Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

ETUDE COMPARATIVE SUR

LE BLOCAGE, LE FILTRAGE ET LE RETRAIT DE CONTENUS ILLEGAUX SUR INTERNET

Extrait, pages 236-255

Ce document fait partie de l'Etude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet dans les 47 Etats membres du Conseil de l'Europe, qui a été préparée par l'Institut suisse de droit comparé à l'invitation du Secrétaire Général. Les opinions exprimées dans ce document n'engagent pas la responsabilité du Conseil de l'Europe. Elles ne donnent, des instruments juridiques qu'il mentionne, aucune interprétation officielle pouvant lier les gouvernements des Etats membres du Conseil de l'Europe, les organes statutaires du Conseil de l'Europe ou la Cour européenne des droits de l'homme.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

Le 24 novembre 2014, le Conseil de l'Europe a formellement mandaté l'Institut suisse de droit comparé (« ISDC ») pour réaliser une étude comparative des lois et pratiques en matière de filtrage, blocage et retrait de contenus illégaux sur Internet dans les 47 Etats membres du Conseil de l'Europe.

Comme convenu entre l'ISDC et le Conseil de l'Europe, l'étude présente les lois et, pour autant que les informations soient facilement disponibles, les pratiques de filtrage, blocage et retrait de contenus illégaux sur Internet dans plusieurs contextes. Elle examine la possibilité de telles mesures en cas de menace à l'ordre public ou à la sécurité intérieure ainsi qu'en cas de violation des droits de la personnalité et des droits de propriété intellectuelle. Dans chaque cas, l'étude examine le cadre juridique qui sous-tend les décisions de filtrer, bloquer ou retirer les contenus illégaux sur Internet, l'autorité habilitée à prendre de telles décisions et les conditions d'exécution de ces décisions. Par ailleurs, l'étude se penche sur les possibilités de contrôle extrajudiciaire des contenus en ligne et présente une brève description de la jurisprudence pertinente et importante.

Elle s'organise, pour l'essentiel, en deux parties principales. La première partie consiste en une compilation de rapports nationaux pour chacun des Etats membres du Conseil de l'Europe. Elle présente une analyse plus détaillée des lois et des pratiques en matière de filtrage, blocage ou retrait des contenus illégaux sur Internet dans chaque Etat membre. Afin de faciliter la lecture et les comparaisons, tous les rapports nationaux sont présentés suivant la même structure (voir ci-dessous, questions). La deuxième partie présente des considérations comparatives sur les lois et les pratiques en matière de filtrage, blocage ou retrait de contenus illégaux en ligne dans les Etats membres. Elle vise ainsi à faire ressortir et à tenter d'expliquer les convergences et les divergences qui existent le cas échéant entre les approches des Etats membres sur les questions couvertes par l'étude.

II. MÉTHODOLOGIE ET QUESTIONS

1. Méthodologie

La présente étude a été déployée en trois temps. Dans une première phase, la phase préliminaire, l'ISDC a élaboré un questionnaire détaillé, en coopération avec le Conseil de l'Europe. Une fois approuvé par le Conseil de l'Europe, ce questionnaire (voir point 2 ci-dessous) a servi de base aux rapports nationaux.

La deuxième phase a consisté à produire les rapports par pays relatifs aux différents Etats membres du Conseil de l'Europe. Cette tâche a été accomplie soit par le personnel de l'ISDC soit par des correspondants externes pour les Etats membres que l'Institut ne pouvait pas couvrir en interne. Les principales sources sur lesquelles se sont appuyés les rapports nationaux sont les lois pertinentes et, lorsqu'elles étaient disponibles, les publications académiques sur les questions examinées. En plus, dans certains cas, en fonction de la situation, des entretiens ont eu lieu avec les parties concernées afin de se faire une idée plus précise de la situation. Cela étant dit, les rapports ne sont pas fondés sur des données empiriques et statistiques, dans la mesure où ils visent principalement à analyser le cadre juridique en vigueur.

Dans la phase suivante (la troisième), l'ISDC et le Conseil de l'Europe ont examiné tous les rapports par pays et fourni des informations en retour aux différents auteurs. En plus de cela, l'ISDC a rédigé les commentaires comparatifs sur la base des différents rapports nationaux ainsi que sur la base des publications académiques et des autres ressources disponibles, notamment au niveau du Conseil de l'Europe.

Le Conseil de l'Europe a ensuite envoyé les rapports par pays finalisés aux représentants des États membres concernés pour commentaires. Des commentaires sur certains des rapports ont été envoyés par les États membres concernés et soumis aux auteurs des rapports. Les rapports par pays ont été modifiés en conséquence seulement lorsque les auteurs l'ont jugé approprié. En outre, aucune tentative n'a été faite, en général, pour incorporer les nouveaux développements survenus après la date effective de l'étude.

Tout au long de ce processus, l'ISDC a coordonné ses activités étroitement avec le Conseil de l'Europe. Cependant, le contenu de l'étude relève de la responsabilité exclusive des auteurs et de l'ISDC. Cela dit, l'ISDC ne peut assumer la responsabilité du caractère complet, correct et exhaustif des informations figurant dans les différents rapports nationaux.

2. Questions

En accord avec le Conseil de l'Europe, tous les rapports nationaux sont, dans la mesure du possible, structurés suivant les axes ci-après :

1. Quels sont les fondements juridiques des mesures de blocage, filtrage ou retrait des contenus illégaux sur Internet ?

Liste indicative de ce que cette partie devrait couvrir :

- Ce domaine est-il réglementé ?

- Des normes internationales, notamment des conventions concernant les contenus illégaux sur Internet (tels que des conventions sur la protection de l'enfance, la cybercriminalité ou la lutte contre le terrorisme) ont-elles été transposées dans le cadre réglementaire nationale ?
- Cette réglementation est-elle fragmentée entre plusieurs domaines du droit, ou forme-t-elle plutôt un corpus de règles spécifique à Internet ?
- Présenter un aperçu des sources juridiques qui réglementent les activités de blocage, filtrage ou retrait des contenus illégaux sur Internet (une analyse plus détaillée sera présentée dans la réponse à la question 2).

2. Quel est le cadre juridique qui réglemente :

2.1. Le blocage et/ou le filtrage de contenus illégaux sur Internet ?

Liste indicative de ce que cette partie devrait couvrir :

- Pour quels motifs des contenus Internet sont-ils bloqués ou filtrés ? Cette partie devrait couvrir tous les motifs suivants, le cas échéant :
  - la protection de la sécurité nationale, l'intégrité territoriale ou la sûreté publique (par exemple, le terrorisme) ;
  - la défense de l'ordre et la prévention du crime (par exemple, la pornographie mettant en scène des enfants) ;
  - la protection de la santé publique ou des bonnes mœurs ;
  - la protection de la réputation ou des droits d'autrui (par exemple, les droits relatifs à la diffamation, à la vie privée ou à la propriété intellectuelle) ;
  - la prévention de la diffusion d'informations confidentielles.
- Quelles exigences et garanties le cadre juridique énonce-t-il pour un tel blocage ou filtrage ?
- Quel est le rôle des fournisseurs d'**accès** à Internet dans la mise en œuvre de ces mesures de blocage et de filtrage ?
- Existe-t-il des instruments juridiques non contraignants (meilleures pratiques, codes de conduite, lignes directrices, etc.) dans ce domaine ?
- Une description concise de la jurisprudence pertinente.

2.2. Le retrait ou la suppression de contenus illégaux sur Internet ?

Liste indicative de ce que cette partie devrait couvrir :

- Pour quels motifs des contenus Internet sont-ils retirés ou supprimés ? Cette partie devrait couvrir tous les motifs suivants, le cas échéant :
  - la protection de la sécurité nationale, l'intégrité territoriale ou la sûreté publique (par exemple, le terrorisme) ;
  - la défense de l'ordre et la prévention du crime (par exemple, la pornographie mettant en scène des enfants) ;
  - la protection de la santé publique ou des bonnes mœurs ;
  - la protection de la réputation ou des droits d'autrui (par exemple, les droits relatifs à la diffamation, à la vie privée ou à la propriété intellectuelle) ;
  - la prévention de la diffusion d'informations confidentielles.

- Quel est le rôle des fournisseurs d'hébergement sur Internet et des médias sociaux et autres plateformes (réseaux sociaux, moteurs de recherche, forums, blogs, etc.) dans la mise en œuvre de ces mesures de retrait ou de suppression de contenus ?
- Quelles exigences et garanties le cadre juridique énonce-t-il pour une telle suppression ?
- Existe-t-il des instruments juridiques non contraignants (meilleures pratiques, code de conduite, lignes directrices, etc.) dans ce domaine ?
- Description concise de la jurisprudence pertinente.

3. Aspects procéduraux : quels sont les organes habilités à décider du blocage, filtrage ou retrait de contenus Internet ? Comment la mise en œuvre de ces décisions est-elle organisée ? Des possibilités de révision sont-elles prévues ?

Liste indicative de ce que cette partie devrait couvrir :

- Quels sont les organes (judiciaires ou administratifs) habilités à décider du blocage, filtrage ou retrait de contenus illégaux sur Internet ?
- Comment ces décisions sont-elles mises en œuvre ? Décrire les étapes de la procédure jusqu'au blocage, filtrage ou retrait effectif du contenu Internet incriminé.
- Quelles sont les obligations de notification de la décision aux individus ou parties concernés ?
- Les parties concernées ont-elles la possibilité de solliciter et d'obtenir la révision d'une telle décision par un organe indépendant ?

