Le Forum des droits sur l'internet

RECOMMANDATION

Les enfants du Net III

Conditions nécessaires à la mise en place du filtrage des sites pédopornographiques par les FAI

29 octobre 2008

www.foruminternet.org

Le Forum des droits sur l'internet
6, rue Déodat de Séverac 75017 PARIS

INTRODUCTION

Le Forum des droits sur l'internet, dont les travaux sur la protection de l'enfance menés en 2004 et 2005 avaient tissé un susbtrat commun aux acteurs publics et privés, a relancé sa réflexion sur ce thème en 2007. Un groupe de travail composé de représentants des pouvoirs publics, des professionnels du secteur de l'internet et des représentants de la société civile a été formé. Parmi les réflexions du groupe de travail, la question du filtrage des sites pédopornographiques au niveau de l'accès à l'internet a été largement débattue.

Dans le même temps, les pouvoirs publics ont témoigné de leur intérêt sur cette question à travers, notamment, des actions de lutte contre la cybercriminalité menées par Mme Alliot-Marie, ministre de l'Intérieur ou des discussions menées par Madame Nadine Morano, secrétaire d'État chargée de la Famille.

Dans ce contexte, le Forum des droits sur l'internet a souhaité fournir une recommandation sur les conditions nécessaires à la mise en place du filtrage des sites pédopornographiques par les FAI dans l'éventualité où la volonté des pouvoirs publics se confirme en ce sens. Cette recommandation a fait l'objet d'une consultation auprès de l'ensemble des membres du Forum des droits sur l'internet du 7 au 21 octobre 2008. Elle a été définitivement adoptée par le Conseil d'orientation du Forum des droits sur l'internet le 29 octobre 2008.

I. – CONTEXTE

En matière de sites internet contenant des images ou représentations d'abus sexuels sur mineurs, les services de police et de gendarmerie et la justice ont une capacité forte à traiter le cas des sites hébergés et accessibles sur le territoire français.

De plus, conformément aux dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, les hébergeurs français doivent retirer de leurs serveurs les sites internet contenant des images ou représentations d'abus sexuels sur mineurs dès qu'ils ont connaissance de leur existence (article 6 I 2 LCEN), et ce d'autant plus qu'il s'agit de contenus « manifestement » illicites compris dans le champ de l'article 6 I 7 al.3 de la LCEN, lequel vise aussi une obligation de signalement de ces contenus auprès des autorités publiques lorsqu'elles en ont connaissance.

Il en va différemment des sites hébergés et édités à l'étranger, malgré l'existence d'accords internationaux sur cette question, les demandes de retrait effectuées auprès de l'éditeur et de l'hébergeur restant, dans ces derniers cas, largement insatisfaites par certains hébergeurs.

Dès lors, et s'agissant des sites hébergés à l'étranger, le filtrage des sites contenant des images ou représentations d'abus sexuels sur mineurs apparaît comme un levier supplémentaire permettant de lutter contre ce type de contenu. Une telle mesure permettrait également d'éviter leur banalisation. Par ailleurs, ces sites étant souvent de nature commerciale, cela limiterait leur accès à un potentiel marché français.

Dans certains États, notamment européens, les fournisseurs d'accès ont accepté de pratiquer un filtrage volontaire de ces sites. Dans ces pays, les mesures de filtrage portent sur des listes pouvant contenir plusieurs milliers d'adresses, mises à jour en permanence. En France, les fournisseurs d'accès ne sont pas opposés au principe même du filtrage de l'accès. Ils estiment toutefois que la mesure présente plusieurs risques et pourrait s'avérer inefficace, disproportionnée et coûteuse. Les opérateurs fixes et mobiles souhaitent mettre en exergue le fait que la mise en œuvre d'un tel dispositif sur leurs réseaux peut vraisemblablement avoir un impact négatif en termes de qualité de service. Ils considèrent en outre les caractéristiques des infrastructures réseau ainsi que le cadre juridique national actuellement en vigueur comme des obstacles à la mise en place d'un filtrage proactif et volontaire.

Ces acteurs se sont néanmoins toujours sentis extrêmement concernés par la protection de l'enfance sur l'internet et se sont fortement mobilisés sur ce sujet à travers des actions pédagogiques envers les internautes, la fourniture de solutions gratuites de contrôle parental, la mise en place d'un point de contact permettant aux internautes de leur signaler les contenus en ligne attentatoires à la dignité humaine et la participation au réseau INHOPE (Fédération internationale de services d'assistance en ligne). L'action menée dans le cadre du « point de contact » témoigne du haut degré de coopération déjà existant avec les services spécialisés des forces de l'ordre.

Des réponses existent donc déjà mais elles ne sont pas sans poser de problèmes en matière de lutte contre la pédopornographie diffusée sur des sites hébergés à l'étranger. Ainsi, la protection par le biais de logiciels installés par le client sur son poste (sur le modèle des logiciels de contrôle parental) ne semble pas cohérente avec l'objectif de limiter l'accès de l'ensemble de la population française aux sites contenant des images ou représentations d'abus sexuels sur mineurs. En effet, même s'il faut naturellement inciter à leur généralisation, l'installation de ces logiciels repose sur une base volontaire et il s'avère utopique de pousser l'ensemble de la population internaute française à installer de telles solutions sur ses ordinateurs. Des débats portent aussi sur les risques de sécurité évidents en cas de communication de la liste des pages recensées par les

services de police et de gendarmerie aux éditeurs de listes blanches et noires. Si le principe d'un filtrage au niveau de l'accès était retenu, une telle communication deviendrait superflue. Enfin, il convient de noter que le filtrage par l'installation d'un logiciel n'est actuellement pas envisageable pour les téléphones mobiles, en raison de la capacité de calcul embarquée dans les terminaux jugée insuffisante pour permettre une expérience de navigation sous contrôle parental raisonnablement satisfaisante.

Compte tenu de ces limites et de la volonté partagée par l'ensemble des acteurs d'améliorer le dispositif de lutte, l'objectif du groupe de travail du Forum des droits sur l'internet est de réfléchir à un cadre juridique et technique « acceptable » par l'ensemble des acteurs, permettant d'obtenir des résultats probants, en matière de filtrage au niveau de l'accès des sites contenant des images ou représentations d'abus sexuels sur mineurs.

II. – OBJECTIFS DE LA MESURE

Il est important à ce stade de préciser l'objectif du dispositif de filtrage des sites contenant des images ou représentations d'abus sexuels sur mineurs, car il implique d'importantes conséquences sur le mécanisme juridique à retenir.

Ainsi, il est nécessaire d'opérer une distinction entre les mesures destinées à constater les infractions au droit pénal, à en rassembler les preuves ou à en rechercher les auteurs et celles qui n'ont d'autre finalité que de prévenir les infractions et de préserver l'ordre public.

