent) une analyse approfondie des éléments de droit qui sont pertinents pour, et pourraient être en conflit avec une telle mesure.

Puique le filtrage d'Internet est une mesure qui est débattue internationalement, cette étude se concentrera particulièrement sur le droit international et européen, tout en donnant quelques exemples d'application aux niveaux des lois nationales.

Au sein de ces systèmes juridiques, le filtrage d'Internet peut être incompatible avec deux domaines de loi, à savoir les droits de l'homme et les libertés fondamentales et certaines clauses relatives aux communications électronique d'autre part. Sa compatibilité avec certains aspects de ces droits et libertés dépend de la proportionalité de la mesure de filtrage d'Internet adoptée.

Le défi est de déterminer dans quelle mesure une liberté peut être limitée dans le but d'en préserver une autre. Chacune de ces libertés nécessite d'être étudiée en détail pour permettre de conclure sur les conditions dans lesquelles le filtrage d'Internet pourrait être considéré comme acceptable au niveau des principes juridiques.

De nombreux systèmes juridiques nationaux, tout comme les systèmes juridiques européens et internationaux, donne une place importante aux droits de l'homme et aux libertés fondamentales, qui peuvent être invoqués pour justifier une mesure de filtrage, ou qui peuvent être affectés de manière inappropriée par une telle mesure.

La sauvegarde des droits de l'homme et en particulieur ceux qui peuvent être en conflit avec une mesure de filtrage d'Internet, par exemple le droit à la vie privée ou le droit à la liberté d'expression, est souvent considérée comme intrinsèque à la démocratie. La relation entre démocratie et liberté peut être vue sous trois aspects :
– les élections le principe de participation de tous à la vie publique ;
– la séparation des pouvoirs les structures institutionnelles pour la séparation des pouvoirs ; et
– les droits fondamentaux la volonté de l'état et son engagement à respecter les libertés.

La différence entre les droits de l'homme, les libertés fondamentales et les libertés publiques réside principalement dans la personne détentrice des droits, qui dépend du contenu accordé au droit, de la valeur juridique du texte et de l'importance de sa sauvegarde. Les trois qualifications peuvent s'appliquer à un droit particulier, comme le sont les droits à la protection de la vie privée et à la liberté d'expression dans de nombreux pays. Les libertés publiques sont des limitations du pouvoir de l'autorité publique envers les citoyens.

Aux notions de droits de l'homme et de libertés publiques, a été ajoutée celle de droits fondamentaux ou de libertés fondamentales . Les droits et libertés fondamentaux sont :
– protégés contre l'exécutif et contre le pouvoir du Parlement ;
– garantis non seulement par la loi mais avant tout par la Constitution ou par les textes internationaux ou supranationaux ;
– préservés des pouvoirs executif et juridique, à travers l'application de la Constitution (ou des textes internationaux), la compétence non seulement des juges ordinaires, mais égamement des juges consitutionnels et même internationaux.

Les premiers textes qui ont reconnus les droits de l'homme et les libertés fondamentales étaient nationaux. Les textes internationaux sont venus après la deuxième guerre mondiale et ont contribué à modifier les systèmes juridiques nationaux. Leur contenu a également été reconnu par les institutions de l'Union européenne.

Les tentatives de filtrage d'Internet ont besoin d'être analysées à la lumière des principales libertés fondamentales qui semblent être en conflit celui-ci ce qui inclut la liberté d'expression et le droit au respect de la vie privée et familiale ou qui semblent l'étayer ce qui inclut le droit des enfants à être protégés contre la violence et l'exploitation.

Les instruments internationaux relatifs aux droits de l'homme et aux libertés fondamentales ont été adoptés dans le cadre de l'Organisation des nations Unies et du Conseil de l'Europe. Ils commprennent :
- la Charte des Nations unies ;
- la Déclaration universelle des droits de l'homme de l'ONU (DUDH) ;
- le Pacte international relatif aux droits civils et politiques de l'ONU (PIDCP) ;
- la Convention relative aux droits de l'enfant de l'ONU ;
- la Convention relative aux droits des personnes handicapées de l'ONU ;
- la Convention internationale sur l'élimination de toutes les formes de discrimination raciale de l'ONU ;
- la Convention européenne des droits de l'homme du Conseil de l'Europe (CEDH) ;
- la Convention sur la cybercriminalité du Conseil de l'Europe

Bien que l'Union européenne n'ait pas encore adhéré à la Convention européenne des droits de l'homme, l'Union européenne reconnaît la nécessité de préserver les libertés fondamentales et de respecter la CEDH. L'Union européeenne met aussi l'accent sur certaines catégories de droits tout comme les textes internationaux analysés, tels que les droits de l'enfant, les droits pour les personnes handicapées ou le droit à ne pas être discriminé.

Les libertés fondamentales susceptibles d'être en contradiction avec le filtrage

Le filtrage d'Internet peut avoir une incidence sur certains droits de l'homme et sur certaines libertés fondamentales.
- Les tentatives de filtrages d'Internet peuvent s'immiscer dans le **droit à la vie privée**, permettant ou nécessitant la conservation de données Internet qui sont protégées par la confidentialité, ou empêchant les individus de se servir de certaines potentialités offertes par Internet et faisant ainsi obstacle à la possibilité de créer certaines connexions ou de faire certains choix de connexion, ce qui entre dans le droit à la liberté de la vie privée. C'est en particulier le cas au regard du sur-filtrage qui impacte des sites web complétement innocents.
- Les tentatives de filtrage d'Internet peuvent s'immiscer dans **la liberté d'expression**, en empêchant les gens d'accéder aux informations en ligne ou de rendre disponibles de telles informations. Cela a une incidence négative sur la diffusion de l'information, la communication et la réception.
- Le filtrage d'Internet s'immisce dans les droits spécifiques accordés à certaines catégories de personnes, comme **le droit pour les personnes handicapées** d'accéder aux communications électroniques.
- Le filtrage d'Internet peut être vu comme un succédané pour respecter les obligations de la Convention sur les droits de l'enfant exigeant que les états prennent toutes les mesures internationales appropriées pour empêcher l'exploitation des enfants dans un but pornographique.