4. La surveillance générale d'Internet : existe-t-il dans votre pays une entité responsable de la surveillance des contenus Internet ? Dans l'affirmative, sur quelle base cette activité de surveillance est-elle mise en œuvre ?

Liste indicative de ce que cette partie devrait couvrir :

- Il s'agit ici des entités chargées de contrôler les contenus Internet et d'évaluer leur conformité avec les prescriptions légales, y compris les droits de l'homme – il peut s'agir d'entités spécifiques responsables d'un tel contrôle ainsi que des fournisseurs de services Internet. De telles entités existent-elles ?
- Quels critères d'évaluation des contenus Internet appliquent-elles ?
- De quels pouvoirs disposent-elles pour s'attaquer aux contenus illégaux sur Internet ?

5. Evaluation de la jurisprudence de la Cour européenne des droits de l'homme

Liste indicative de ce que cette partie devrait couvrir :

- La législation régissant le blocage, filtrage ou retrait de contenus Internet satisfait-elle aux exigences de qualité (prévisibilité, accessibilité, clarté et précision) énoncées par la Cour européenne des droits de l'homme ? Existe-t-il des garanties pour la protection des droits de l'homme (notamment la liberté d'expression) ?
- La législation inclut-elle les garanties nécessaires pour prévenir l'abus de pouvoir et l'arbitraire conformément aux principes établis par la jurisprudence de la Cour européenne des droits de l'homme (par exemple, la garantie que les décisions de blocage ou de filtrage sont aussi ciblées que possible et ne sont pas utilisées comme un moyen de blocage à grande échelle) ?

- Les prescriptions légales sont-elles respectées dans la pratique, notamment pour ce qui est de l'évaluation de la nécessité et de la proportionnalité de toute ingérence dans l'exercice de la liberté d'expression ?
- En cas d'existence d'un cadre d'autoréglementation dans ce domaine, est-il assorti de garanties de protection de la liberté d'expression ?
- La jurisprudence pertinente est-elle en conformité avec la jurisprudence pertinente de la Cour européenne des droits de l'homme ?

Dans certains rapports nationaux, cette partie reflète principalement des publications académiques nationales ou internationales sur ces questions dans l'Etat concerné. Dans d'autres rapports, les auteurs font une évaluation plus indépendante.

FRANCE

Dans la version anglaise, cette partie apparaît dans les pages 236 à 255

1. Sources

La France est partie à l'ensemble des conventions du Conseil de l'Europe en matière de gouvernance d'internet. Elle a signé et ratifié la Convention sur la cybercriminalité conclue à Budapest le 23 novembre 2001. Celle-ci a été publiée au Journal Officiel de la République française par le biais du décret 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité[1]. Le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, a également fait l'objet d'une publication au Journal Officiel par le biais du décret 2006-597 du 23 mai 2006[2].

La Convention pour la prévention du terrorisme adoptée le 16 mai 2005 à Varsovie, signée par la France le 22 mai 2006, a été publiée dans le Journal Officiel par le biais du décret 2008-1099 du 28 octobre 2008[3].

La Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels, signée à Lanzarote le 25 octobre 2007, a, quant à elle, été publiée dans le Journal Officiel par le biais du décret 2011-1385 du 27 octobre 2011[4].

Enfin, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée à Strasbourg le 28 janvier 1981 a été publiée au Journal Officiel par le biais de la loi 82-890 du 19 octobre 1982[5]. Le Protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, adopté le 8 novembre 2001 à Strasbourg a été, quant à lui, publié dans le Journal Officiel par le biais de la loi 2007-301 du 5 mars 2007[6].

La matière relative au blocage, filtrage de sites internet ainsi que de retrait de contenus illicites d'internet est régie, en France, par des **lois et règlements** qui varient selon les motifs qui sont à la base de ces mesures de restriction.

---

1 Décret 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, JORF, 24 mai 2006.

2 Décret 2006-597 du 23 mai 2006 portant publication du protocole additionnel à la convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, JORF, 27 mai 2006.

3 Décret 2008-1099 du 28 octobre 2008 portant publication de la convention du Conseil de l'Europe pour la prévention du terrorisme (ensemble une annexe), adoptée le 16 mai 2005 à Varsovie, signée par la France le 22 mai 2006, JORF, 30 octobre 2008.

4 Décret 2011-1385 du 27 octobre 2011 portant publication de la convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels (ensemble une déclaration et une réserve), signée à Lanzarote le 25 octobre 2007, JORF, 29 octobre 2011.

5 Loi 82-890 du 19 octobre 1982 portant publication de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée à Strasbourg le 28 janvier 1981, JORF, 20 octobre 1982, 3163.

6 Loi 2007-301 du 5 mars 2007 autorisant l'approbation du Protocole additionnel à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, adopté le 8 novembre 2001 à Strasbourg, JORF, 7 mars 2007.

La loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (ci-après «LCEN») représente le texte législatif principal sur la question du blocage et du retrait de contenus illicites sur internet. Elle prévoit des possibilités pour l'autorité judiciaire mais aussi pour l'autorité administrative d'ordonner le blocage ou filtrage de certains sites qui remplissent certains critères ainsi que le retrait de contenus de ces sites internet. Les dispositions pertinentes de cette loi pour cette étude ont d'abord été modifiées par la loi 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite loi LOPPSI 2; la LCEN a été complétée plus récemment par la loi 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

Dans le domaine des droits de la propriété intellectuelle, on relève que le Code de la propriété intellectuelle prévoit également des dispositions permettant au juge d'ordonner le retrait de contenus de sites internet constituant une violation des droits intellectuels.

Dans le domaine de la protection de la vie privée, le code civil prévoit la possibilité pour le juge civil d'ordonner toute mesure permettant d'empêcher ou de faire cesser à l'atteinte en cause.

Certains autres domaines connaissent un dispositif de blocage administratif ou semi-administratif: Ainsi, dans le domaine de la protection des données à caractère personnel, la Commission nationale de l'informatique et des libertés dispose de pouvoirs pour faire cesser les traitements de données à caractère personnel intervenant sur internet dans des conditions précisées dans la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Dans le même sens, l'Autorité de régulation des jeux en ligne est en mesure de requérir auprès du président tribunal de grande instance que les hébergeurs de sites internet et les fournisseurs d'accès à internet rendent impossible l'accès à un service de jeux en ligne en contravention aux conditions légales.

2. Réglementation applicable

2.1. Blocage et/ou filtrage de contenu illégal d'internet

2.1.1. En matière de protection de la sécurité nationale et des bonnes mœurs

En application des articles 12 al. 3 de la directive 2000/31/CE sur le commerce électronique, la LCEN prévoit que les fournisseurs d'accès à internet (ci-après «FAI») peuvent être contraints, **par la voie judiciaire**, à faire cesser ou à prévenir le dommage occasionné par le contenu d'un site internet. En effet, la LCEN prévoit que:

> «l'autorité judiciaire peut prescrire en référé ou sur requête, [au fournisseur d'hébergement] ou, à défaut, [au fournisseur d'accès à des services de communication au public en ligne], 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»[7].

Concrètement, ces mesures ordonnées par le juge civil consistent à rendre inaccessible un contenu sur internet. Une telle action judiciaire peut aboutir tant à des mesures provisoires qu'à une décision définitive. Les mesures sont d'abord ordonnées à l'égard du fournisseur d'hébergement (voir section 2.2); ce n'est que si lesdits hébergeurs s'avèrent défaillants que les mesures sont ordonnées à l'encontre des différents fournisseurs d'accès à internet; dans ce dernier cas, il convient de réitérer l'opération auprès de chaque intermédiaire technique. Au vu du caractère général de cette

[7] Art. 6.I.8 LCEN.

disposition, elle doit être considérée comme susceptible de s'appliquer **indépendamment du motif de l'illicéité** du contenu constatée par le juge. Comme exposé ci-après, certains domaines bénéficient toutefois d'une réglementation spécifique sur le thème du blocage, filtrage et retrait de contenu illicite sur internet.

La question de l'étendue des pouvoirs du juge à l'encontre des FAI dans le cadre de l'art. 6, I, 8 LCEN s'est posée devant les juridictions françaises dans une affaire dans laquelle le Ministère de l'Intérieur avait entendu lutter contre une série de sites internet qui dénonçaient les violations policières en France et qui, ce faisant, diffusaient des propos injurieux et diffamatoires envers l'administration publique (en particulier la police) ainsi que des données personnelles collectées à l'insu des personnes concernées. Nous présentons cette affaire en détail à la section 2.1.3. ci-dessous, relative aux mesures de blocage et filtrage prises en vue de la protection de la vie privée et des données personnelles.

Dans une décision du 10 février 2012 en lien avec cette affaire, le tribunal de grande instance de Paris a ordonné que l'accès au site concerné soit bloqué par les différents FAI, pour une durée de six mois. Ce faisant, le tribunal a précisé qu'il était démontré concernant ce site que les hébergeurs ou les éditeurs du site internet en cause n'avaient pas pu être identifiés malgré les démarches entreprises par le Ministère de l'Intérieur sur ce point. En ce qui concerne d'autres sites internet sur lequel portait également la demande en justice, le tribunal a décidé que le blocage n'était pas opportun étant donné que le Ministère de l'Intérieur n'avait pas indiqué s'il avait tenté ou non d'identifier leurs hébergeurs et éditeurs.

De plus, aux fins de renforcer la lutte contre le terrorisme en particulier et de réorganiser celle contre la pédopornographie, le législateur français a récemment[8] modifié le code de procédure pénale ainsi que la LCEN.