C'est ce deuxième objectif qui sert de base aux réflexions du groupe de travail du Forum des droits sur l'internet.

Dans cette optique, le filtrage permettrait de lutter contre les expositions à des sites pédopornographiques non intentionnelles, ou incitées via des sites eux-mêmes légaux (par exemple via certains sites pornographiques), et les expositions dues à des renvois via des hyperliens (notamment dans le cadre de spams) ou par de la publicité. Il rendrait également plus difficile (mais pas impossible) la consultation volontaire de ces mêmes sites. Cette mesure peut aussi contribuer à la sensibilisation de ceux qui seraient tentés de se connecter à des sites pédopornographiques par simple curiosité, si le choix d'un renvoi vers une page d'information sur le dispositif est fait.

Un tel filtrage ne permet donc pas de lutter directement contre les contenus visés, ni d'en rechercher les auteurs et les victimes. Cela est du domaine des services spécialisés de police et de gendarmerie et s'effectue dans le cadre d'une coopération internationale. Les sites, eux, continuent d'exister. Ces solutions sont en revanche un moyen d'en réduire la visibilité, d'en limiter l'accès involontaire et de complexifier les accès volontaires.

En conséquence, les parties prenantes doivent comprendre que les solutions de filtrage constituent un levier supplémentaire dans la lutte contre les sites édités ou hébergés à l'étranger, mais qu'elles ne doivent ni remplacer le travail de lutte contre les auteurs et éditeurs de ces contenus, ni légitimer un affaiblissement des actions de sensibilisation des internautes, notamment en termes de responsabilité parentale.

Les opérateurs de services de communications électroniques mettent en avant le risque de perte d'efficacité de la mesure du fait du développement et de la diffusion de moyens de contournement. Les filtres mis en place sont, en effet, contournables par un internaute avisé et par les éditeurs des sites litigieux, ce qui révèle la faillibilité technique du filtrage et peut faire redouter la création d'une illusion de sécurité pour les utilisateurs.

Ils insistent également sur la lourdeur de la mise en œuvre de ces systèmes au regard des infrastructures des opérateurs, fixes et/ou mobiles, tant au niveau technique qu'économique.

Ces précisions effectuées, un certain nombre de problématiques doivent être étudiées dans la perspective d'une mise en œuvre de telles mesures de filtrage parmi lesquelles :

- les implications sur la liberté d'expression et de communication ;
- les débats sur les solutions techniques ;
- le choix d'une architecture juridique ;
- …

III. – SCÉNARIOS JURIDIQUES

Préalable :

L'architecture juridique mise en place doit garantir aux FAI le respect de leur neutralité et de la prohibition d'imposer des mesures générales de surveillance des contenus qui transitent par leurs infrastructures[1].

En l'état actuel du droit, l'article 12 de la directive 2000/31/CE du 8 juin 2000 dite « commerce électronique » limite les conditions d'engagement de la responsabilité des fournisseurs d'accès du fait des informations transmises par leur intermédiaire. L'article 12 §3 précise toutefois que ces règles n'affectent pas « la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation ».

La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a transposé le texte communautaire en droit français. L'article 6. I. 8 de la loi confie à « l'autorité judiciaire » le pouvoir de « prescrire en référé ou sur requête [aux prestataires de services d'hébergement] ou, à défaut, [aux fournisseurs d'accès] toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ». En 2004, le législateur n'a pas utilisé la faculté offerte aux États de confier à l'autorité administrative le pouvoir de prendre de telles mesures et l'a réservé à la seule autorité judiciaire.

Quelle que soit la technique de filtrage retenue, dans l'hypothèse où une telle mesure serait considérée comme pertinente par les pouvoirs publics, il est essentiel de prémunir les éditeurs de sites conformes à la loi contre un blocage abusif de leur site. Ainsi l'architecture juridique devant préalablement être mise en place doit nécessairement garantir des possibilités de recours à bref délai pour les titulaires de sites abusivement bloqués ainsi que les prémunir contre une action ultérieure de leurs propres clients du fait de ce blocage.

Le présent document évoquera successivement deux pistes, à savoir un filtrage opéré en tant que mesure judiciaire (A) et un filtrage opéré en tant que mesure administrative (B).

[1] Article 6-I-7 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : *« Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites(…) »*

A. – Le filtrage comme mesure judiciaire

La loi du 21 juin 2004 pour la confiance dans l'économie numérique, dans son article 6.I.8, prévoit une procédure spécifique lorsque la priorité est d'empêcher ou de faire cesser le trouble occasionné par un contenu illicite[2].

Afin qu'un juge puisse ordonner une mesure de filtrage aux fournisseurs d'accès, il est souhaitable d'avoir au préalable accompli les diligences nécessaires auprès de l'éditeur et de l'hébergeur du site incriminé. Ce n'est que lorsque cette procédure s'est avérée vaine que le juge peut imposer une mesure de filtrage aux fournisseurs d'accès.

Si l'on comprend aisément le but de cette disposition, surtout eu égard à des solutions de filtrage trop larges et susceptibles de bloquer l'ensemble d'un serveur, force est de constater que *la procédure judiciaire, parfois longue, semble peu adaptée* à l'objectif que la France pourrait se donner d'empêcher l'accès à des contenus pédopornographiques. Ces derniers ont en effet, la plupart du temps, une durée de vie extrêmement brève et sont majoritairement consultés dans les premières heures suivant leur mise en ligne.

Le tribunal de grande instance de Paris avait rappelé dans une ordonnance du 25 mars 2005 (Affaire « Aaargh », TGI Paris, 25 mars 2005) que le principe était d'assigner en priorité les fournisseurs de contenu et d'hébergement.

Toutefois la Cour de cassation, dans son arrêt du 19 Juin 2008 est venue confirmer l'arrêt d'appel (affaire « Aaargh », CA Paris, 24 novembre 2006) en précisant que la prescription des mesures de filtrage n'était « pas subordonnée à la mise en cause préalable des prestataires d'hébergement ». Le déclenchement de la procédure de filtrage des sites contenant du matériel pédopornographique gagne donc en réactivité en permettant au juge, dans le cadre du référé LCEN, d'ordonner directement au FAI la mise en place de « toutes mesures propres à interrompre l'accès à partir du territoire français au contenu du service de communication en ligne ».