Le droit au respect de la vie privée et familiale est un droit de l'homme et une liberté fondamentale et, par conséquent, une liberté publique. Il concerne directement les adultes et les enfants, même si la Convention des Nations unies sur les droits de l'enfant complète ceci avec une déclaration spécifique en son article 16 sur le droit des enfants au respect de leur vie privée.

Le droit à la vie privée

Ces textes protègent les individus d'une immixtion arbitraire dans leur vie privée, leur famille, leur domicile ou leur correspondance et des atteintes à leur honneur et à leur réputation. La DUDH déclare que *Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* . Le PIDCP déclare la même chose et ajoute que **les immixtions doivent être légales**, ce qui remet en question certaines

initiatives de filtrage menées pas des industries, qui n'ont aucune justification légale. La CEDH autorise certaines ingérences aux conditions décrites dans la fameuse clause d'ordre public , comprenant le principe de légalité.

Le principe de correspondance privée, que la Cour européenne des droits de l'homme interprète comme *protégeant la confidentialité des communications privées*", est l'une des libertés Fondamentales qui pourrait être directement ébranlée par une mesure de filtrage d'Internet.

Selon la cible du filtrage (type de contenus, protocoles de communication) les moyens utilisés pour le filtrage et les règles supplémentaires potentiellement mises en place pour atteindre l'objectif particulier du mécanisme dans son ensemble, les tentatives de filtrage d'Internet peuvent parfois conduire à la conservation du contenu d'une communication ou de certains détails de ce contenu en relation avec une personne spécifique, sans le consentement de cette personne.

Même si les communications reçues ou émises par une personne ne sont pas classées comme étant une correspondance, elles n'en sont pas moins protégées par le droit à la vie privée. Sur la base de ce principe, une mesure de filtrage qui amenerait à surveiller ou à conserver des données relatives aux contenus qu'une personne reçoit, émet ou consulte, même s'il ne s'agit que de la consultation d'un site web d'une nature particulière, pourrait être une immixtion dans le droit à la vie privée. Ce serait également une ingérence dans le droit à la protection des données personnelles.

Le principe de la protection des données personnelles implique la confidentialité de ces données, lorsqu'elles sont associées avec des données permettant l'identification directe ou indirecte d'une personne physique. Chaque morceau de donnée permettant la surveillance des personnes est considéré comme dangereux, même s'il n'est pas utilisé, particulièrement dans un état démocratique.

La liberté de la vie privée peut être comprise comme la liberté d'établir et à maintenir des relations, également *via* les communications électroniques, mais également de faire en ligne des choix culturels, de loisir ou de consommation ou de naviguer librement et d'accéder aux informations sur le réseau. La liberté de correspondance, qui est le pouvoir de correspondre avec des personnes choisies, est elle-même protégée par le droit au secret de la correspondance.

Une mesure de filtrage d'Internet qui aurait une influence négative sur la liberté de correspondre serait par conséquent en conflit avec l'article 8 de la DUDH.

Le filtrage d'Internet peut être considéré comme étant en conflit avec une liberté fondamentale aussi longtemps qu'il présente **un risque de s'immiscer dans une telle liberté, même s'il n'a pas vocation à utiliser la fonctionnalité qui présente un tel risque.**

La liberté d'expression

La liberté d'expresssion est un droit de l'homme et une liberté fondamentale et, par conséquent, une liberté publique. Elle s'applique aux adultes et aux enfants et la Convention de l'ONU sur les droits de l'enfant ajoute une déclaration spécifique sur le droit des enfants 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 considération de frontière* . Ce droit doit être exercé *sans qu'il puisse y avoir ingérence d'autorités publiques* . La DUDH et le PIDCP ajoutent la liberté *de chercher* des informations et des idées *par quelque moyen d'expression que ce soit* pour la DUDH, alors 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 disposent que l'exercice de la liberté d'expression comporte des *devoirs et responsabilités* et peut être soumise à certaines restrictions.

La liberté d'expression inclut le droit de recevoir de l'information, notamment à travers d'Internet. Toute mesure de filtrage d'Internet qui empêcherait une personne d'accéder au contenu serait par conséquent en conflit avec cette liberté. Cela serait pire pour une mesure qui préconise la suspension de l'accès Internet, empêchant ou entravant ainsi l'usage du réseau Internet dans son ensemble ou d'une partie de celui-ci.

Dans le cadre de la réforme de la législation sur les télécoms, le Parlement européen a répété, le 6 mai 2009 qu' *aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux sans décision préalable des autorités judiciaire [] sauf lorsque la sécurité publique est menacée* . Plusieurs auteurs et les membres du Parlement européen ont cru que cela était une reconnaissance de l'accès à Internet comme étant un droit fondamental.

Que l'accès à Internet soit ou non un droit fondamental *indépendant*, celui-ci est tout au moins protégé comme un moyen d'exercer la liberté d'expression, et toute mesure de filtrage d'Internet qui tente d'empêcher les personnes d'accéder à l'information est par conséquent en conflit avec cette liberté. Toute mesure de filtrage limite le droit à la liberté d'expression, de manière plus ou moins large selon les caractéristiques du filtrage et le degré de sur-filtrage, puisque l'objectif final d'une telle mesure est de limiter l'accès à un contenu particulier.

Les droits de l'enfant

Toute mesure de filtrage d'Internet qui voudrait empêcher les enfants d'accéder aux informations qui pourraient être utiles pour leur développement ou leur éducation à une vie responsable, pourrait être en conflit avec la Convention sur les droits de l'enfant et certainement avec le droit à la liberté d'expression, particulièrement si cela n'est pas sous le contrôle des parents.

Les droits des personnes handicapées

Les personnes handicapées connaissent le problème supplémentaire que leur handicap peut parfois restreindre le plein exercice de leurs droits. Ils peuvent être aidés par l'utilisation de communications électroniques y compris les services Internet. Par conséquent, une mesure de filtrage d'Internet qui empêcherait les personnes handicapées d'accéder aux communications électroniques pourrait empêcher certaines d'entre elles d'exercer des droits fondamentaux que les personnes non-handicapées seraient toujours en mesure d'exercer malgré une interdiction d'utiliser Internet ou une partie de ce dernier.