Le législateur français a en effet introduit de nouvelles dispositions dans la LCEN en vertu desquelles les sites internet diffusant des images constitutives d'infractions pénales à caractère **pédopornographique**[9] ou de **provocation à des actes de terrorisme ou d'apologie du terrorisme**[10],

---

8 Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions sur la lutte contre le terrorisme, disponible sur: www.legifrance.gouv.fr.

9 L' article 227-23 du code pénal prévoit: « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.
Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.
Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende.
Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée.
La tentative des délits prévus au présent article est punie des mêmes peines.

peuvent faire l'objet d'un **retrait** d'internet ou d'un **blocage**. Ces mesures interviennent par une décision de l'autorité administrative compétente – et donc, sans intervention judiciaire.

D'après le décret du 5 février 2015[11] chargé de mettre en œuvre les dispositions récemment introduite dans la LCEN par la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme, l'autorité administrative en charge du blocage et/ou du retrait ces sites internet est la direction générale de **la police nationale**, Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (ci-après «OCLCTIC»). Au sein de cette autorité administrative, seuls certains agents individuellement désignés et dûment habilités par le chef de l'office sont autorisés à mettre en œuvre la procédure de blocage.

En application de l'art. 6-1, al. 1er LCEN, l'OCLCTIC ordonne aux fournisseurs d'hébergement sur internet des sites en cause de **retirer** les contenus internet. Le dispositif mis en place prévoit qu'en l'absence de retrait dans un délai de 24 heures, l'OCLCTIC peut **notifier aux FAI la liste des adresses électroniques** des services de communication au public en ligne contrevenant auxdites dispositions pénales. Dans les 24 heures de la notification susmentionnée, les FAI doivent empêcher par tout moyen approprié l'accès aux services fournis par les adresses électroniques figurant sur la liste et le transfert vers ces services. Toutefois, la LCEN prévoit qu'en l'absence de mise à disposition du public des informations relatives à l'éditeur du site – publication qui est prescrite par l'art. 6, III LCEN –, l'OCLCTIC peut notifier aux FAI les adresses des sites internet devant être bloqués selon sa décision, sans avoir préalablement requis le retrait de ces données.

Les personnes morales qui manqueraient aux obligations prévues par la LCEN en ce qui concerne les contenus relatifs à la pédopornographie ou à la provocation ou l'apologie du terrorisme, tels que présentés ci-dessus, sont punis d'une **amende** de 375 000 Euros et encourent également **l'interdiction**, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales. En outre, la décision en question sera affichée ou diffusée soit dans la presse écrite, soit par tout autre moyen de communication au public par voie électronique.

En outre, en application du nouvel article 706-23 du Code de procédure pénale, introduit par la loi du 13 novembre 2014 renforçant les dispositions sur la lutte contre le terrorisme, le juge pénal agissant en référé peut ordonner, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir, l'arrêt d'un service de communication en ligne au public pour les faits constitutifs d'infraction pénale de provocation à des actes de terrorisme ou d'apologie du terrorisme, lorsque ces faits constituent un trouble manifestement illicite[12].

Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. »

10 L'article 421-2-5 du code pénal prévoit: «Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende. Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne.
Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.»

11 Décret 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, J.O., 6 février 2015. Ce décret est entré en vigueur le 7 février 2015.

12 Une disposition similaire est contenue dans la loi du 29 juillet 1881 sur la liberté de la presse, en ce qui concerne certaines infractions y contenues, notamment la provocation à la discrimination, à la haine, à

Enfin, on relève que, **dans le domaine des jeux en ligne**, c'est l'**Autorité de régulation des jeux en ligne** (ci-après «ARJEL») qui est en charge du contrôle des sites internet de jeux en ligne, le cas échéant sous le contrôle du juge. L'ARJEL peut également être saisie par le ministère public et toute personne physique ou morale ayant intérêt à agir.

L'ARJEL adresse en effet aux opérateurs de jeux ou de paris en ligne non autorisés en vertu d'un droit exclusif ou de l'agrément prévu par la loi et à toute personne proposant une quelconque offre de jeux d'argent et de hasard en ligne en contravention aux dispositions légales et réglementaires, par tout moyen propre à en établir la date de réception, **une mise en demeure** rappelant les dispositions relatives aux sanctions encourues et celles relatives au blocage et/ou retrait de sites internet, enjoignant à ces opérateurs de respecter cette interdiction et les invitant à présenter leurs observations dans un délai de huit jours.

A l'issue de ce délai, en cas d'inexécution par l'opérateur intéressé de l'injonction de cesser son activité d'offre de paris ou de jeux d'argent et de hasard, le président de l'ARJEL peut **saisir le président du tribunal de grande instance de Paris** aux fins d'ordonner, en la forme des référés, **l'arrêt de l'accès à ce service aux hébergeurs de sites internet et aux fournisseurs d'accès à internet.**

Le président de l'Autorité de régulation des jeux en ligne peut également saisir le président du tribunal de grande instance de Paris aux fins de voir prescrire, en la forme des référés, toute mesure destinée à **faire cesser le référencement du site d'un opérateur concerné** par un moteur de recherche ou un annuaire.

2.1.2. La protection des droits de propriété intellectuelle

Le code de la **propriété intellectuelle** (ci-après «CPI») contient des dispositions, qui sont spécifiques à la matière des droits intellectuels, et qui sont de nature à permettre le blocage de sites internet dont les activités portent atteinte aux droits de propriété intellectuelle.

Ainsi, l'art. L.336-2 CPI prévoit qu'en présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits d'auteur ou des organismes de défense professionnelle, **toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier**[13]. Ces mesures peuvent ainsi consister en des mesures de blocage ou de filtrage de même que le retrait d'internet des produits contrefaisants.

---

la violence, l'apologie de crimes et la contestation de crimes contre l'humanité (art. 50-1 de la loi du 29 juillet 1881).

13 Dans le même sens, l'art. 336-1 du code de la propriété intellectuelle prévoit que: «Lorsqu'un logiciel est principalement utilisé pour la mise à disposition illicite d'œuvres ou d'objets protégés par un droit de propriété littéraire et artistique, le président du tribunal de grande instance, statuant en référé, peut ordonner sous astreinte toutes mesures nécessaires à la protection de ce droit et conformes à l'état de l'art.
Les mesures ainsi ordonnées ne peuvent avoir pour effet de dénaturer les caractéristiques essentielles ou la destination initiale du logiciel.»

C'est sur la base de l'art. L.336-2 CPI que le tribunal de grande instance de Paris a rendu, le 4 décembre 2014, un jugement ordonnant aux FAI de bloquer l'accès en France aux sites internet du réseau *the piratebay*, ceux-ci étant entièrement dédié ou quasiment entièrement dédié à la représentation de phonogrammes sans le consentement des auteurs, ce qui constitue une atteinte aux droits d'auteur telle que prévue à l'art. L.336-2 CPI[14]. Le dispositif du jugement rendu en référé dispose que la mesure de blocage doit être exécutée par les FAI au plus tard dans les quinze jours à compter de la signification dudit jugement et pendant une durée de douze mois à compter de la mise en place de ces mesures. C'est également sur cette base légale que le tribunal de grande instance de Paris a ordonné, en référé, que le site internet T411 soit bloqué par les différents FAI en raison du fait que son activité est entièrement ou quasi entièrement dédiée à la représentation de phonogrammes sans le consentement des auteurs, ce qui constitue une violation aux droits d'auteur[15].

En matière de **contrefaçon de marques** aussi, des mesures peuvent être prises pour prévenir ou faire cesser un dommage. Sur internet, le juge peut ordonner à des intermédiaires tels que des exploitants de plateformes de commerce en ligne de rendre inaccessibles des offres de produits contrefaisants.

Dans le cadre d'une procédure urgente en référé, l'art. L.716-6 CPI prévoit ainsi que le juge civil peut:

> «ordonner, au besoin sous astreinte, à l'encontre du prétendu contrefacteur ou des intermédiaires dont il utilise les services, toute mesure destinée à prévenir une atteinte imminente aux droits conférés par le titre ou à empêcher la poursuite d'actes argués de contrefaçon»[16].

De plus, lorsque les circonstances exigent que ces mesures ne soient pas prises contradictoirement, notamment lorsque tout retard serait de nature à causer un préjudice irréparable au demandeur, le juge peut également «ordonner toutes mesures urgentes sur requête»[17].

La juridiction peut ainsi interdire la poursuite des actes argués de contrefaçon ou ordonner la saisie ou la remise entre les mains d'un tiers des produits soupçonnés de porter atteinte aux droits conférés par le titre, pour empêcher leur introduction ou leur circulation dans les circuits commerciaux[18]. Le juge civil peut ainsi ordonner au FAI le blocage d'un site internet proposant à la vente les produits contrefaisants, de même que le retrait de ces produits du site en cause par l'hébergeur ou l'éditeur.

Dans le cadre de cette procédure de référé en contrefaçon de marque, il conviendra au demandeur d'apporter la preuve du caractère vraisemblable de l'atteinte portée à ses droits ou du fait qu'une telle atteinte est imminente. A cet égard, on peut relever que, dans une affaire dans laquelle la société SwissLife Prévoyance Santé a agi en contrefaçon de marque à l'encontre de l'un de ses courtiers, en application de l'art. L.716-6 CPI, le juge des référés a refusé d'ordonner qu'il soit mis fin sous astreinte à ladite contrefaçon — par le retrait desdites marques des sites internet en cause— estimant que le demandeur n'avait pas rapporté la preuve du caractère vraisemblable de l'atteinte à la marque par le défendeur, et ce, d'autant plus que l'éditeur du site internet sur lequel l'atteinte avait été constatée n'avait pas pu être identifié.