Néanmoins, cette solution nécessiterait, conformément au système juridique français actuel, de saisir l'autorité judiciaire à chaque fois qu'une mesure de filtrage est nécessaire, et d'appeler à la procédure l'ensemble des fournisseurs d'accès français. Si le recours à une juridiction est la solution actuellement prévue par le droit positif national, il présente une faiblesse en termes de réactivité et semble inadapté à l'objectif de bloquer une liste importante de sites pédopornographiques hébergés à l'étranger et se déplaçant en permanence. En effet, une liste de plus en plus volumineuse de pages, mise à jour en temps réel, devrait être fournie par les forces de police et de gendarmerie.

La publicité des décisions suscite également des inquiétudes. Ainsi dans l'affaire Aaargh, cela a apporté une exposition supplémentaire aux contenus incriminés. Il convient néanmoins d'opérer une distinction entre la publicité des débats pour laquelle des dérogations sont envisageables et la publicité de la décision. Toutefois, la non publicité des adresses concernées, au sein des décisions de justice, éviterait d'apporter un éclairage inopportun sur ce type de site.

Il ressort nettement que le cadre juridictionnel s'avère actuellement trop étroit pour permettre à un dispositif de filtrage relatif à des sites contenant des images ou représentations d'abus sexuels sur mineurs d'être réellement efficace.
Afin de rendre le dispositif plus réactif et homogène, il pourrait cependant être envisagé de limiter le recours à certaines juridictions détenant une compétence spécialisée.

[2] Art. 6. I.8 LCEN du 21 Juin 2004 : « *L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.* »

B. – Le filtrage comme mesure administrative

1. – Le recours à une mesure administrative

Au-delà du recours au juge, il est possible de considérer la mesure de filtrage comme relevant d'une opération de police administrative.

Les mesures de police administrative relèvent de la seule responsabilité du pouvoir exécutif et ne peuvent avoir d'autre finalité que de préserver l'ordre public et de prévenir les infractions. Elles se distinguent en cela des opérations de police judiciaire qui sont destinées à constater les infractions à la loi pénale, à en rassembler les preuves et à en rechercher leurs auteurs.

La mesure de filtrage étant conçue comme permettant de prévenir la commission d'une infraction, elle semble donc entrer dans le champ dévolu aux opérations de police administrative.

Pour autant, il est régulièrement mis en avant qu'une procédure de cet ordre, n'étant pas placée sous la surveillance de l'autorité judiciaire, pourrait porter atteinte à des libertés individuelles et notamment à la liberté d'expression et de communication. Ce débat a d'ores et déjà eu lieu s'agissant notamment d'interceptions de sécurité (loi n°91-646 du 10 juillet 1991) ou encore des procédures de réquisitions administratives de données techniques de connexion dans le cadre de la loi relative à la lutte contre le terrorisme (loi n°2006-64 du 23 janvier 2006).

Cette solution serait notamment compatible avec l'article 12 § 3 de la directive commerce électronique, sous réserve que la législation nationale évolue et prévoit une dérogation expresse à l'article 6. I. 8 de la loi pour la confiance dans l'économie numérique (Voir supra page 7).

a. – Débat sur la notion de liberté d'expression

Au niveau européen, si l'article 10 de la CEDH met en avant le principe de la liberté d'expression, il dispose également que « l'exercice de [cette liberté] comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, 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 ».

Des limitations au principe même de la liberté d'expression sont donc acceptables dans certains cas particulièrement graves et peuvent ainsi notamment justifier l'adoption de mesures préventives lorsque les restrictions sont prévues par la loi, visent un but légitime et répondent à un besoin social impérieux[3].

En France, l'article 66 de la Constitution dispose : « Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi ».
S'il ne fait aucun doute que la police administrative est susceptible d'affecter la liberté de la personne, la publication des Cahiers du Conseil Constitutionnel[4] a néanmoins été

[3] Voir notamment CEDH, 8 juillet 1986
[4] Voir Cahiers du Conseil Constitutionnel n° 20 relatif à la décision n°2005-532 DC du 19 janvier 2006.

l'occasion de rappeler que « la vision assimilant toute restriction de la liberté personnelle (du fait de la police administrative) à une atteinte à la liberté individuelle au sens de l'article 66 de la Constitution (appelant par conséquent le contrôle préalable de l'autorité judiciaire) se heurterait à de manifestes impossibilités pratiques. (…) La liberté individuelle (au sens de l'article 66 de la Constitution) s'entend de la liberté de ne pas être arbitrairement détenu (« habeas corpus »). Les autres composantes de la liberté personnelle sont protégées par d'autres normes constitutionnelles (….) Sauf en matière de détention, ou lorsqu'une législation républicaine constante le prévoit dans des cas spécifiques (perquisitions…), ces normes n'imposent pas nécessairement l'intervention du juge judiciaire. »

Ainsi, si la liberté d'expression est protégée par l'article 11 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789, une mesure administrative portant atteinte à ce principe n'appelle pas nécessairement le recours au juge judiciaire, mais doit être entourée de garanties fortes. La mesure de filtrage envisagée touchant non seulement à une liberté individuelle mais également à une liberté collective, cette nécessité parait d'autant plus renforcée.

b. – Garanties nécessaires

S'il appartient au législateur de concilier la prévention des atteintes à l'ordre public et l'exercice de la liberté d'expression et de communication, celui-ci a déjà eu l'occasion d'assortir la procédure administrative de limitations et précautions, notamment dans le cadre de l'article 6 de la loi relative à la lutte contre le terrorisme. Ces garanties ont été jugées suffisantes par le Conseil Constitutionnel[5].

En l'espèce, s'inspirant du dispositif en vigueur en matière « d'interceptions de sécurité », le législateur a :

- Limité la possibilité d'exiger la communication des données aux « seuls agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions ».

- Limité la liste des données susceptibles d'être communiquées.

- Obligé à ce que les demandes des agents soient « motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'Intérieur. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'Intérieur qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les demandes, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

  Cette instance peut à tout moment procéder à des contrôles relatifs aux opérations de communication des données techniques. Lorsqu'elle constate un manquement aux règles définies par le présent article ou une atteinte aux droits et libertés, elle saisit le ministre de l'Intérieur d'une recommandation. Celui-ci lui fait connaître dans un délai de quinze jours les mesures qu'il a prises pour remédier aux manquements constatés. »

- Assuré que les personnes ayant un intérêt à agir ne soient pas privées de leur droit au recours.

[5] Voir notamment décision n° 2005-532 DC

S'inspirant de ces éléments, il est possible de transposer la réflexion aux mesures de filtrage des sites contenant des images ou représentations d'abus sexuels sur mineurs.

2. – Garanties de mise en œuvre

La demande de filtrage effectuée, comme mesure de police administrative, suppose l'intervention de quatre étapes distinctes :

1. Le travail effectif des forces de police et de gendarmerie pour identifier les sites pédopornographiques. Cette identification repose également sur les signalements opérés par les internautes et sur la coopération internationale puisque, par exemple, près de 60 % des sites pédopornographiques sont actuellement hébergés aux États-Unis[6].