Droits et libertés fondamentaux susceptibles d'étayer le filtrage d'internet

La protection de certains autres droits et libertés pourrait étayer le filtrage d'Internet. Trois de ces droits sont :
- les droits 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 grandement protégés contre la violence. Il existe deux aspects de la protection du bien-être de l'enfant qui ont un intérêt particulier.
- Le nombre important de textes qui mettent l'accent sur la prohibition de la violence physique et mentale envers les enfants, particulièrement de nature sexuelle.
- La prohibition de l'image même d'un crime de nature sexuelle commis envers un enfant, à travers la prohibition de la pédo-pornographie.

L'importance du combat contre la pédo-pornographie, ainsi que l'importance de la protection des enfants contre la violence et la déterioration du développement personnel, constitue très fréquemment un argument justifiant la mise en œuvre du filtrage d'Internet.

S'il fallait accepter les arguments avancés pour étayer le filtrage, il serait juridiquement difficile de comprendre pourquoi une mesure de blocage serait restreinte uniquement à la pédo-pornographie, puisque le droit protège également spécifiquement d'autres catégories de personnes contre les menaces, notamment les menaces engendrées par la discrimination.

Les droits de l'homme et les libertés fondamentales sont accordés à chaque individu sans distinction. Cependant, comme la discrimination a été et devrait encore être un problème dans certains pays, plusieurs textes ont été signés pour insister particulièrement sur le droit de tout individu à être protégé contre la discrimination. Les contenus d'Internet qui entrent dans ces interdictions peuvent être des textes encourageant la discrimination, mais également les images de tortures ou de meurtres, commis pour des considératons raciales. Ces images sont très perturbantes et pourraient tout aussi bien offrir une justification valable pour le filtrage d'Internet, en plus de la pédo-pornographie.

Les droits de propriété industrielle (DPI) sont protégés par de nombreux traités au niveau international. La déclaration générales de tels droits comprend notamment le droit d'auteur et les droits connexes, qui *protègent les droits des créateurs, artistes interprètes ou exécutants, producteurs et radiodiffuseurs, et contribuent au développement culturel et économique des nations* . Le droit à la protection des DPI est par conséquent considéré comme un droit de l'homme et une liberté fondamentale, et devrait aussi être une liberté publique dans certains pays. Ce droit pourrait donc être évoqué pour justifier une mesure de filtrage d'Internet, tant qu'une telle mesure servirait, en réalité, à le protéger.

Les dispositions spécifiques relatives aux communications électroniques

Une mesure de filtrage envisagée pour l'Union européenne doit en outre respecter les règles européennes s'appliquant aux communications électroniques.

- Ces règles comprennent les obligations pour le fournisseur d'accès à Internet en terme de **qualité de service** et **les obligations de service universel** et **l'obligation de neutralité** du fournisseur d'accès à Internet.
- Les règles concernant la **responsabilité** des fournisseurs d'accès à Internet leur fournissent une raison supplémentaire sur laquelle se baser pour plaider contre les mesures de filtrage mises en œuvre en dehors du cadre d'une loi.

Les services inclus dans le champ du **service universel** sont des services de communication de base, comprenant les communications vocales et une connexion à Internet. Toute mesure de filtrage qui empêcherait un utilisateur d'Internet d'accéder au réseau de téléphone public serait donc en conflit avec cette obligation de service universel. Autoriser les citoyens à accéder à Internet reste un objectif qui doit respecter un équilibre avec d'autres droits et libertés et avec l'intérêt général du public.

Si l'internet à haut-débit est reconnu à l'avenir comme un composant du service universel et si les révisions en cours de la législation de l'UE sur les télécoms est finalement approuvée, un état ne serait donc pas autorisé à prendre toute mesure de filtrage de l'utilisateur sans respecter la Convention européenne des droits de l'homme, particulièrement en ce qui concerne la nécessité de respecter la clause d'ordre public et le droit à un procès équitable, devant une cour de justice.

Les opérateurs de communications électroniques doivent également assurer une certaine **qualité de service de l'accès** qu'ils fournissent. Ils sont en charge de véhiculer le service public d'information, en plus des obligations spécifiques qu'ils sont susceptibles de devoir respecter lorsqu'ils assurent un service universel ou une obligation de service public.

Les réseaux publics informatiques sont très complexes techniquement et la plupart des mesures de filtrage d'Internet augmentent la probabilité que le réseau souffre de pannes et de temps de latence. Par conséquent, **exploiter un réseau de communications électroniques et le filtrer relèvent de philosophies antinomiques** et demander à un opérateur de mettre en œuvre une mesure de filtrage peut le placer dans une position où deux obligations avec des effets contradictoires doivent être respectées.

Les fournisseurs d'accès à Internet ont une obligation de neutralité vis-à-vis des contenus des communications électroniques échangées sur Internet, suivant l'exemple d'autre catégories de transporteurs (comme les services traditionnels de téléphonie et les services postaux). Il en résulte qu'un fournisseur d'accès à Internet ne peut pas choisir de transmettre ou non un message en fonction de son contenu, excepté avec le consentement du consommateur ou une obligation légale qui justifierait le non-respect du principe de neutralité.

Un fournisseur d'accès à Internet ne peut pas surveiller les contenus qui sont échangés à travers son réseau, excepté sur la base d'obligations spécifiques établies par la loi. Toute mesure de filtrage qui nécessiterait une surveillance des contenus échangés sur le réseau pour identifier des contenus spécifiques illégaux ne serait donc pas autorisée à moins d'être spécialement prévue par une loi respectant la clause d'ordre public européenne.

Sans une loi les contraignant à filtrer des contenus spécifiques, les fournisseurs d'accès à Internet ne peuvent surveiller ni filtrer les contenus du Web sans enfreindre la condition des protections de leur responsabilité mises en œuvre par la directive européenne, et par conséquent ils risquent leur responsabilité pour les contenus qu'ils transmettent.

Un fournisseur d'accès à Internet qui sélectionnerait certains contenus à filtrer, sans être contraint par une loi de le faire, serait susceptible de tomber en dehors des obligations établies par le régime de responsabilité actuel. Un tel fournisseur d'accès à Internet prendrait donc le risque de voir sa responsabilité récusée devant un tribunal, pour chaque portion de contenu ou d'activité illégal qui serait transmis par ses services. Une telle situation serait juridiquement tout à fait incertaine. Cela compromettrait les propres activités du fournisseur d'accès à Internet et, plus globalement, le développement technique du pays.