---

14 TGI Paris, 3ème ch., réf., 4 décembre 2014, n°14/03236, disponible sur: www.legalis.net (30.04.2015).

15 TGI Paris, 3ème ch., 1ère sect., 2 avril 2015, n°14/08177, disponible sur: www.legalis.net (08.04.2015).

16 Art. L.716-6 CPI.

17 Ibidem.

18 Ibidem.

En ce qui concerne le fond du litige en contrefaçon de marque, les art. L.716-13 et L.716-15 CPI permettent au juge d'ordonner le retrait, la destruction ou la confiscation des produits contrefaisants ainsi que des matériaux et instruments liés à ces contrefaçons. Sur internet, ces mesures concernent toutefois les hébergeurs et les éditeurs des sites internet en cause (voir ci-dessous, section 2.2.2); elles sont ordonnées tant par le juge civil que par le juge pénal.

En ce qui concerne la protection des **noms de domaine**, lorsque le signe dont l'usage est contrefaisant est un nom de domaine, le titulaire de la marque contrefaite peut demander l'annulation de l'enregistrement du nom de domaine ou même le transfert à son profit du nom de domaine en cause[19], ce qui implique le blocage du site internet correspondant au nom de domaine en cause.

Enfin, on relève que le 11 mars 2015, la Ministre de la Culture et de la Communication a présenté en Conseil des ministres une communication relative à la lutte contre le piratage des œuvres sur internet. Ce plan d'action vise notamment à développer le recours aux procédures de référé, de référé d'heure à heure, de requête simple ou de requête conjointe dans les recours judiciaires permettant de suivre dans le temps l'effectivité des mesures, notamment de blocage, prononcées à l'encontre des intermédiaires techniques. De plus, le plan propose aussi de mettre en place une centralisation régionale de l'action judiciaire dans le domaine[20]. Ces mesures ne sont toutefois qu'à l'état de projet à la date de rédaction du présent rapport.

2.1.3. La protection de la vie privée et des données personnelles

Les mesures pour mettre fin aux atteintes portées sur internet à la vie privée, au droit à l'image ainsi qu'aux données personnelles d'une personne visent surtout - et logiquement – le retrait du contenu illicite d'internet. Nous y reviendrons dans le cadre de la section 2.2.3.

On relève toutefois qu'en application de l'art. 9 du Code civil, le juge civil peut prescrire, y compris en référé, toutes mesures «propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée». Cependant, d'autres bases légales d'action sont plus propices à la matière du numérique. Ainsi, comme énoncé dans la section 2.1.1, en application de la LCEN, les FAI (de même que les autres acteurs d'ailleurs) peuvent être contraints, **par la voie judiciaire**, à faire cesser ou à prévenir le dommage occasionné par le contenu d'un site internet.

La question de l'étendue des pouvoirs du juge à l'encontre des FAI dans le cadre de l'art. 6, I, 8 LCEN s'est posée devant les juridictions françaises dans une affaire dans laquelle le Ministère de l'Intérieur avait entendu lutter contre une série de sites internet qui dénonçaient les violations policières en France et qui, ce faisant, diffusaient des propos injurieux et diffamatoires envers l'administration publique (en particulier la police) ainsi que des données personnelles collectées à l'insu des personnes concernées. Dans une décision du 10 février 2012, le tribunal de grande instance de Paris a ordonné que l'accès à l'un des sites concernés soit bloqué par les différents FAI, pour une durée de six mois. Ce faisant, conformément à ce que prévoit l'art. 6, I, 8 LCEN, le tribunal a précisé qu'il était démontré en l'espèce concernant ce site que les hébergeurs ou les éditeurs du site internet en cause n'avaient pas pu être identifiés malgré les démarches entreprises par le Ministère de l'Intérieur sur ce point. En ce qui concerne d'autres sites internet sur lesquels portait également la demande en

---

19 Art. L.45-2, 2° et L.45-6 Code des postes et télécommunications électroniques. Voir aussi: Com. 9 juin 2009, Prop. Ind. 2009, comm. 61.

20 Ministère de la Culture et de la Communication, Plan d'action pour la lutte contre le piratage, 11 mars 2015, disponible sous: www.culturecommunication.gouv.fr *(30.04.2015).*

justice, le tribunal a décidé que le blocage n'était pas opportun étant donné que le Ministère de l'Intérieur n'avait pas indiqué s'il avait tenté ou non d'identifier leurs hébergeurs et éditeurs.

2.2. Retrait de contenu illégal d'internet

2.2.1. En matière de protection de la sécurité nationale et des bonnes mœurs

Comme exposé ci-avant (voir section 2.1.1.), le droit français prévoit la possibilité pour les juges en matière civile d'ordonner, en référé ou pas, aux fournisseurs d'hébergement ou hébergeurs, toutes mesures aux fins de faire cesser ou de prévenir un dommage occasionné par le contenu d'un service de communication au public en ligne. Comme le précise l'art. 6, I, 8 LCEN, les juges adresseront leurs mesures d'abord aux hébergeurs, et seulement si ceux-ci ne sont pas connus, aux FAI.

De plus, la LCEN met en place un dispositif organisant le retrait d'internet, par les hébergeurs, de contenus illicites. Ce système, présent dans plusieurs juridictions, est connu sous l'expression «*notice and take-down*». A cet égard, la LCEN prévoit que la responsabilité civile des hébergeurs ne peut pas être engagée «du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible»[21].

Ainsi, il ne peut y avoir retrait de contenu d'internet s'il n'y a pas, par l'hébergeur, **connaissance effective du caractère illicite** du contenu. Pour faciliter la preuve de la connaissance effective du caractère illicite du contenu, la loi pose une **présomption simple de connaissance des faits litigieux** par l'hébergeur lorsqu'il reçoit notification de différents éléments énumérés par la LCEN, tels que la date des faits, leur description, leur localisation, les motifs pour lesquels le contenu doit être retiré avec mention des dispositions légales et les justifications de fait, copie de la correspondance adressées à l'auteur ou l'éditeur des informations par laquelle il est demandé leur interruption, leur retrait ou modification ou justification de ce que l'auteur ou l'éditeur n'a pu être contacté. Cette procédure de notification facultative permet de démontrer la connaissance par l'hébergeur du contenu illicite qu'il héberge, et ainsi, le contraindre à agir promptement. Ceci dit, d'après le texte de la loi, si la notification permet de présumer la connaissance effective du caractère illicite du contenu, cette connaissance peut également être prouvée par tous autres moyens.

Il ne suffit pas de notifier l'existence d'un contenu illicite pour que l'hébergeur soit reconnu responsable faute d'avoir retiré promptement ledit contenu d'internet. L'hébergeur conserve une **marge d'appréciation**: il est libre de retirer le contenu notifié comme illicite; il ne sera toutefois contraint de le faire que dans des circonstances particulières. En effet, en application d'une réserve d'interprétation du Conseil Constitutionnel:

> «Ces dispositions [relatives à la responsabilité des hébergeurs] ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge»[22].

Ainsi, en l'absence d'une injonction judiciaire, l'hébergeur n'est tenu de rendre inaccessible le contenu illicite présent sur internet que si celui-ci présente un **caractère manifestement illicite**[23]. L'hébergeur ne sera ainsi pas sanctionné pour ne pas avoir retiré un contenu dont le caractère illicite n'est pas évident. Initialement, la notion de contenu manifestement illicite ne devait concerner que les contenus à caractère pédopornographique, incitant à la haine raciale ou faisant l'apologie d'un

---

21 Art. 6, I, 2 LCEN.

22 Const., 10 juin 2004, n° 2004-496 DC, disponible sous: www.conseil-constitutionnel.fr (30.04.2015).

23 Voir notamment C.A. Paris, 4 avril 2013, Pole 1, disponible sous: www.legalis.net (30.04.2015).

crime contre l'humanité. Cependant, plusieurs décisions judiciaires ont eu pour effet d'étendre la notion de manifestement illicite à de nouvelles catégories de contenus tels qu'en matière d'infractions aux droits d'auteur ou de diffamation (voir les sections 2.2.2 et 2.2.3). Selon un auteur, le caractère manifestement illicite des informations litigieuses est la conséquence d'un manquement délibéré à une disposition de droit positif explicite et dénuée d'ambiguïté[24]. De plus, compte tenu des modifications législatives intervenues récemment en vue de renforcer la lutte contre le terrorisme, il paraît raisonnable de considérer que des images ou propos constitutifs d'infractions pénales d'actes de provocation à des actes de terrorisme ou d'apologie du terrorisme hébergeurs constituent des contenus à caractère manifestement illicite, contraignant de ce fait les hébergeurs à rendre ces contenus inaccessibles, et ce, même sans intervention judiciaire, sous peine d'engager leur responsabilité civile et pénale.

Concernant ces mêmes infractions de pédopornographie ou d'actes de provocation à des actes de terrorisme et d'apologie du terrorisme, la LCEN prévoit également un blocage par simple décision administrative de l'OCLCTIC. En effet, en application de l'article 6-1 alinéa 1 de la LCEN, l'OCLCTIC peut demander aux fournisseurs d'hébergement sur internet des sites en cause ou aux éditeurs de retirer ces contenus d'internet. Ce faisant, l'autorité administrative est tenue d'en informer simultanément les fournisseurs d'accès. En l'absence de retrait de ces contenus dans un délai de 24 heures, l'OCLCTIC pourra notifier aux FAI la liste des sites en cause qui devront alors empêcher sans délai l'accès à ces adresses.