2. La constitution d'une liste de sites à filtrer par les forces de police et de gendarmerie, mission actuellement confiée à l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), et l'envoi de cette liste à une « autorité nationale compétente ». (Canal unique).

3. La validation de la liste par l'autorité nationale compétente, seule habilitée à transmettre la liste aux opérateurs de communication électronique et à leur demander de procéder au filtrage de ces sites au niveau de l'accès. (Canal unique).

4. Le contrôle a posteriori de la procédure et des blocages de sites requis par l'autorité nationale compétente, ainsi que la fourniture d'une voie de recours.

Ce dispositif nécessite un certain nombre de garanties de mise en œuvre :

- que l'objectif de la mesure reste la seule préservation de l'ordre public pour faire cesser un trouble existant, fût-il susceptible d'être constitutif d'infraction, et la prévention des infractions. Toute demande de filtrage ayant pour but de réprimer une infraction, d'en conserver des preuves ou d'en rechercher les auteurs, ne saurait entrer dans le cadre de la mesure de police administrative et nécessiterait l'intervention du juge judiciaire. C'est bien en ce sens qu'il faut interpréter la censure partielle de l'article 6 de la loi relative à la lutte contre le terrorisme par le Conseil Constitutionnel qui a requis l'abandon de l'objectif de « répression » initialement prévu dans le texte.

- que la possibilité de transmettre la liste de sites à filtrer à l'autorité soit limitée aux « seuls agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions »

- que les demandes de filtrage soient strictement limitées aux sites contenant des images ou représentations d'abus sexuels sur mineurs.

- que les modifications législatives nécessaires soient effectuées dans le cadre d'une loi spécifique à la lutte contre la pédopornographie sans extension du périmètre de la mesure à d'autres contenus. Si la lutte contre la pédopornographie constitue à l'évidence un objectif consensuel, les craintes de dérive vers une censure excessive sont présentes. Il est donc primordial d'opérer une restriction des mesures de blocage aux seuls contenus pédopornographiques, sans que ce périmètre puisse

[6] Chiffres communiqués par l'OCLCTIC

être ultérieurement étendu à d'autres types de contenus. C'est là un aspect fondamental du dispositif dont le non respect serait susceptible d'affaiblir l'acceptabilité collective d'une telle mesure.

- que le pouvoir de prononcer les mesures de filtrage soit confié à une autorité nationale compétente. Cette autorité jouerait le rôle d'intermédiaire entre les forces de l'ordre et les fournisseurs d'accès à l'internet, sur le modèle de ce qui a été conçu en matière de réquisition administrative de données techniques de connexion.

  Par « autorité nationale compétente », le Forum des droits sur l'internet n'entend pas présager du type même de structure à mettre en place.

  Divers schémas peuvent s'inscrire dans un tel cadre et notamment l'intervention directe des services administratifs de l'État, un dispositif de type autorité administrative indépendante (AAI) ou encore une commission administrative. Compte tenu de ces éléments, il peut notamment être envisagé, s'agissant de la validation de la liste, l'intervention d'une personnalité qualifiée « placée auprès du ministre de l'Intérieur ».

  Cette autorité nationale compétente devrait être construite selon quatre axes principaux :

  1. <u>La réactivité.</u> Quelle que soit l'architecture choisie, il convient que l'autorité nationale compétente soit en mesure de traiter l'ensemble des envois d'adresses dans un délai suffisamment court. Cela nécessite donc que cette autorité :
     - soit dotée des moyens humains nécessaires pour accomplir sa mission. Il pourrait être prévu un « comité restreint permanent » à même de traiter les dossiers quotidiennement ou le recours à une personnalité qualifiée, ainsi que cela a été mis en œuvre en matière de réquisition administrative de données techniques de connexion[7].
     - et qu'elle intervienne aussi *a posteriori*, afin de contrôler l'exercice qui a été fait de la mesure.

  2. <u>La protection des libertés fondamentales.</u> Dans ce but, l'autorité nationale compétente doit apporter des garanties équivalentes à celles issues de l'article 6 paragraphe 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales en termes d'indépendance, d'impartialité, de respect du contradictoire et de confidentialité. Par ailleurs, la mesure de filtrage prononcée par l'autorité nationale compétente devrait être notifiée à l'éditeur et à l'hébergeur du contenu lorsque ceux-ci sont identifiés.

     Toutefois, si la décision doit être publique, les pages bloquées devraient néanmoins être masquées en cas de communication au public des décisions afin d'éviter d'en faire la publicité. Enfin, la compétence de cette autorité doit être strictement limitée aux contenus revêtant un caractère manifestement pédopornographique. Les contenus ne présentant pas ce caractère manifeste devraient être renvoyés devant l'autorité judiciaire,

[7] Article 6 I de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

notamment au regard de la décision 96-378 DC du 23 juillet 1996 du Conseil constitutionnel[8].

3. Le respect de la transparence. S'il parait essentiel qu'une certaine transparence existe autour de la mise en œuvre d'une mesure de filtrage, il est néanmoins nécessaire de pouvoir l'aménager afin de prendre en considération la spécificité des contenus visés.
   En effet, la fonction de validation de la liste doit, à des fins de réactivité et parce qu'il n'est pas souhaitable qu'un nombre conséquent de personnes soient mises en relation avec des contenus d'ordre pédopornographique, être concentrée entre un nombre limité de personnes.
   En revanche, concernant le contrôle a posteriori des opérations de blocage, celui-ci pourrait, dans un souci de respect du pluralisme, être ouvert à un nombre restreint de représentants des pouvoirs publics, des acteurs économiques et du secteur associatif. Les débats étant, quant à eux, soumis à confidentialité.
   Enfin, l'autorité nationale compétente serait appelée à produire un rapport annuel d'activité.

4. L'existence de possibilités de recours en cas de filtrage abusif ou de décision infondée. Il est ainsi souhaitable de permettre le choix entre un recours gracieux devant l'autorité nationale compétente (qui devra statuer dans un bref délai) ou un recours contentieux devant le juge. En effet, il est notamment important que les propriétaires de sites ayant subi un dommage puissent solliciter l'arrêt du blocage ainsi que la réparation de leur préjudice. La mise à jour des listes doit ainsi nécessairement permettre le retrait des sites faisant l'objet d'un surblocage.