0.6 Respecter l'équilibre entre les libertés fondamentales

D'après le Pacte international relatif aux droits civils et politiques et la Convention européenne des droits de l'homme, la question de trouver un équilibre entre des libertés se place toujours dans le cadre d'une limitation d'une libertée protégée dans le but d'en préserver une autre.

Dans le cadre d'une mesure de restriction de l'Internet, les droits des enfants, ceux des personnes à ne pas être discriminées ou ceux concernant la propriété intellectuelle, doivent respecter un équilibre avec les droits et libertés de la vie familiale et la liberté d'expression, qui s'opposent aux premiers.

Quelques-uns des droits identifiés par le Pacte international relatif aux droits civils et politiques et la Convention européenne des droits de l'homme sont considérés comme absolus , comme par exemple le droit à la vie ou celui de ne pas être torturé, tandis que d'autres sont conditionnels parce qu'ils peuvent être soumis à des dispenses et/ou des limitations, comme le droit à la vie privée et le droit à la liberté d'expression.

Pour réussir à respecter l'équilibre entre des libertés fondamentales conditionnelles lorsque différents droits se trouvent en conflit, il faut utiliser une analyse des processus adoptée par la Cour européenne des droits de l'homme qui peut fournir des directives sur la faǫn de mettre en place des mesures de filtrage de l'Internet. Cela nécessite de prendre en compte la **clause stricte d'ordre public** qui comprend **les principes de nécessité dans une société démocratique** . Ces principes sont ensuite appliqués à différentes initiatives de filtrage d'Internet en évaluant les objectifs de ces initiatives et comment elles pourraient être jugées selon les directives de la CEDH. La légitimité des objectifs d'une initiative de filtrage d'Internet et la validité de certains systèmes doivent être examinés et débattus. Une série d'étapes peut être suivie pour évaluer la légitimité des propositions de restriction de l'Internet dans une société démocratique.

La clause d'ordre public

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

- Certaines dispositions proclamant des droits conditionnels énumèrent de manière restrictive les situations où une limitation est acceptable.
- D'autres dispositions proclamant des droits conditionnels, comme les articles 8 et 10 de la CEDH en relation avec le droit au respect de la vie privée et à la liberté d'expression, établissent comme principe général ou comme une *clause générale d'ordre public* que les ingérences doivent être **prévues par la loi** , poursuivre **un ou plusieurs buts légitimes** au regard de l'article qui déclare le droit conditionnel et être **nécessaires dans une société démocratique pour atteindre le ou lesdits buts** .

Cette clause d'ordre public contient avant tout 3 principes fondamentaux qui sont :
- la **compétence exclusive de la loi pour limiter les libertés** ;
- le **besoin de poursuivre un des buts légitimes listés par la Convention** ;
- la **nécessité de l'ingérence dans un pays démocratique , qui est interprétée par la Cour européenne des droits de l'homme comme impliquant que l'ingérence dans une société qui entend demeurer démocratique**
  - corresponde à un **besoin social impérieux** ;
  - soit proportionnée au but légitime poursuivi .

Le principe de légalité

Toute mesure de filtrage, du moins dans le cadre de la CEDH, doit être prévue par une loi répondant à cette définition :
- *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 .

La seule sorte d'accord qui pourrait autoriser une mesure de filtrage serait le contrat entre l'utilisateur d'Internet et le fournisseur d'accès. La légalité d'une telle mesure de filtrage dépendrait pour beaucoup du type de contenu consulté, de la nature de l'entorse aux droits et libertés et des preuves requises. Si cela n'est pas précisé d'une faqn raisonnable, il est facile d'envisager que de tels contrats soient considérés comme des entorses à la directive européenne sur les clauses contractuelles abusives, particulièrement si cela permet au fournisseur d'accès à Internet de prendre des sanctions unilatérales à l'encontre de son client.

Le principe d'un but légitime

La Convention des droits de l'homme et, en ce qui concerne la liberté d'expression, le PIDCP établissent une liste exhaustive des buts légitimes pour lesquels une ingérence dans les libertés fondamentales peut être légitime.

Un but légitime, prévu par la loi qui permet une mesure de filtrage d'Internet, n'est de toute faqn pas suffisant pour considérer la limitation comme légitime d'après la législation européenne. Cette mesure doit aussi être nécessaire dans un pays démocratique.

En ce qui concerne le droit à la vie privée, la CEDH (article 8) autorise les ingérences nécessaires :
- *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 .*

En ce qui concerne le droit à la liberté d'expression, la CEDH (article 8) autorise les ingérences nécessaires :
- *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 .*

En ce qui concerne le droit à la liberté d'expression, le PIDCP (article 19) autorise les ingérences nécessaires :
- *au respect des droits ou de la réputation d'autrui ;*
- *à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques .*

Pour être légitime, toute mesure de filtrage doit donc poursuivre un des buts listés dans le texte qui s'y applique, selon la convention dont le pays concerné fait partie et selon la liberté fondamentale limitée par cette mesure. L'une des questions clés peut être de déterminer l'intérêt ou le but poursuivi par cette mesure.

Le filtrage des pourriels (spam) Le but du filtrage des pourriels est tout d'abord la protection des droits du fournisseur d'accès à Internet de préserver l'existence de son service de courriel, et ensuite la protection de la liberté de correspondance des utilisateurs de ce service. C'est pourquoi le but d'une mesure de filtrage des pourriels, qui peut limiter la liberté de correspondance et surtout le droit à la vie privée, semble être *la protection des droits et libertés d'autrui* , ce qui est un but légitime d'après l'article 8 de la CEDH.

L'objectif de protéger les intérêts de la victime Un des buts d'une mesure de filtrage visant des contenus illégaux, pourrait être l'intérêt de la victime à ne pas être vue dans le contexte d'une scène de crime. C'est pourquoi cela remplit l'objectif spécifié précédemment comme *la protection des droits d'autrui* , quand cela limite soit le droit à la vie privée ou le droit à la liberté d'expression. Comme toute pédopornograpie n'inclut pas forcément des informations permettant l'identification, cela n'a pas toujours un but légitime et, à cause de l'inadéquation technique des mesures de filtrage, le filtrage peut, au mieux, prétendre partiellement **respecter** ce critère.