En outre, d'après la LCEN, l'OCLCTIC peut notifier les adresses électroniques des sites concernés par ces deux types d'infractions pénales aux moteurs de recherche ou aux annuaires, lesquels sont alors tenus de prendre toutes les mesures utiles pour faire **cesser le référencement** du site en cause.

Complétant le décret du 5 février 2015, le décret n° 2015-253 du 4 mars 2015 vient préciser les modalités de déréférencement des sites contrevenant aux dispositions des articles 227-23 et 421-2-5 du code pénal. Aux termes de ce décret, l'OCLCTIC est autorisée à notifier aux exploitants de moteurs de recherche ou d'annuaires, les adresses électroniques de ces sites illicites, à des fins de déréférencement. Ce déréférencement peut être demandé même pour des sites dont le blocage administratif a déjà été demandé. Comme les FAI, les exploitants de moteurs de recherche ou d'annuaires, qui ne peuvent modifier la liste d'adresses et doivent préserver la confidentialité des données qui leur sont confiées, ont alors quarante-huit heures pour prendre toute mesure utile destinée à faire cesser le référencement des sites internet concernés. L'OCLCTIC devra en outre vérifier au moins une fois par trimestre que ces adresses renvoient toujours à un contenu illicite.

2.2.2. La protection des droits intellectuels

Certaines des mesures de retrait de sites d'internet au motif que leur contenu contrevient aux droits intellectuels sont fondées sur les mêmes dispositions que les mesures de blocages examinées ci-avant (voir ci-dessus, section 2.1.2). Il en irait ainsi des injonctions judiciaires de cesser le dommage résultant d'un site internet ou de l'empêcher, rendues en application de l'art. 6, I, 8 LCEN (voir ci-dessus, section 2.1.2).

Le domaine de la protection des droits intellectuels comprend ceci dit des dispositions légales ayant le même effet mais étant spécifiques au domaine en cause. Ainsi, l'art. L.336-2 CPI prévoit qu'en présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner à la demande des titulaires de droits sur les œuvres et objets

[24] C. Castets-Renard, Droit de l'internet: droit français et européen, Paris, 2012, p. 295, n°789.

protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits d'auteur ou des organismes de défense professionnelle, **toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier.**

En outre, la procédure de «*notice and take down*» présentée ci-dessus (voir section 2.2.1) étant d'application générale, elle est également valable en ce qui concerne les sites internet violant les droits intellectuels. L'utilisateur peut notifier à l'hébergeur du site l'existence d'un contenu illicite; dès qu'il en est prévenu, celui-ci est contraint de retirer le contenu qui est manifestement illicite; il reste par contre libre de retirer le contenu qui ne présente pas de caractère *manifestement* illicite. Dans le domaine des droits intellectuels, il sera souvent difficile d'établir le caractère *manifestement* illicite du contenu d'un site. En effet, l'appréciation du caractère contrefaisant de l'usage d'une marque ou d'une œuvre nécessite le plus souvent une appréciation des circonstances ayant entouré la diffusion en cause, ce qui par principe échappe à l'intermédiaire technique qu'est l'hébergeur. Ainsi, le tribunal de grande instance de Paris a eu l'occasion de se prononcer sur la contrefaçon d'une marque dans une affaire portée par des sociétés du groupe H&M à l'encontre de Google et Youtube concernant l'hébergement par ces dernières sociétés de vidéos associant la marque H&M à des images de sang et aux termes notamment de «Haine et Mort» et «Harcèlement et Mort». Saisi au stade des référés, le tribunal a décidé que l'usage de la marque sur le site internet en cause «ne vise pas plus à désigner qu'à promouvoir un produit qui serait offert à la vente, mais seulement à informer l'internaute du comportement éventuel de la société titulaire de la marque en question, de sorte qu'il n'a pas pour but de renseigner le consommateur sur la nature ou l'origine d'un produit et n'est nullement utilisé dans la vie des affaires»; pour cette raison, il a été jugé que la contrefaçon de la marque n'apparaît pas vraisemblable et que l'hébergeur n'a pas commis de faute en ne retirant pas le contenu en cause, qui n'est pas manifestement illicite. Cela n'a pas empêché le juge des référés d'ordonner, dans un souci d'apaisement, que le contenu du site, dont le caractère manifestement illicite n'est pas établi, soit retiré ou rendu inaccessible au motif que son maintien serait de nature à causer au demandeur un préjudice qu'il convient d'éviter[25].

D'autres dispositions du CPI permettent au juge d'ordonner des mesures spécifiques telles que la **confiscation ou la destruction** des produits contrefaits ou violant les droits d'auteur, de même que le **retrait de ces produits des circuits commerciaux**. Ainsi, l'art. L.331-1-4 CPI prévoit que:

> «en cas de condamnation civile pour contrefaçon, atteinte à un droit voisin du droit d'auteur ou aux droits du producteur de bases de données, la juridiction peut ordonner, à la demande de la partie lésée, que les objets réalisés ou fabriqués portant atteinte à ces droits, les supports utilisés pour recueillir les données extraites illégalement de la base de données et les matériaux ou instruments ayant principalement servi à leur réalisation ou fabrication soient rappelés des circuits commerciaux, écartés définitivement de ces circuits, détruits ou confisqués au profit de la partie lésée».

Il en va de même dans le domaine des marques notamment, l'art. L.716-13 CPI disposant que:

> «Les personnes physiques coupables de [certains délits de contrefaçon de marque, en particulier le fait d'importer, d'exporter ou de produire des marchandises sous une marque contrefaisante en vue de vendre, fournir, offrir à la vente ou louer ces marchandises ou encore le fait de détenir sans motif légitime des marchandises sous une marque contrefaisante, le fait de reproduire, imiter, utiliser une marque ou encore le fait de sciemment livrer un produit ou service autre que celui qui demandé sous la marque

---

25 TGI, Paris, ord. réf., 4 avril 2013, RLDI 2013/94 n°3129.

enregistrée[26]] peuvent être condamnées, à leurs frais, à retirer des circuits commerciaux les objets jugés contrefaisants et toute chose qui a servi ou était destinée à commettre l'infraction.

La juridiction peut ordonner la destruction aux frais du condamné ou la remise à la partie lésée des objets et choses retirés des circuits commerciaux ou confisqués.»

Ainsi, en ce qu'elles peuvent contraindre l'hébergeur ou l'éditeur du site de retirer les produits concernés de son site internet de vente en ligne, ces mesures constituent des mesures de retrait de contenu illicite d'internet. Ceci dit, même lorsqu'il n'y a pas de disposition spécifique permettant d'ordonner l'interdiction de mettre en ligne les produits contrefaisants, la jurisprudence estime que les mesures d'interdiction de poursuivre une activité jugée en violation des dispositions de protection des droits intellectuels, constitue l'une des modalités de la réparation intégrale du préjudice dont le juge civil apprécie souverainement la pertinence, et ce, même en l'absence de texte la prévoyant. C'est ce qu'a fait le tribunal de grande instance de Paris dans une affaire dans laquelle la société nationale des chemins de fer français se plaignait de la contrefaçon, par l'éditeur d'un site internet, de ses marques aux fins d'un usage lui portant préjudice[27].

Enfin, quant au fait pour l'hébergeur ainsi qu'au service de référencement d'empêcher qu'un contenu illicite retiré d'internet soit remis en ligne en particulier via une autre adresse url, la Cour de Cassation a décidé, par trois arrêts, que l'hébergeur de même que le service de référencement ne pouvaient être tenus responsables pour n'avoir pas empêché toute remise en ligne du contenu illicite

---

26 Art. L.716-9 CPI: «Est puni de quatre ans d'emprisonnement et de 400 000 euros d'amende le fait pour toute personne, en vue de vendre, fournir, offrir à la vente ou louer des marchandises présentées sous une marque contrefaite:
a) D'importer, d'exporter, de réexporter ou de transborder des marchandises présentées sous une marque contrefaisante;
b) De produire industriellement des marchandises présentées sous une marque contrefaisante;
c) De donner des instructions ou des ordres pour la commission des actes visés aux a et b.
Lorsque les délits prévus au présent article ont été commis en bande organisée ou sur un réseau de communication au public en ligne ou lorsque les faits portent sur des marchandises dangereuses pour la santé, la sécurité de l'homme ou l'animal, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende.»
Art. L.716-10 CPI: «Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait pour toute personne:
a) De détenir sans motif légitime, d'importer ou d'exporter des marchandises présentées sous une marque contrefaisante;
b) D'offrir à la vente ou de vendre des marchandises présentées sous une marque contrefaisante;
c) De reproduire, d'imiter, d'utiliser, d'apposer, de supprimer, de modifier une marque, une marque collective ou une marque collective de certification en violation des droits conférés par son enregistrement et des interdictions qui découlent de celui-ci. L'infraction, prévue dans les conditions prévues au présent c, n'est pas constituée lorsqu'un logiciel d'aide à la prescription permet, si le prescripteur le décide, de prescrire en dénomination commune internationale, selon les règles de bonne pratique prévues à l'article L. 161-38 du code de la sécurité sociale;
d) De sciemment livrer un produit ou fournir un service autre que celui qui lui est demandé sous une marque enregistrée.
L'infraction, dans les conditions prévues au d, n'est pas constituée en cas d'exercice par un pharmacien de la faculté de substitution prévue à l'article L. 5125-23 du code de la santé publique.
Lorsque les délits prévus aux a à d ont été commis en bande organisée ou sur un réseau de communication au public en ligne ou lorsque les faits portent sur des marchandises dangereuses pour la santé ou la sécurité de l'homme ou l'animal, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende.»