   S'agissant de la possibilité de réclamer à bref délai l'arrêt d'un blocage, rappelons que la loi du 30 Juin 2000[9] est venu alléger les procédures d'urgence du contentieux administratif en créant le « référé-liberté ». Ainsi , le Code de justice administrative prévoit désormais, dans son article L.521-2 que « Saisi d'une demande en ce sens justifiée par l'urgence, le juge des référés peut ordonner toutes mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle une personne morale de droit public ou un organisme de droit privé chargé de la gestion d'un service public aurait porté, dans l'exercice d'un de ses pouvoirs, une atteinte grave et manifestement illégale. Le juge des référés se prononce dans un délai de quarante-huit heures. »

---

[8] Considérant 27 : « Considérant qu'aux termes de l'article 34 de la Constitution, la loi fixe les règles concernant les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il appartient au législateur d'assurer la sauvegarde des droits et des libertés constitutionnellement garantis ; que s'il peut déléguer la mise en œuvre de cette sauvegarde au pouvoir réglementaire, il doit toutefois déterminer lui-même la nature des garanties nécessaires ; que, s'agissant de la liberté de communication, il lui revient de concilier, en l'état actuel des techniques et de leur maîtrise, l'exercice de cette liberté telle qu'elle résulte de l'article 11 de la Déclaration des droits de l'homme et du citoyen, avec, d'une part, les contraintes techniques inhérentes aux moyens de communication concernés et, d'autre part, les objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels ».

[9] Loi n° 2000-597 du 30 juin 2000 relative au référé devant les juridictions administratives

IV. – DISPOSITIF OPÉRATIONNEL

Indépendamment du dispositif juridique choisi, il est nécessaire :

- que la liste élaborée par les forces de police et de gendarmerie soit au minimum mise à jour quotidiennement et que ses évolutions soient transmises à l'autorité nationale compétente pour validation et transmission aux FAI.

- que cette liste puisse être élaborée en tenant compte de l'éventuelle coexistence de systèmes de filtrage différents et d'architectures réseaux différentes. Par exemple, en fournissant une liste servant au filtrage par DNS et une autre pour le filtrage « hybride » ainsi qu'en tenant compte des spécificités du réseau mobile, actuellement plus centralisé et gérant des flux moins importants.

- que la mise à jour de la liste prenne également en considération les sites devant être retirés de celle-ci, par exemple parce que celui-ci ne contient plus de contenus illicites ou encore à la suite d'un recours pour blocage abusif. Cette tâche pourrait éventuellement être confiée à l'autorité nationale compétente. En tout état de cause, un financement spécifique eu égard aux contraintes importantes en matière de ressources humaines sera nécessaire, et ce d'autant plus que, ainsi qu'il a été évoqué plus haut, la rotation de ces sites est assez fréquente et que le travail d'épure de la liste est primordial.

- que l'autorité nationale se voit confier la tâche de veiller à ce que les systèmes de filtrage restent cohérents avec les évolutions techniques futures des réseaux, le cas échéant en s'appuyant sur les compétences du Conseil Général des Technologies de l'Information (CGTI).

- qu'à réception de la liste, les FAI procèdent à l'inclusion des adresses litigieuses dans leur dispositif de filtrage dans les délais les plus brefs. Là encore, le nécessaire besoin de réactivité en la matière implique des délais d'exécution raccourcis.

- que la transmission de la liste des adresses à filtrer se fasse de manière sécurisée et cryptée entre les différents acteurs :

    1. Entre l'OCLCTIC et l'autorité nationale compétente, cette transmission doit néanmoins permettre la consultation, après décryptage de la liste, des adresses « en clair » afin que l'autorité nationale compétente puisse étudier les pages concernées en vue de prononcer sa décision.

    2. Entre l'autorité nationale compétente et les FAI.
       Deux méthodes sont envisageables.
       La première consisterait à désigner au sein de chaque FAI une personne habilitée à recevoir la liste, à la décrypter et à l'intégrer dans le dispositif de filtrage. Cette intervention humaine vient cependant affaiblir le dispositif en créant un risque de communication des adresses de la liste et une responsabilité supplémentaire pour les FAI. Toutefois, il convient de noter que les processus utilisés pour la communication des listes à l'étranger ne semblent pas être plus sécurisés.
       La seconde méthode consisterait à utiliser un procédé de chiffrement ne permettant pas la consultation des adresses en clair par les fournisseurs d'accès. Elle serait automatiquement intégrable dans le dispositif de filtrage. Ce procédé apporterait une garantie de sécurité supplémentaire et pourrait accroître la rapidité de mise à jour des listes. Elle pourrait augmenter le coût du dispositif.

- que lorsqu'un internaute voit sa navigation bloquée par la mise en place de la mesure de filtrage, une page d'information apparaisse afin de lui expliquer les raisons du filtrage. Cette page d'information pourrait idéalement inclure les éléments suivants :
    - Logo(s) Ministériel(s)
    - Mention de la coopération entre les forces de l'ordre et les FAI
    - Explication de la raison du filtrage (site diffusant des contenus pédopornographiques)
    - Article de loi : 227-23 du Code Pénal
    - Procédures de recours en cas de contestation
    - Procédure de signalement

V. – TECHNIQUES DE FILTRAGE AU NIVEAU DE L'ACCÈS

Plusieurs familles de solutions techniques sont d'ores et déjà déployées à l'étranger.

À titre préalable, il convient de noter qu'aucune des solutions ne se montre totalement imperméable par rapport à un éventuel contournement. Des solutions de contournement sont accessibles à la fois par l'éditeur du site proposant des images ou représentations d'abus sexuels sur mineurs tout comme par un utilisateur avisé.

En effet, tout internaute pourra trouver sur le web des sites proposant des solutions de contournement. Le risque est donc présent que les mesures de filtrage entrainent un durcissement de ces techniques de contournement, ce qui rendrait plus difficile, de fait, le travail des forces de l'ordre dans le cadre de la recherche des preuves et des poursuites contre les personnes consultant à titre habituel ce type de contenus.

Par ailleurs, si certaines des solutions présentées ci-après semblent plus susceptibles que d'autres de créer des risques de surblocage, ceux-ci constitueraient également une incitation pour certains hébergeurs à être plus vigilants par rapport aux contenus qu'ils hébergent.

Plus spécifiquement, s'agissant des opérateurs de téléphonie mobile, se pose la question de l'encapsulage des adresses par les moteurs de recherche et du redimensionnement des pages web pour les terminaux mobiles. Ces deux techniques particulières nécessitent de réécrire l'adresse du site recherché dans un format compatible. Ce qui les rend en quelque sorte invisibles pour les opérateurs mobiles et diminue d'autant l'efficacité d'un dispositif de blocage, engageant ainsi la responsabilité des opérateurs concernés. Ce point précis doit également faire l'objet des études préalables, en partenariat étroit avec les moteurs de recherche et l'AFOM.