L'objectif d'empêcher les gens de voir des contenus illégaux la morale ou la protection des sensibilités individuelles Une mesure de filtrage d'Internet visant des contenus illégaux pour empêcher les personnes de voir des contenus illégaux, protégeant de cette manière la morale ou les sensibilités individuelles des personnes les plus faibles de la société peut s'accorder avec l'intérêt de *protection de la santé ou de la morale* . *Si le but de protéger les sensibilités des citoyens les plus faibles peut être vu comme légitime*, le lien avec la morale semble au contraire très faible, surtout en Europe, puisque d'habitude les gens dénoncent les contenus illégaux pour qu'il y ait enquête. Dans ce contexte, il est aussi important de se rappeler (comme mentionné ci-dessus) que la vaste majorité des contenus signalés ne sont en fait pas illégaux.

L'objectif de prévenir le crime Un autre but des mesures de filtrage visant les contenus illégaux, pourrait être la prévention du crime.
- Voir de la pédo-pornographie pourrait inciter des personnes, qui ne sont pas pédophiles, à développer de tels comportements par la vue répétée d'images de pornographie enfantine, bien qu'il y existe très peu de preuves confirmant cette hypothèse.
- Les tentatives de filtrage d'Internet peuvent déjouer le commerce de pédo-pornographie et de ce fait prévenir le crime, si les entreprises en question n'ont pas mis en place des techniques de contournement pour éviter le filtrage.

L'objectif de punir les crimes Généralement, le filtrage d'Internet n'a pas pour objectif de punir le crime, étant donné qu'une mesure de filtrage ne supprime pas les contenus d'Internet. Le filtrage d'Internet peut toujours être contourné et ne facilite pas les investigations pour retrouver les producteurs, les distributeurs ou les victimes. Certains pays pourraient décider d'empêcher les gens d'accéder à Internet pour punir un crime ou une infraction. Cette sanction pourrait églament conduire à de la prévention du crime.

Le principe de nécessité dans une société démocratique

Le troisième et dernier principe contenu dans 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* , corresponde à un *besoin social impérieux* et soit "*proportionné au but légitime poursuivi* . Le principe de nécessité implique donc 2 éléments : un besoin social impérieux et la proportionnalité entre l'ingérence et la légitimité du but poursuivi.

Un besoin social impérieux Pour la Cour européenne des droits de l'homme, *l'adjectif nécessaire [] implique l'existence d'un besoin social impérieux* et n'est pas synonyme d'*indispensable*, il na pas non plus la souplesse de termes tels qu'*admissible, normal, utile, raisonnable ou opportun.* Une mesure de filtrage d'Internet doit donc correspondre à un besoin réel de la société et l'efficacité de cette mesure doit être prouvée. De tels besoins sociaux impérieux peuvent comprendre :
- la protection des droits de propriété intellectuelle ;
- la morale et la protection des personnes contre la vision de pédo-pornograhpie ;
- la protection des victimes ;
- la prévention des crimes, y compris empêcher les personnes de devenir pédophiles, déjouer le modèle économique de l'industrie pédo-pornographique, ou empêcher les échanges de pédo-pornographie ;

– la répression du crime.

La proportionnalité au but légitime poursuivi Les ingérences dans les libertés fondamentales causées par les mesures de filtrage d'Internet doivent être proportionnées au but poursuivi, en plus d'être autorisées par la loi, afin de poursuivre un des buts *restrictifs* prévus par la CEDH et considérés comme répondant à un besoin social impérieux. Il existe de nombreux facteurs pour déterminer le juste équilibre dans un cas particulier. Un de ces facteurs est **l'effet global d'une restriction particulière** . Un autre facteur est de savoir **s'il existe une base suffisante permettant de croire qu'un intérêt particulier était en péril** . La Cour européenne des droits de l'homme peut également statuer sur la proportionnalité du *comportement même* qui est restreint.

Le filtrage d'Internet et les critères de proportionnalité

à la lumière de tous les critères analysés ci-dessus, l'analyse de la proportionnalité d'une mesure de filtrage, comparée au but qu'elle poursuit, requiert une distinction claire entre chaque mesure, en se basant sur le but de cette mesure précise.

Le filtrage des pourriels (spam) Le filtrage des pourriels se base sur un danger réel qui menace les services de courriel, lorsque le comportement restreint est le droit d'envoyer des courriels sans respecter les règles établies pour éviter l'arrosage (spam). Cela semble être une ingérence raisonnable, au regard du danger de ne plus pouvoir envoyer de courriel du tout, ou de perdre la confiance des utilisateurs dans le service de courriel. Finalement, il ne semble pas y avoir de mesure moins restrictive qui puisse préserver les objectifs poursuivis par une mesure de filtrage des pourriels.

Le filtrage du web et du P2P *dans l'intérêt de l'industrie de la propriété intellectuelle* Une mesure de filtrage du web ou du P2P, qui servirait l'intérêt des ayants droit, aurait probablement un effet global plus négatif :
– tout d'abord, si le filtrage du P2P peut être présenté comme menant à un chiffrement des échanges rendant toute surveillance ou la plupart des contenus impossible, il deviendrait alors impossible de surveiller ces communications, même dans les conditions où cela est autorisé ;
– ensuite, cela impliquerait des coûts ęllcolorred Élevés pour l'industrie d'Internet, les gouvernements et les internautes ;
– enfin, cela mènerait à coup sûr au filtrage de fichiers légaux.

Au regard du critère qui requiert qu'il existe une base suffisante pour croire que les intérêts des ayants-droits soient en péril , nous pouvons dire qu'il n'y a aucune preuve d'un tel danger. Il n'y a aucune preuve de la nature et de l'étendue des pertes possibles dont souffrent les ayants-droits à cause des infractions commises à l'encontre de leurs droits sur le web ou les réseaux P2P, étant donné que les études sur ce problème sont insuffisantes ou démontrent un résultat inverse.

Le filtrage de contenus illégaux du Web ou du P2P *dans le but de protéger l'image des victimes* Cette proportionnalité semble acceptable vis à vis de l' effet global , tant que la mesure de filtrage n'a pas pour effet de bloquer d'autres contenus. Malheureusement, d'autres contenus seraient probablement bloqués à cause des failles des systèmes de filtrage d'Internet et aussi parce qu'une image de pédo-pornographie peut montrer une scène de crime sans permettre de reconnaître de la victime.