27 TGI Paris, 3ème ch., 2ème section, 11 juin 2010, disponible sous: www.legalis.net (30.04.2015).

retiré, en l'absence d'une autre notification les avisant de la remise en ligne du contenu illicite déjà retiré conformément à la procédure de «*notice and take down*». Ce faisant, la Cour de Cassation indique que contraindre ces acteurs d'internet à empêcher toute remise en ligne aboutirait à les soumettre à une obligation générale de surveillance des images qu'ils stockent et de recherche des reproductions illicites et à leur prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps[28].

2.2.3. La protection des droits relatifs à la vie privée

En matière d'atteinte à la vie privée, le Code civil français prévoit, en son art. 9, la possibilité pour le juge civil de, «sans préjudice de la réparation du dommage subi, prescrire toutes mesures (…) propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée». Ces mesures peuvent, s'il y a urgence, être ordonnées en référé. A ce titre, la Cour de Cassation a précisé que la seule constatation de l'atteinte caractérise l'urgence.

Cependant, d'autres bases légales sont plus propices au domaine numérique. Il en va ainsi de la possibilité pour les juges en matière civile d'ordonner, en référé ou pas, aux fournisseurs d'hébergement ou hébergeurs, toutes mesures aux fins de faire cesser ou de prévenir un dommage occasionné par le contenu d'un service de communication au public en ligne (voir ci-dessus, section 2.1.3). Comme le précise l'art. 6, I, 8 LCEN, les juges adresseront leurs mesures d'abord aux hébergeurs, et seulement si ceux-ci ne sont pas connus, aux FAI.

De même, la procédure de «*notice and take down*» présentée ci-dessus (voir section 2.2.1) étant d'application générale, elle est également valable en ce qui concerne les sites internet constituant une violation de la vie privée de tiers. L'utilisateur peut notifier à l'hébergeur du site l'existence d'un contenu illicite; dès qu'il en est prévenu, celui-ci est contraint de retirer le contenu qui est manifestement illicite; il reste par contre libre de retirer ou non le contenu qui ne présente pas de caractère *manifestement* illicite. Dans le domaine de la protection de la vie privée, de la diffamation etc., il peut être difficile d'établir le caractère *manifestement* illicite du contenu d'un site.

Selon un auteur, un contenu est manifestement illicite s'il est la conséquence d'un manquement délibéré à une disposition de droit positif explicite et dénuée d'ambiguïté, et donne pour exemple des propos révisionnistes et antisémites. La jurisprudence semble en effet adopter une approche restrictive quant à ce qu'elle considère comme étant un contenu manifestement illicite. En matière de diffamation, on relève que dans une affaire ayant opposé des sociétés du groupe H&M à plusieurs hébergeurs de sites internet, le tribunal de grande instance a décidé, au stade des référés, que l'appréciation du caractère éventuellement diffamatoire du contenu de ces sites internet supposait une analyse des circonstances ayant présidé à leur diffusion, laquelle échappait par principe à celui qui n'est qu'un intermédiaire technique. Le tribunal en a conclu que les hébergeurs n'avaient pas commis de faute en considérant que ces propos, éventuellement diffamatoires, n'étaient pas manifestement illicites[29]. Dans le même sens, la Cour d'appel de Paris a considéré que la diffusion sur un site internet d'un article reproduisant des propos de la demanderesse en les critiquant

---

[28] Cass. civ. 12 juillet 2012, n°11-15.165, 11-13.669 et n° 11-13.666, disponible sous: www.legalis.net; A. Casanova, La Cour de Cassation préfère le «notice and take down» au «notice and stay down», au risque de voir les ayants droit «knocked down», Hebdo édition affaires n°307, 6 septembre 2012, Lexbase, n°N3328BTG.

[29] TGI, Paris, ord. réf., 4 avril 2013, disponible sous: www.legalis.net (30.04.2015). Pour plus d'informations sur cette affaire, voir section 2.2.2 ci-avant.

fermement, ne constituait pas un contenu manifestement illicite de nature à justifier une mesure de retrait[30].

Enfin, il convient de relever que les mesures de déréférencement sont désormais reconnues par une jurisprudence française récente[31], s'appuyant sur la jurisprudence de la Cour de Justice de l'Union européenne[32] qui consacre un droit pour tout ressortissant européen au déréférencement d'un contenu liée à sa vie privée, c'est-à-dire l'effacement des liens pointant vers des pages internet sur lesquelles son nom ou des informations le concernant sont présentes, sans pour autant que ces informations soient effacées du site source.

2.2.4. La protection des données personnelles

En matière de protection des données personnelles, on relève que la Commission nationale de l'informatique et des libertés (la «CNIL») dispose de pouvoirs exceptionnels en vue de mettre fin à tout traitement de données personnelles qui ne respecterait pas les conditions posées par la loi 78-17 du 6 janvier 1978 sur l'informatique, les fichiers et les libertés[33]. Quant aux conditions imposées pour le traitement de données à caractère personnel, la loi 78-17 précitée impose notamment, en fonction du type de traitement en considération, un régime de déclaration ou d'autorisation préalable par la CNIL, voire un régime d'interdiction de traitement de certaines données à caractère personnel. Ainsi, la formation restreinte de la CNIL est en mesure d'ordonner audit responsable du traitement de cesser le traitement en cause lorsque celui-ci relève d'une obligation de déclaration ou de lui retirer l'autorisation lorsqu'une telle autorisation lui a été accordée par la CNIL préalablement au traitement. Cette décision intervient après une procédure contradictoire et dans l'hypothèse où le responsable de traitement ne s'est pas conformé à la mise en demeure que lui a adressée la CNIL[34]. De plus, si le traitement de données à caractère personnel entraîne la violation des libertés, telles que l'identité humaine, les droits de l'homme, la vie privée, les libertés individuelles et publiques, la

---

30 CA, Paris, pôle 1, 2ème ch., 4 avril 2013, disponible sous: www.legalis.net (30.04.2015).

31 TGI de Paris, ord. réf., 19 décembre 2014, Marie France M. c. Google France et Google Inc., disponible sous : www.legalis.net.

32 CJUE, arrêt de grande chambre C-131/12, 13 mai 2014, demande de décision préjudicielle, Google Spain SL, Google Inc. c. AEPD, Mario Costeja González, disponible sous: www.curia.europa.eu.

33 Loi 78-17 du 6 janvier 1978 sur l'informatique, les fichiers et les libertés, disponible sous: www.legifrance.gouv.fr (30.04.2015). L'art. 2 de cette loi en précise le champ d'application: Celle-ci s'applique «aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions [du champ d'application territorial prévues à l'art. 5 de la loi].
Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.
Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction».

34 Art. 45 I de la loi 78-17 du 6 janvier 1978 sur l'informatique, les fichiers et les libertés, disponible sous: www.legifrance.gouv.fr (30.04.2015).

CNIL peut engager une procédure d'urgence. Au terme de cette procédure, la CNIL peut décider d'interrompre le traitement pour une durée maximale de trois mois ou de verrouiller les données en cause pour la même durée maximale, ou encore, lorsque le traitement en cause est mis en œuvre par l'Etat, d'informer le Premier Ministre pour qu'il prenne les mesures pour faire cesser la violation constatée. Enfin, en cas d'atteinte grave et immédiate aux droits et libertés susmentionnées, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés[35].

3. Questions de procédure

3.1. Blocage et retrait d'ordre administratif

La procédure aboutissant au blocage administratif des sites internet diffusant des images constitutives des infractions pénales de pédopornographie ainsi que de provocation à des actes terroristes ou d'apologie du terrorisme, telle que prévue par la LCEN, est décrite dans le décret du 5 février 2015 relatif **au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.**

D'après ce décret du 5 février 2015, l'autorité administrative en charge du blocage et/ou du retrait administratif de ces sites internet est la direction générale de la **police nationale**, **Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication** («OCLCTIC»). Au sein de cette autorité administrative, **seuls certains agents individuellement désignés** et dûment habilités par le chef de l'office sont autorisés à mettre en œuvre la procédure de blocage[36].

D'après l'art. 6-1 LCEN, l'OCLCTIC doit d'abord solliciter le retrait du contenu illicite auprès de l'hébergeur et/ou l'éditeur. Ce faisant, l'alinéa 1er de l'art. 6-1 LCEN prévoit qu'il est **tenu d'informer simultanément les FA**I. L'hébergeur et/ou l'éditeur disposent d'un délai de 24 heures pour retirer le contenu illicite.

Au cas où l'OCLCTIC serait dans l'impossibilité de contacter le l'éditeur ou l'hébergeur en vue de requérir le retrait du contenu illicite – et ce, alors que les données de ces personnes doivent légalement être mises à la disposition du public –, le même OCLCTIC peut requérir le blocage du site internet directement auprès du FAI, sans solliciter préalablement le retrait du contenu auprès de l'hébergeur ou de l'éditeur. L'OCLCTIC procède également au blocage auprès des FAI si le contenu illicite n'a pas été retiré par l'hébergeur ou l'éditeur dans un délai de 24 heures.

La **transmission des adresses électroniques** concernées aux FAI en vue du blocage s'effectue selon un **mode sécurisé** qui en garantit l'intégrité et la confidentialité. De plus, les adresses électroniques concernées comportent soit un nom de domaine, soit un nom d'hôte caractérisé par un nom de domaine précédé du nom de serveur. Les **FAI ne peuvent pas modifier la liste des adresses électroniques concernées** par l'ordre de blocage, que ce soit par ajout, suppression ou altération et elles sont tenues de préserver la confidentialité des données qui leur sont confiées.