Enfin, il faut rappeler que le risque de surblocage sera d'autant plus réduit que les services qui auront la charge de l'élaboration de la liste viseront en priorité les sites étrangers dont l'activité principale est la diffusion de contenus d'ordre pédopornographique.

A. – Le filtrage sur le nom de domaine (filtrage par *Domain Name Server*)

Cette première solution repose sur des systèmes de blocage au niveau du serveur DNS, derrière lequel se trouve le site internet visé. On vient donc filtrer l'ensemble du domaine internet qui héberge le site litigieux, ce qui entraîne nécessairement un risque de « surblocage » élevé puisque le blocage peut conduire à fermer l'accès à l'ensemble du site concerné et non aux seules pages litigieuses. Dans le cas d'un service d'hébergement de vidéos communautaires pouvant héberger des millions de vidéos, c'est l'ensemble du service qui pourrait ainsi être bloqué, quand bien même il n'hébergerait qu'une seule vidéo à caractère pédopornographique. Ce risque a été illustré au Brésil avec le blocage par les FAI brésiliens, sur décision judiciaire, d'une plate-forme de partage de vidéos en raison de l'hébergement d'un contenu illicite.

De plus, le blocage peut s'étendre à d'autres sites internet, qui sont eux parfaitement licites, mais qui se trouvent derrière le même serveur DNS. Techniquement, plusieurs milliers de sites peuvent ainsi relever d'un unique serveur DNS. C'est notamment le cas pour des services d'hébergement mutualisé ou les « pages personnelles ».

Cette technique pose également avec acuité le problème du paramétrage des filtres DNS par les opérateurs. Ainsi, elle pourrait aboutir au filtrage de communications non visées par la requête, (ex : envoi/réception de courriels relatifs au domaine).

De plus, le DNS du fournisseur de la connectivité IP d'un abonné n'est pas exclusif : un abonné peut tout à fait choisir d'opter pour un DNS fourni par un tiers.

Un tel système pose donc d'évidentes difficultés et s'avère potentiellement contraire à la liberté d'expression et de communication ainsi qu'à la liberté du commerce et de l'industrie. De ce fait, il présenterait un risque d'engagement de la responsabilité de l'État et/ou des fournisseurs d'accès.

Par ailleurs, devant la volatilité des contenus de l'Internet, il devient nécessaire de procéder à des mises à jour régulières afin d'éviter qu'un site ayant été bloqué à juste titre à une époque, continue de l'être malgré une modification de ses contenus.

Cette solution, déjà mise en œuvre dans certains pays scandinaves, a cependant l'avantage d'être relativement simple et moins onéreuse, tout en étant loin d'être gratuite en raison des coûts de maintenance et de développement qu'elle implique pour respecter les exigences imposées en terme de qualité de service. Elle parait compatible avec l'architecture du réseau français.

Néanmoins, le réseau français reposant sur une architecture dite « ouverte » et élaborée en vue de faire face à un important trafic tout en conservant une qualité de service en terme de rapidité des flux (en comparaison avec les autres pays ayant mis en œuvre un système de filtrage), il convient de souligner que la mise en œuvre de cette solution ne peut être strictement identique à celle retenue à l'étranger, et notamment en Norvège. Les différences en terme de débit et d'infrastructure, l'impact d'un tel dispositif sur la « qualité de service » ainsi que les coûts de mise en œuvre nécessitent donc la réalisation d'études menées par les opérateurs. Celles-ci devront également prendre en compte la spécificité des réseaux mobiles.

B. – Le filtrage sur l'adresse IP

Cette technique permet aux opérateurs de configurer leurs routeurs afin que ceux-ci ignorent une liste définie d'adresses IP.

Néanmoins, cette technique ne permet pas d'obtenir une granularité assez fine puisque des contenus différents, voire des sites différents utilisant la même adresse IP, seront bloqués indifféremment. Les risques de surblocage sont donc particulièrement importants, d'autant plus que les techniques de mutualisation d'adresses IP se développent.

Là encore cette technique s'avère facilement contournable par un utilisateur avisé et par les éditeurs de sites contenant des images ou représentations d'abus sexuels sur mineurs (noms de domaines réassignés automatiquement à de nouvelles IP à intervalles réguliers).

De plus, il existe des solutions cryptées de contournement par des systèmes d'anonymisation.

Cette technique nécessiterait que la mise à jour de la liste soit effectuée avec une fréquence encore plus grande par l'autorité chargée de son élaboration. En effet, les adresses IP changeant continuellement, il serait nécessaire d'en filtrer de nouvelles et de supprimer les adresses n'étant plus contrevenantes sous peine d'engorger rapidement le réseau.

C. – Le filtrage « hybride »

Ces solutions techniques permettent un blocage au niveau des URL (c'est-à dire au niveau des pages elles-mêmes et non du serveur entier). Il s'agit notamment de solutions expérimentées avec succès au Royaume-Uni, en Nouvelle-Zélande (ex : Cleanfeed et NetClean). Cette technique a l'avantage de ne traiter qu'une partie résiduelle du trafic du fait de l'existence d'un tri préalable effectué par les routeurs sur les adresses IP.

Cette technique nécessite donc dans un premier temps que les FAI soient destinataires d'une liste d'adresse IP correspondant aux noms de domaines où sont hébergées les contenus pédopornographiques, puis, dans un second temps, que ceux-ci paramètrent leurs routeurs afin que toute requête pour accéder à l'une des adresses IP de la liste soit redirigée vers une plateforme spécifique de filtrage. Un premier « tri » est donc effectué, suivi d'un second lorsque la plateforme vérifie si la page recherchée correspond bien à l'une des adresses de la liste.

Si tel est le cas, la transmission est bloquée. Dans le cas contraire, la plateforme permet à la communication d'être relayée normalement.

Là encore, cette technique est contournable par un internaute avisé tout comme l'éditeur du site litigieux.
L'une des grandes difficultés consiste ici à anticiper le volume de requêtes amené à être traité par la plateforme de filtrage. Notons également que ce volume est susceptible d'évolution du fait de l'accroissement du nombre de sites présents dans la liste noire élaborée par les forces de police et de gendarmerie[10], mais également du fait des pratiques des éditeurs de site eux-mêmes qui déplacent leurs sites régulièrement.

De plus, cette solution ne permettrait pas de gérer la Navigation Web Sécurisée puisque, dès lors, l'URL demandée n'est plus visible une fois la session établie.
Elle pose également le problème du risque de propagation d'erreurs dues notamment à de mauvaises manipulations et qui pourraient avoir pour conséquence de démultiplier le nombre d'adresses à rerouter. Compte tenu des limitations matérielles et logicielles, l'inclusion malencontreuse de portions significatives de sous-réseaux vers les serveurs de filtrage pourrait conduire à une dégradation substantielle du service.