Quant à la base pour croire que l'intérêt des victimes est en péril , leurs intérêts pourraient aussi être satisfaitsen rendant un plus grand nombre de personnes conscientes au sujet du crime subit par la victime, en encourageant les signalements vers les numéros d'urgences et en stimulant la pression croissante des citoyens auprès des gouvernements pour les inciter à agir contre de tels crimes et donc améliorer les investigations et les ressources dédiées aux enquêtes.

La proportionnalité du comportement d'accès à la pornographie infantile peut être analysée à la lumière de l'intérêt du public à identifier ainsi la victime et dépendra de la motivation de chaque personne qui aura vu les contenus. Ces motivations pourraient consister en un désir ou une volonté de voir un crime par curiosité,

ce qui n'est pas approprié ; le désir d'en savoir davantage sur l'existence de tels crimes afin d'agir contre ; ou le désir de signaler de telles images pour enquête.

Le filtrage des contenus illégaux du Web ou du P2P *dans le but de protéger la morale* ou *dans le but de protéger les intérêts des personnes sensibles* Une mesure de filtrage pourrait conduire à empêcher ces personnes d'accéder à des contenus non controversés, à cause des faiblesses des mécanismes techniques. De plus cela n'empêcherait pas les criminels d'y avoir accès. Il en résulterait notamment que l'effet global serait une réduction du droit à la liberté d'expression, tandis que les criminels auraient toujours accès aux contenus immoraux ou choquants et les usagers pourraient toujours avoir accès à des contenus immoraux ou choquants d'autres sortes. Une telle situation ne serait pas proportionnée.

Le filtrage des contenus illégaux du web ou du P2P *dans le but de la prévention du crime* L'objectif de la prévention du crime devrait être d'empêcher les gens de commettre des crimes ou délits ou d'en être complices en achetant, téléchargeant ou vendant des, contenus illégaux. Sa proprotionnalité dépendrait de l'équilibre trouvé entre, d'une part, le pourcentage de la population qui ne commettrait plus de délits puisque n'ayant plus accès aux contenus illégaux et, d'autre part, les restrictions des libertés publiques que causerait la mesure. L'effet de la mesure ne devrait pas être une réduction significative de la liberté d'expression ni du droit à la vie privée de chaque citoyen. Il n'existe pour l'instant aucune preuve qu'une mesure de filtrage pourrait aboutir à une diminution des crimes et délits, alors qu'elle restreindrait certains comportements légitimes et proportionnés.

Filtrer l'accès d'une personne à internet *dans le but de la prévention et de la répression du crime* L'effet global de filtrer une personne dans le but de la répression et de la prévention du crime est d'empêcher cette personne d'accéder à Internet et parfois d'accéder aux services téléphoniques et télévisuels. Un tel effet est redoutable puisqu'il s'agit de priver complétement une personne de sa liberté de recevoir et de communiquer des informations électroniques, de sa liberté de jouir de sa vie privée et familiale et de sa liberté de correspondance, dans le monde électronique. Cette mesure ne peut être proportionnée que si elle est justifiée par le crime commis et l'objectif poursuivi à travers sa répression ou bien entendu sa prévention.

Les conséquences supplémentaires du principe de stricte nécessité des ingérences

Des ingérences supplémentaires sont permises par plusieurs mesures de filtrage d'Internet, à cause de la nature des mécanismes installés pour mettre en œuvre le filtrage. Par exemple, certains mécanismes de filtrage des pourriels permettent à un FAI d'analyser chaque message envoyé ou reu, ce qui provoque d'autres ingérences telles que la conservation de données personnelles en relation avec un message entier ou à certains mots du contenu.

La proportionnalité de chaque mesure qui s'immisce dans des libertés doit être évaluée tout d'abord en fonction de son but déclaré, puis en fonction de son effet global, qui ne doit pas aller au-delà ce qui est nécessaire pour atteindre l'objectif poursuivi et, dans tous les cas, qui doit ***laisser du champ libre*** **pour l'exercice de la liberté restreinte et ne pas *éteindre* cette liberté.**

Chaque fois qu'une mesure de filtrage d'Internet est permise, certaines garanties doivent être prises pour empêcher ces mesures de filtrage d'être utilisées d'une manière qui compromettrait davantage les libertés au-delà de ce qui est nécessaire pour atteindre l'objectif annoncé. C'est nécessaire même si la mesure poursuit un but légitime et si sa fonction de base n'entrave pas d'autres libertés de manière disproportionnée. La mesure peut présenter l'un des risques soulignés dans cette sous-section. Ces garanties peuvent être techniques, en gardant sous contrôle les fonctionnalités qui autoriseraient la compromission de libertés additionnelles, ou juridiques, en prohibant les fonctionnalités additionnelles ou leur usage, lorsqu'ils ne sont pas essentiels au fontionnement du mécanisme de filtrage. Un juge doit à chaque fois être autorisé à évaluer la proportionnalité de toute mesure de filtrage spécifique.

La compétence du juge dans l'examen de la proportionnalité des ingérences dans les libertés fondamentales

La Cour européenne des droits de l'homme supervise les mesures, prises par les états signataires, s'immiscant dans les libertés fondamentales et leur appréciation par les juges nationaux. Les tribunaux nationaux sont également habilités à rendre un jugement sur des différends relatifs à une mesure de filtrage dont un citoyen aurait fait l'objet ou à un contenu que ce citoyen aurait désiré envoyer, recevoir ou consulter.

Si avoir le droit d'attaquer devant un tribunal une décision qui limite une des libertés est un droit fondamental, cela suppose que cette limitation a déjà été mise en place et que le citoyen a déjà subi ses effets. Par conséquent, il est essentiel qu'un juge puisse intervenir avant qu'une telle décision de filtrage ne soit prise. En ce qui concerne le filtrage d'Internet, ces situations sont tout d'abord relatives à l'estimation et la déclaration d'illégalité d'un contenu ou d'une action, puis à l'appréciation de la proportionnalité de la réponse apportée à la situation illégale.

Comme vu ci-dessus et détaillé au chapitre 7 du rapport complet, il semble que les seules mesures de filtrage d'Internet qui devraient être autorisées sans obtenir une décision d'une cour de justice sont le *filtrage des pourriels* et le *filtrage dans le but de protéger la morale*, bien que ce dernier implique une série d'autres objections d'ordre juridique et pratique.