---

35 Art. 45 II et III de la loi 78-17 du 6 janvier 1978 sur l'informatique, les fichiers et les libertés, disponible sous: www.legifrance.gouv.fr (30.04.2015).

36 Voir plus d'informations ci-dessus, section 2.1.1.

Les utilisateurs des services de communication au public en ligne auxquels l'accès est empêché sont dirigés vers **une page d'information du ministère de l'intérieur**, indiquant pour chacun des deux cas de blocage (sites pédopornographiques et sites provoquant à des actes de terrorisme ou en faisant l'apologie) les motifs de la mesure de protection et les voies de recours. Certaines personnes conservent un accès aux adresses électroniques des services de communication au public en ligne auxquels l'accès est empêché: il s'agit des agents de l'OCLCTIC, individuellement désignés et dûment habilités par l'autorité hiérarchique dont ils relèvent ainsi qu'une personnalité qualifiée désignée en son sein par la Commission nationale de l'informatique et des libertés (CNIL), dont la mission est de s'assurer de la régularité des demandes de retrait et blocage et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste des adresses électroniques concernées. Cette personnalité qualifiée de la CNIL peut à tout moment recommander de mettre fin à une mesure de blocage et/ou de retrait si elle constate une irrégularité. Si l'OCLCTIC ne suit pas sa recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête.

La mesure de blocage du site internet en cause peut faire l'objet des recours réguliers en matière administrative et judiciaire. Ainsi, la décision administrative de bloquer un site internet peut faire l'objet d'un recours administratif gracieux ou hiérarchique au terme duquel le réexamen du dossier par l'autorité administrative est sollicité. Le recours administratif est porté devant la même administration (recours gracieux), l'OCLCTIC, ou devant son supérieur hiérarchique (recours hiérarchique), en l'espèce le Ministre de l'Intérieur. Si cette voie de recours n'aboutit pas à une modification de la situation, l'administré peut encore introduire un recours contentieux, en saisissant le tribunal administratif compétent, puis en appel, la Cour d'appel administrative; enfin, en dernier lieu, il est également possible d'introduire un recours en cassation devant le Conseil d'Etat.

L'OCLCTIC **vérifie au moins chaque trimestre** que le contenu du service de communication contrevenant présente toujours un caractère illicite. Lorsque ce service a disparu ou que son contenu ne présente plus de caractère illicite, l'Office retire de la liste les adresses électroniques correspondantes et notifie sans délai ce retrait à la personnalité qualifiée de la CNIL et aux FAI. Dans un délai de vingt-quatre heures suivant cette notification, ceux-ci rétablissent par tout moyen approprié l'accès aux services fournis par les adresses électroniques retirées de la liste et le transfert vers ces services.

Le décret 2015-125 prévoit encore que **les éventuels surcoûts** résultant des obligations mises à la charge des fournisseurs d'accès en matière de blocage administratif de sites internet font l'objet d'une **compensation financière prise en charge par l'Etat**. Le terme de «surcoût» désigne les coûts des investissements et interventions spécifiques supplémentaires résultant de ces obligations.

Pour obtenir une compensation, les fournisseurs d'accès adressent à l'OCLCTIC un document détaillant le nombre et la nature des interventions nécessaires ainsi que le coût de l'investissement éventuellement réalisé. Le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies analyse le document transmis, notamment au regard des coûts habituellement estimés dans le secteur concerné. L'Etat procède, sur présentation d'une facture, au paiement des compensations correspondant aux surcoûts justifiés au vu de l'analyse du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies.

Le décret n° 2015-253 du 4 mars 2015, pris en application des nouvelles dispositions de la LCEN introduites par la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, **détaille la procédure en matière de déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. En vertu de ce décret, l'OCLCTIC notifie aux exploitants de**

moteurs de recherche ou d'annuaires les adresses électroniques **dont le référencement doit être bloqué en application de l'art**. 6-1 LCEN. Ces adresses sont transmises sous un mode sécurisé en garantissant la confidentialité et l'intégrité. Dans un délai de quarante-huit heures suivant la notification, les exploitants de moteurs de recherche ou d'annuaires prennent toute mesure utile destinée à faire cesser le référencement de ces adresses. Ils ne modifient pas les adresses électroniques, que ce soit par ajout, suppression ou altération, et préservent la confidentialité des données qui leur sont ainsi confiées. La personnalité qualifiée désignée en son sein par la Commission nationale de l'informatique et des libertés exerce ses fonctions de contrôle de la régularité des procédures de déréférencement de la même manière que dans le cadre du blocage administratif de sites internet. Les voies de recours ouvertes aux administrés sont également les mêmes que dans le cadre du blocage administratif de sites internet.

3.2. Blocage et retrait d'ordre judiciaire

Les autres mesures de retrait ou de blocage de sites internet, exposées ci-avant, sont ordonnées par le juge de **l'ordre judiciaire**: il s'agit essentiellement de la possibilité pour le juge d'ordonner, en référé ou sur requête, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un site internet (art. 6, I, 8 LCEN) [37]; la même possibilité existe en matière de droits d'auteur et droits voisins (art. 336-2 CPI)[38] de même qu'en matière d'atteinte à la vie privée (art. 9 CC)[39].

Comme tout jugement, ces injonctions judiciaires sont notifiées aux parties défenderesses soit les FAI, les hébergeurs, les éditeurs, les moteurs de recherche, etc. A défaut d'exécution volontaire par les parties concernées, les injonctions judiciaires peuvent, en principe, faire l'objet d'une exécution forcée. Les parties perdantes peuvent, le cas échéant, introduire un recours de droit commun contre les jugements rendus en premier ressort devant la Cour d'appel, puis un pourvoi en cassation devant la Cour de Cassation.

4. Surveillance générale d'internet

D'après la LCEN, **les hébergeurs et les FAI ne sont pas soumis à une obligation générale de surveiller** les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Cette interdiction a encore récemment été rappelée par la Cour de Cassation, lorsqu'elle a indiqué que contraindre les acteurs d'internet à empêcher toute remise en ligne d'un contenu illicite retiré par leurs soins après notification régulière par des utilisateurs, aboutirait à les soumettre à une obligation générale de surveillance des images qu'ils stockent et de recherche des reproductions illicites, ce qui ne peut être admis[40].
La LCEN prévoit que ces acteurs d'internet peuvent toutefois être requis par l'autorité judiciaire d'opérer une **surveillance ciblée et temporaire**. Ainsi, on relève par exemple que le tribunal de commerce de Paris a ordonné, en référé, la suppression d'annonces proposant la vente de parfums en dehors du réseau de distribution sélective agréé ainsi que la mise en place, pendant une période

---

37 Voir les sections 2.1.1 et 2.1.2.

38 Voir les sections 2.1.2 et 2.2.2.

39 Voir les sections 2.1.3 et 2.2.3.

40 Cass. civ. 12 juillet 2012, n°11-15.165, 11-13.669 et n° 11-13.666, disponible sous: www.legalis.net; A. Casanova, La Cour de Cassation préfère le «notice and take down» au «notice and stay down», au risque de voir les ayants droit «knocked down», Hebdo édition affaires n°307, 6 septembre 2012, Lexbase, n°N3328BTG.

de six mois, d'un système de filtrage a priori permettant de détecter et de retirer les annonces relatives à des produits des marques concernées[41].

Les intermédiaires d'internet sont en outre tenus de mettre en place un dispositif permettant à toute personne de **porter à leur connaissance** toutes données relatives à la répression des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, ainsi que des atteintes à la dignité humaine[42]. Ils ont également **l'obligation de signaler aux autorités publiques** compétentes toute activité illicite qui leur serait signalées et qu'exerceraient les destinataires de leurs services[43].

En outre, les services de la police compétents dans le domaine, **l'OCLCTIC**, exercent une surveillance de l'internet, à la recherche d'éventuelles infractions pénales. Cette surveillance s'exerce en vue de la poursuite des auteurs de ces infractions pénales[44] mais aussi en vue de l'exercice éventuel des prérogatives de ce service en matière de blocage et/ou retrait de certains contenus illicites pour certaines de ces infractions. Comme exposé ci-avant en ce qui concerne les mesures de retrait et de blocage administratifs exercées par l'OCLCTIC, il s'agit des contenus qui sont constitutifs des infractions pénales de pédopornographie et d'actes d'incitation au terrorisme et de son apologie[45]. Cette surveillance s'exerce de l'initiative propre de l'OCLCTIC mais aussi par le biais d'un **dispositif de signalement**, disponible sur internet, permettant à tout utilisateur de signaler tout comportement illicite sur internet[46]. Un système de traitement de ces signalements, dénommé Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements (PHAROS), a également été mis en place; celle-ci permet aux agents de police spécialement affectés à cette plateforme relevant de l'OCLCTIC de traiter les signalements en vue d'aboutir, le cas échéant, à la poursuite des auteurs des infractions pénales identifiées et/ou au blocage et/ou retrait du contenu internet illicite[47].