Enfin, l'obligation de modifier régulièrement les configurations de routage risque d'être particulièrement complexe à gérer pour des opérateurs ayant développés de nombreux accords de peering[11].

Ces solutions, plus chères, limitent cependant considérablement les risques de surblocage et sont donc plus satisfaisantes vis-à-vis du respect de la liberté d'expression et de communication et des libertés fondamentales. Pour autant, elles risquent d'être plus délicates à mettre en œuvre sur le réseau français compte tenu de ses caractéristiques spécifiques (réseau ouvert) et pourraient nécessiter des aménagements importants des infrastructures de certains opérateurs. Elles semblent également, profondément contraires à la philosophie des architectures actuelles, construites pour permettre la communication à grande vitesse et l'accès à des services de plus en plus nombreux et consommateurs de bande passante.

[10] Voir synthèse page 18 pour les éléments de volumétrie

[11] Le Peering est une pratique d'échange du trafic Internet entre fournisseurs d'accès qui nécessite une interconnexion physique et virtuelle entre les réseaux et fait l'objet d'accords commerciaux entre les partenaires.

En conclusion, la solution de blocage qui sera adoptée devra être équilibrée entre :

- l'architecture du réseau de chaque FAI ;
- les adaptations nécessaires entre les réseaux fixes et mobiles ;
- la nécessité de préserver la qualité de service offerte à l'ensemble des internautes français ;
- et l'existence des solutions de contournement.

D. – Synthèse

Le principe retenu par le Forum des droits sur l'Internet est de laisser chaque opérateur libre du choix de sa solution de filtrage et de pouvoir l'adapter en fonction des spécificités des réseaux qu'ils exploitent (fixes et/ou mobiles).

Eu égard aux avantages et inconvénients de chaque solution et aux contraintes techniques propres aux opérateurs français, il s'avère délicat pour chacun de ceux-ci de choisir une solution plutôt qu'une autre sans que des études approfondies à partir d'estimations du volume des sites à filtrer n'aient été réalisées.
Par conséquent, le Forum des droits sur l'internet souhaite mettre en avant les éléments de volumétrie suivants :

- S'agissant de la liste élaborée au sein du ministère de l'Intérieur, celle-ci est constituée des seuls noms de domaines, et ne distingue donc pas actuellement les pages qui, au sein d'un même site, sont litigieuses de celles qui ne posent pas de difficulté particulière. Cette liste compte aujourd'hui 500 noms de domaines et, compte tenu de son évolution permanente, il est permis d'envisager une stabilisation à moyen terme aux alentours de 2000 noms de domaines, après épuration de la liste.

- Le choix d'une solution de filtrage plus fine, sur la base des seules pages litigieuses, nécessiterait, en revanche une liste probablement plus élargie. Ainsi, à titre de comparaison, la liste canadienne totaliserait 11000 adresses. La liste actuellement utilisée en Grande Bretagne fait quant à elle l'objet d'une épure la plus régulière possible des liens morts et d'une volonté de regrouper, autant que possible, les adresses au plus près du nom de domaine afin de limiter la taille de la liste. Cette dernière compte officiellement 1376 adresses. Les opérateurs français devraient ainsi travailler sur la base d'une volumétrie de 5000 adresses (URLs) à moyen terme.

Ces éléments de volumétrie devront guider les opérateurs dans la réalisation de leurs études.

Pour aider les opérateurs à sélectionner une solution de filtrage, le Forum des droits sur l'Internet a souhaité recommander la rédaction d'un « cahier des charges » reprenant les éléments devant nécessairement faire l'objet d'une étude technique par chaque opérateur. Ce document sera réalisé avec le concours du Conseil Général des Technologies de l'Information (CGTI).

Sur la base de ce cahier des charges, chaque opérateur devra donc procéder, dans les délais les plus brefs, à la réalisation d'études permettant de déterminer quel système de filtrage s'avère techniquement et financièrement le plus réaliste à mettre en œuvre sur ses infrastructures. Les opérateurs sont ainsi invités à présenter le résultat de leurs études et le dispositif technique choisi dans les quatre mois suivant la publication du cahier des charges.

La question du financement de la mesure devra donner lieu à une négociation entre les acteurs concernés et l'État sur trois éléments distincts :

1. la constitution et la gestion de la liste ainsi que la mise en place du dispositif juridique, à travers, notamment, la constitution de l'autorité nationale compétente ;
2. les procédures de chiffrement et de transmission des informations ;
3. l'intégration et l'exploitation des dispositifs de filtrage au sein des infrastructures des FAI.

VI. – CONCLUSION

À la suite des travaux menés par le groupe de travail du Forum des droits sur l'internet, et à la volonté déclarée des Fournisseurs d'accès à l'Internet de lutter contre les sites contenant des images ou représentations d'abus sexuels sur mineurs hébergés à l'étranger, le Forum des droits sur l'internet recommande :

- la mise en place, par la voie législative et dans le cadre d'une loi spécifique à la lutte contre la pédopornographie, sur le modèle évoqué au III-B, d'une autorité nationale compétente permettant de requérir des opérateurs de communication électronique qu'ils procèdent au filtrage des sites identifiés par L'OCLCTIC ;

- le strict respect des garanties évoquées quant à la constitution d'une telle autorité ;