Les conditions sous lesquelles le filtrage d'Internet pourrait être acceptable.

Les démocraties libérales doivent respecter les libertés fondamentales et la Cour des droits de l'homme fixe les conditions de leur limitation. Les mesures de filtrage d'Internet ne peuvent être mises en œuvre correctement que si les étapes suivantes sont respectées.

Étape 1 Le filtrage d'Internet nécessiterait d'être mis en œuvre de manière à ce que d'autres droits et libertés ne soient pas violées.

Étape 2 Déterminer les droits et les libertés qui seront limités.

Étape 3 Déterminer l'étendue de la limitation.

Étape 4 Déterminer précisément le(s) objectif(s) poursuivi(s).

Étape 5 établir si le but du filtrage correspond à la réalité.

Étape 6 Déterminer si le filtrage pour l'objectif déterminé répond à un besoin social impérieux.

Étape 7 Analyser la proportionnalité de l'ingérence à l'objectif poursuivi.

Étape 8 Considérer les principes qui doivent gouverner le filtrage à la lumière des critères de la Cour européenne (nécessité dans une société démocratique, besoin social impérieux).

Étape 9 établir si une loi est nécessaire pour empêcher l'utilisation de certaines fonctionnalités du mécanisme de filtrage.
Étape 10 Fournir un système de filtrage dans le cadre de la loi.

Études requises

Durant le cadre de la recherche d'équilibre entre libertés fondamentales, plusieurs études ont été identifiées comme nécessaires pour obtenir une évaluation suffisante des exigences de proportionnalité. En l'absence de cette recherche, la proportionnalité ne peut être démontrée. Ces études comprennent :
– filtrage d'Internet et prévention de la pédo-pornographie ;
– déjouer le modèle économique du commerce de pédo-pornographie ;
– filtrage d'Internet réduisant les échanges de pédo-pornographie ;

– filtrage d'Internet protégeant les personnes ou la morale ;
– filtrage d'Internet protégeant les intérêts des victimes ;
– filtrage des intérêts protégeant les droits de propriété intellectuelle.

0.7 Conclusion

Étant donné les répercussions fondamentales sur nos droits à communiquer librement, nos sociétés ont urgemment besoin de prendre conscience de l'impact des activités de filtrage d'Internet, même si la compréhension commune du filtrage d'Internet semble, à première vue, assez claire. Il existe de nombreuses motivations bien intentionnées pour lesquelles une société envisage d'imposer des mesures de filtrage d'Internet, mais le respect des droits de l'homme et les questions juridiques, politiques et techniques sont très complexes. Les cas où des tentatives de filtrage ont été mises en œuvre, ont souvent engendré de la frustration et de la confusion autour de l'efficacité et même du ou des objectifs de tels systèmes. Le filtrage d'Internet a également un effet majeur sur la protection de la vie privée et la sécurité de tous les citoyens. Le présent rapport examine la signification du filtrage d'Internet et en envisage les conséquences pratiques et juridiques.

Il décrit les motivations des tentatives de filtrage d'Internet et la façon dont d'autres approches semblent échouer. Il examine qui effectue le filtrage, ce qui pourrait être filtré, comment l'on peut appréhender le filtrage et qui pourrait être la cible des tentatives de filtrage d'Internet.

Un passage en revue technique des principaux systèmes de filtrage d'Internet utilisés de nos jours, et la façon dont ils s'appliquent à différents services en ligne, soulignent la gamme croissante des contenus et des services qu'on envisage de filtrer. Une analyse de l'efficacité des systèmes de filtrage d'Internet met en évidence de nombreuses questions sans réponse à propos du succès de ces systèmes et de leur capacité à atteindre les objectifs qu'on leur assigne. Presque tous les systèmes ont un impact technique sur la capacité de résistance d'Internet et ajoutent un degré supplémentaire de complexité à un réseau déjà complexe. Tous les systèmes de filtrage d'Internet peuvent être contournés et quelquefois, il suffit de modestes connaissances techniques pour le faire. Il existe des solutions logicielles largement disponibles sur Internet qui aident à échapper aux mesures de filtrage.

Une synthèse complète sur le filtrage d'Internet et le droit, en particulier à propos des droits de l'Homme, des libertés fondamentales et des libertés publiques, suscite des interrogations substantielles sur les systèmes de filtrage couramment mis en œuvre. Le volet juridique de l'analyse examine les instruments nationaux et internationaux, se demande quels droits fondamentaux sont en contradiction avec le filtrage d'Internet et quels droits fondamentaux viennent l'étayer. La complexité du respect de l'équilibre entre des droits contradictoires rend nécessaire que des juges s'en saisissent, car ils ont la compétence pour gérer de telles complexités.

Les fournisseurs d'accès à Internet sont des entités à but lucratif qui sont de plus en plus sollicitées pour mettre en œuvre une politique qui touche la société sans les garanties adéquates qu'on les supervise ou sans qu'ils aient à rendre des comptes. Elles opèrent dans une situation très confuse en ce qui concerne des exigences juridiques concurrentes et parfois contradictoires. Par exemple, il faut d'un côté procurer de hauts niveaux de qualité d'accès à Internet, et de l'autre filtrer l'accès à certains services.

Le problème crucial pour respecter un équilibre entre des libertés fondamentales, lorsque différents droits entrent en conflit, doit faire l'objet d'une analyse détaillée, à l'image de celle qu'a initiée la Cour européenne des droits de l'homme : celle-ci peut fournir indirectement des directives pour savoir comment les mesures de filtrage d'Internet peuvent être mises en œuvre lorsqu'elles sont appropriées, proportionnées et techniquement réalisables. Cette analyse nécessite de prendre en considération la clause stricte d'ordre public et les principes de nécessité dans une société démocratique. Ces principes sont alors appliqués à différentes initiatives de filtrage en examinant leurs objectifs et comment ils peuvent être jugés en utilisant les directives de la Cour européenne des droits de l'homme. Le présent rapport examine les buts légitimes des initiatives de filtrage d'Internet et met en doute la validité de certains dispositifs en usage aujourd'hui.

La mise en œuvre technique des mesures de filtrage d'Internet ne peut exister indépendamment d'un environnement et doit prendre en considération son impact réel sur le crime ou le délit qu'elles visent à empêcher.