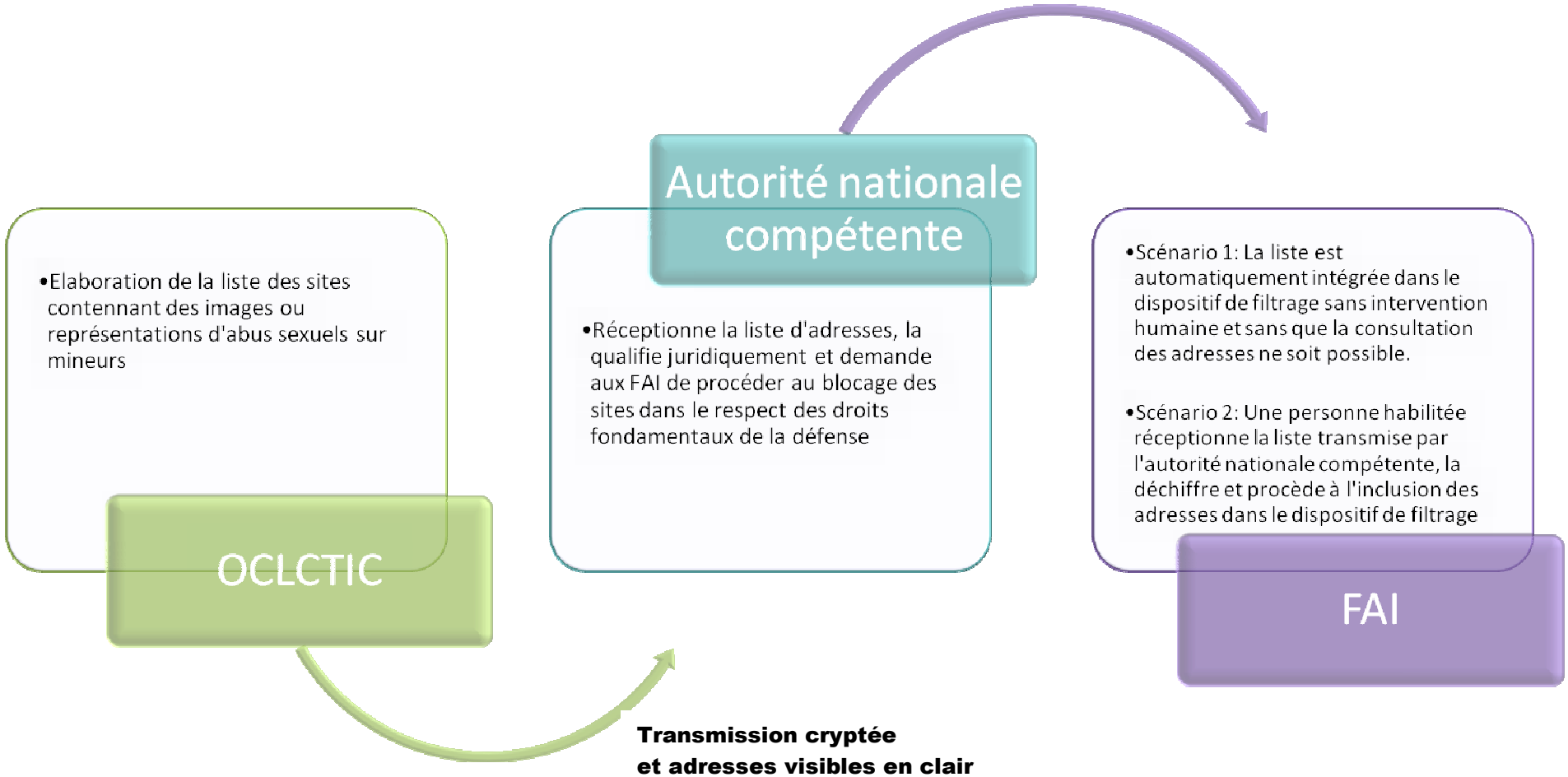
- le libre choix pour les opérateurs de leur solution technique de filtrage ;

- la réalisation par chaque opérateur de communication électronique, sur la base du cahier des charges élaboré par le Forum des droits sur l'Internet en collaboration avec le CGTI, d'études sur la mise en place sur leurs infrastructures de systèmes de filtrage, prenant en compte les spécificités fixes et mobiles. Ces études devront permettre à chaque opérateur de présenter le type de solution de filtrage qu'il souhaite retenir, dans les quatre mois suivant la publication du cahier des charges.

Le projet d'architecture décrit ci-dessus fera l'objet d'un accord entre les pouvoirs publics et les opérateurs de communication électronique. Cet accord devra inclure les éléments d'ordre financier sur les trois points précédemment cités. Il permettra la finalisation du dispositif global de filtrage dans le respect des objectifs de la loi.

PROCESSUS DE TRANSMISSION DE LA LISTE

Transmission cryptée et adresses non visibles en clair



Transmission cryptée et adresses visibles en clair

ANNEXE – COMPOSITION DU GROUPE DE TRAVAIL

Représentants des acteurs économiques :

- **Association des fournisseurs d'accès et de services internet (AFA)**

  Dahlia KOWNATOR
  Déléguée générale

  Carole GAY et Estelle DE MARCO
  Responsables des affaires juridiques et réglementaires

- **Association Française des Opérateurs Mobiles (AFOM)**

  Nicolas HERBRETEAU
  Chargé de Mission

- **Bouygues Telecom**

  Eglantine VIAL
  Juriste réglementaire

- **Google France**

  Olivier ESPER
  Responsable des relations institutionnelles

- **Microsoft France**

  Frédéric GÉRAUD DE LESCAZES
  Responsable des affaires publiques

- **Orange**

  Raynald HENRY
  Chargé d'affaires réglementaires

- **SFR**

  Frédéric DEJONCKHEERE
  Juriste – Direction de la réglementation

- **Xooloo**

  Grégory VERET
  Président

Représentants des utilisateurs :

- **Action Innocence France**

  Véronique FIMA-FROMAGER
  Responsable Action Innocence France

- **Association pour la Promotion et la Recherche en Informatique Libre**

(APRIL)

Christophe ESPERN
Chargé des relations institutionnelles

- **Confédération Nationale des Associations Familiales Catholiques (CNAFC)**
  Pierre DE BERNIERES
  Responsable mission Médias Enfance

- **Association E-Enfance**

  Christine DU FRETAY
  Présidente

  Dominique DELORME

- **Union nationale des associations familiales (UNAF)**
  Olivier Gérard
  Coordonnateur Média-TIC-Université des Familles

Experts :

- **Marie DEMOULIN**
  Directrice de l'unité « Commerce électronique », Centre de Recherche Informatique et Droit, Facultés Universitaires Notre Dame de la Paix, Namur (CRID – FUNDP)

- **Sophie JEHEL**
  Chercheur en information et communication Laboratoire CARISM/ IFP Université de Paris 2

- **Céline SCHOËLLER**
  Chercheur, Centre de Recherche Informatique et Droit, Facultés Universitaires Notre Dame de la Paix, Namur (CRID – FUNDP)

Observateurs des pouvoirs publics :

- **Défenseure des enfants**
  Odile NAUDIN
  Conseillère près la Défenseure des enfants

- **Délégation interministérielle à la Famille**
  Olivier PERALDI
  Adjoint au Délégué

- **Ministère de l'Intérieur**
  Pierre-Yves LEBEAU
  Capitaine de Police, Chef de la Plateforme Nationale de Signalement
  Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)

  Frédéric MALON
  Commissaire Divisionnaire
  Office Central pour la Répression des Violences aux Personnes (OCRVP)

- **Ministère de la Recherche et de l'Enseignement supérieur**
  Pierre PEREZ
  Secrétaire Général, Délégation aux Usages de l'internet (DUI)

  Yves LABOREY
  Délégation aux Usages de l'internet (DUI)

- **Ministère de la Défense**
  Éric FREYSSINET
  Lieutenant-Colonel
  Direction générale de la Gendarmerie nationale

La coordination des travaux était assurée par Laurent BAUP et David MELISON, juristes chargés de mission au Forum des droits sur l'internet.