On doit également tenir compte de l'exactitude et de l'efficacité de la mesure de filtrage et identifier clairement les conséquences négatives sur le contenu légal et les usages légaux d'Internet. L'évaluation de l'efficacité technique doit être clairement introduite dans l'évaluation de l'équilibre des droits.

De nombreuses mesures de filtrage sont faciles à contourner et par conséquent totalement inefficaces pour un grand nombre d'objectifs déclarés. De façon inattendue, un des systèmes auquel il est le plus facile d'échapper, soit intentionnellement soit accidentellement, est le filtrage par DNS, qu'utilisent aujourd'hui un grand nombre de systèmes de filtrages nationaux. Il est notoire qu'il existe des frustrations significatives au sujet de l'absence d'efficacité de la coopération internationale actuelle contre le cybercrime et également en raison du manque de réactivité de certains pays face aux crimes et délits tels que la pédo-pornographie, l'incitation à la haine et le terrorisme. Toutefois, plutôt que de baisser les bras et d'avoir recours à des stratégies nationales protectionnistes, nous avons besoin d'améliorer ces systèmes internationaux et les rendre efficaces au XXIe siècle.

Il existe très peu de dispositifs de filtrage d'Internet actuellement mis en œuvre qui soient issus de débats publics sérieux animés de façon transparente et responsable. Puisqu'il existe des problèmes complexes sur le plan juridique et sur celui des droits de l'homme, qui peuvent avoir une influence sur l'adoption de services de filtrage d'Internet, ce rapport a préconisé une suite d'étapes à suivre pour évaluer la légitimité des propositions de filtrage d'Internet dans une société démocratique.

Il est curieux que des contenus illégaux tels que la pédo-pornographie, qui est largement illégale dans de nombreux pays, et particulièrement des contenus qui sont universellement condamnés par la morale[7] et presque universellement illégaux, soient autorisés à rester disponibles en ligne à l'accès ou au téléchargement par des utilisateurs. Il est également étrange que les gouvernement autorisent et encouragent des industries privées et des représentants non-élus à mettre en œuvre des filtrages étendus de contenus de façon opaque et sans obligation de rendre de comptes. Après les recherches et les analyses juridiques adéquates, si le filtrage est adopté, il est du ressort du pouvoir législatif de préciser clairement ce qui peut être filtré sur Internet, comment cela peut être fait et comment de tels systèmes devraient être évalués et rendre publiquement des comptes. Il est surprenant que de nombreux gouvernements de l'UE, qui sont incapables de légiférer directement en faveur du filtrage d'Internet, continuent à encourager et à soutenir les initiatives de l'industrie dans ce domaine. Ironiquement, il arrive parfois que les listes noires de ces pays soient élaborées pour l'activité de filtrage par des organisations financées par l'état, sans évaluation indépendante de ces listes.

Ce qu'il faut prendre le plus en considération pour tout filtrage d'Internet est la proportionnalité. La mesure prise doit avoir proportionnellement davantage d'effets négatifs sur les contenus illégaux et les activités criminelles sur Internet que sur les contenus légaux et les activités légales. Une telle mesure doit être prévue par la loi et mise en œuvre de telle sorte que d'autres droits et libertés ne soient pas violés.

En bref, le filtrage d'Internet est conu avec des solutions techniques qui sont elles-mêmes inadéquates et sont sapées par la disponibilité de protocoles alternatifs permettant d'accéder à du matériel illégal et de le télécharger. Il en résulte que l'estimation du caractère proportionné des mesures ne doit pas seulement respecter l'équilibre des divers droits en jeu, mais aussi garder à l'esprit l'incapacité des technologies de filtrage à préserver les droits en question, ainsi que les risques d'effets pervers, tels qu'une diminution de la pression politique pour rechercher des solutions complètes, ou le risque d'introduction de nouvelles stratégies chez les fournisseurs de sites illégaux pour éviter le filtrage, ce qui rendrait à l'avenir plus difficiles encore les enquêtes pénales.

Les résultats de la présente étude montrent que les difficultés pratiques, techniques et juridiques entourant le filtrage confirment que le problème ne se limite pas à un simple choix filtrer ou ne pas filtrer . Les pays qui ont déjà mis en œuvre différents types de procédés de filtrage et ceux qui envisagent de le faire doivent prendre deux mesures concrètes :

[7] Ainsi, le 7 décembre 2008, 193 pays ont ratifié la Convention des droits de l'enfant des Nations unies, ce qui comprend tout les pays membres des Nations unies, à l'exception des états-Unis et de la Somalie. Cependant, même les USA disposent d'une législation condamnant la pédo-pornographie.

- Envisager que le filtrage soit un des choix possibles revient à reconnaître, sinon à accepter implicitement, les échecs de la coopération internationale sur un problème de dignité humaine fondamentale et de protection des personnes les plus vulnérables de nos sociétés (dans la mesure où il s'agit de pédo-pornographie sur Internet).
  Une analyse correcte de la nature exacte de cet échec est nécessaire pour mieux résoudre le problème. Sur la base de cette analyse, tous les pays devraient fournir des rapports officiels sur leurs efforts pour satisfaire l'article 34 de la Convention des droits de l'enfant des Nations unies, qui devraient être publiés chaque année et incorporés aux rapports établis périodiquement aux termes de l'article 44 de cette Convention. Cela inciterait les états à devenir plus actifs dans ce domaine et aurait pour conséquence de retirer un plus grand nombre de sites de l'accès public et de soustraire davantage d'enfants à des situations de maltraitance.
- Une analyse de l'impact concret (de l'accès par inadvertance, de l'accès délibéré, du commerce de la pédo-pornographie et de l'usage de méthodes alternatives de diffusion de contenus illégaux) est possible et nécessaire, en utilisant les données issues des systèmes de filtrage existants. Sans cette analyse, la proportionalité du filtrage et par conséquent sa légalité au regard des instruments principaux des droits de l'homme reste largement discutable. L'incapacité à mener de telles analyses suscite une interrogation persistante sur l'engagement de nombreux pays envers les principes fondamentaux de l'état de droit.
- Les dispositifs de filtrage nécessitent d'être mis en œuvre à travers des législations nationales ou sinon ne pas être mis en œuvre du tout. Les systèmes de filtrage auto-régulés n'ont ni la transparence appropriée ni la capacité de rendre compte adéquate.