De plus, il convient de préciser que le Code de la sécurité intérieure(CSI) prévoit la possibilité de recueillir des renseignements avec l'aide des opérateurs d'internet en vue de protéger la sécurité nationale, de sauvegarder les éléments essentiels du potentiel scientifique et économique de la France, ou prévenir le terrorisme, la criminalité et la délinquance organisées et la reconstitution ou le maintien de groupements dissous en application de la loi. Ainsi, l'art. L. 851-1 CSI prévoit qu'aux fins susmentionnées, **peut être autorisé le recueil, auprès des FAI et des hébergeurs, des informations**

---

41 T. com., Paris, réf., 26 juillet 2007 et 31 octobre 2007, disponible sous: www.legalis.net (30.04.2015).

42 Art. 6, I, 7, al. 3 et 4 LCEN.

43 Art. 6, I, 7, al. 4 LCEN.

44 Les moyens de surveillance mis à disposition des services de police judiciaire ont notamment été renforcés par la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. L'art. 706-87-1 du code de procédure pénale prévoit notamment que certains actes commis par les services compétents de la police judiciaire en vue de la constatation d'infractions commises sur internet, tels que la prise de contact sous un pseudonyme avec les personnes susceptibles d'être les auteurs d'infractions, ne sont pas punissables dans le chef des agents concernés.

45 Voir, ci-dessus, les sections 2.1.1 et 2.2.1.

46 Voir le site: https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action (30.04.2015).

47 **Arrêté du 16 juin 2009 portant création d'un système dénommé «PHARO » (plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), disponible sous: www.legifrance.gouv.fr (30.04.2015).**

ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications[48].

En outre, la **Loi relative au renseignement** a été promulguée le 24 Juillet 2015[49]. La Loi vise à créer un cadre légal général aux activités des services de renseignement, celui-ci étant inexistant jusqu'à présent. En application de cette loi, le Premier Ministre peut, sur avis de la Commission nationale de contrôle des techniques de renseignement, une nouvelle autorité administrative indépendante, imposer aux FAI et aux hébergeurs en particulier, de mettre en œuvre, sur les informations traitées par eux, un dispositif destiné à révéler, sur la seule base d'un traitement automatisé d'éléments anonymes, une menace à caractère terroriste. Ce dispositif ne vaut que pour les besoins de la prévention du terrorisme. La loi prévoit que si une telle menace s'avère réelle, le Premier Ministre pourrait décider de lever l'anonymat[50].

Enfin, après les attaques terroristes contre le journal français Charlie Hebdo, le gouvernement a présenté un plan national de lutte contre le racisme et l'antisémitisme, dont un des aspects est la lutte contre la propagation du racisme et de l'antisémitisme sur l'internet. En particulier, le gouvernement a annoncé son intention d'établir une unité nationale de lutte contre la haine sur Internet[51] en charge de la mise en place de " cyberpatrouilles " destinées à rechercher sur internet le contenu à caractère raciste ou antisémite le plus emblématique et le plus partagé et de réaliser des enquêtes en vue de poursuites pénales. Notre recherche n'a pas jusqu'ici permis d'identifier des mesures législatives ou réglementaires concrètes en vue de mettre en place ce mécanisme de surveillance.

5. Evaluation au regard de la jurisprudence de la Cour européenne des droits de l'homme

La liberté d'expression est prévue dans la Déclaration des droits de l'homme et du citoyen de 1789 auquel le Préambule de la Constitution de la République française fait référence expresse. L'art. 11 de la Déclaration de 1789 dispose en effet comme suit:

> «La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme: tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi.»[52]

La LCEN rappelle en son article 1er son attachement à la liberté de la communication au public par voie électronique, et précise que:

---

48 Voir aussi les articles L.246-2 à 5 CSI pour plus d'informations sur la procédure d'accès administratif aux données de connexion.

49 Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, disponible sous: www.legifrance.gouv.fr (17.11.2015).

50 Art. L. 851-3 CSI.

51 Plan national de lutte contre le racisme et l'antisémitisme, 17 Avril 2015, disponible sous: http://www.gouvernement.fr/sites/default/files/liseuse/4040/master/index.htm.

52 Déclaration des droits de l'homme et du citoyen de 1789, disponible sous: www.legifrance.gouv.fr (30.04.2015).

> «[l]'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.»[53]

Les dispositions de cette loi relatives au blocage et retrait administratifs en présence de contenus internet illicite ont toutefois donné lieu à de vifs débats. Le décret du 5 février 2015 chargé de mettre en œuvre les dispositions récemment introduite dans la LCEN par la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme et le décret du 4 mars 2015 pris en ce qui concerne le déréférencement de sites visés par cette même loi, font l'objet d'un recours devant le Conseil d'Etat[54].

Le système de blocage administratif des **sites pédopornographiques**, initialement introduit en 2011 par la Loi d'orientation et de programmation pour la performance de la sécurité intérieure (dite «LOPPSI 2»), a été soumis, avant sa promulgation, au contrôle du Conseil Constitutionnel saisi par une partie des membres de l'Assemblée nationale et du Sénat. Dans sa décision du 10 mars 2011, le Conseil Constitutionnel a toutefois validé le dispositif en précisant que:

> «les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789»[55].

Ainsi, d'après le Conseil Constitutionnel français, le blocage de sites internet qui «diffusent des images de pornographie infantile» par simple décision administrative constitue une restriction aux libertés, en particulier la liberté d'expression, qui est proportionnée au but légitime défendu par ailleurs, soit la sauvegarde de l'ordre public. Elle offre par ailleurs une protection suffisante contre l'arbitraire et l'abus de droit étant donné que la décision administrative est encadrée par une loi et, surtout, qu'elle peut à tout moment être contestée devant un juge.

C'est renforcé par ce précédent que le Gouvernement a soumis au Parlement le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, qui a abouti à la loi du 13 novembre 2014 exposée ci-avant, et en application de laquelle l'OCLCTIC est en mesure de bloquer ou retirer non seulement les sites pédopornographiques mais également les sites dont le contenu provoque à des actes de terrorisme ou en fait l'apologie. Les défenseurs de ce dispositif de blocage administratif ainsi mis en place ont en effet rappelé la restriction faite aux libertés, en particulier la liberté d'expression, se justifiait par la nécessité d'assurer la sécurité nationale:

---

53 Art. 1er IV LCEN.

54 Conseil d'Etat (Association French Data Network et autres), disponible sous : www.arianeinternet.conseil-etat.fr.

55 Conseil Constitutionnel, 2011-625, 10 mars 2011, par. 8, disponible sous: www.conseil-constitutionnel.fr (30.04.2015).

> «Nous avons su, dans notre histoire, suspendre à un moment donné les libertés démocratiques. Celles-ci, en effet, ne peuvent pas avoir le même contenu en temps de paix et en temps de guerre. Or la guerre nous a été déclarée»[56].

De plus, les défenseurs du dispositif mis en place considèrent que la restriction à la liberté d'expression est sujette d'une part au contrôle de la personnalité qualifiée au sein d'une autorité administrative indépendante (CNIL) et d'autre part au contrôle juridictionnel *a posteriori*, ce que le Conseil Constitutionnel a jugé constituer une garantie suffisante, à tout le moins en ce qui concerne le blocage administratif de sites «qui diffusent des images de pornographie infantile»[57].

Nonobstant ce qui précède, deux institutions ont rendu un avis négatif au projet de loi ayant abouti à la loi du 13 novembre 2014. Le Conseil national du numérique souligne notamment le caractère disproportionné de la mesure qui, à son avis, n'est pas justifiée par des conditions comme l'urgence imminente ou l'absence de toute autre solution disponible. De plus, il souligne que:

> «[c]ontrairement aux dispositions relatives à la pédopornographie (…) la qualification des notions de commission d'actes terroristes ou de leur apologie prête à des interprétations subjectives et emporte un risque réel de dérive vers le simple délit d'opinion»[58].

De son côté, la Commission nationale consultative des droits de l'homme estime, dans son avis, que

> «l'intervention d'un juge [est] nécessaire pour ordonner et contrôler le blocage d'un site internet, dès lors que cette mesure constitue une ingérence grave dans la liberté d'expression et de communication. En effet, toute restriction préalable à l'expression sur internet entraîne une présomption lourde d'incompatibilité avec l'article 10 de la CESDH»[59].

A ce titre, il a recommandé au Gouvernement de confier le pouvoir de bloquer l'accès à internet à un juge des libertés, statuant dans un délai très bref, sur saisine du parquet compétent, notamment à la suite d'un signalement par le biais de PHAROS – recommandation qui n'a pas été suivie.

L'intervention du juge pour ce type de restriction est en outre commandée, selon la Commission, par le fait que la mesure relève de la police judiciaire et non administrative. Elle souligne en effet que:

> «[l]e blocage administratif de l'accès aux sites internet incitant à commettre des actes terroristes ou en faisant l'apologie est (…) de nature à brouiller la distinction classique entre police administrative et police judiciaire. Le nouveau texte habilite l'autorité administrative à décider du blocage, alors même qu'une ou plusieurs infractions ont déjà été commises. Il ne peut donc être considéré qu'il s'agit d'une mesure de police purement administrative

---

56 A. Tourret, Assemblée Nationale, Déb., 15 septembre 2014, disponible sous: www.assemblée-nationale.fr (30.04.2015).

57 Conseil Constitutionnel, 2011-625, 10 mars 2011, par. 8, disponible sous: www.conseil-constitutionnel.fr (30.04.2015). Voir, pour un positionnement en faveur du dispositif de la loi du 13 novembre 2014: Y. Mayaud, Terrorisme, Répertoire de droit pénal et procédure pénale, Dalloz, 2015, n°481; P. Ségur, La terrorisme et les libertés sur l'internet, AJDA 2015, p. 160.

58 Conseil National du Numérique, Avis n°2014-3 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, 15 juillet 2014, p. 5., disponible sous: www.cnnumerique.fr (30.04.2014).

59 Commission nationale consultative des droits de l'homme, Avis sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, 25 septembre 2014, JORF n°0231 du 5 octobre 2014, par. 19-20, disponible sous: www.legifrance.gouv.fr (30.04.2015); voir en ce sens aussi: C. Kleitz, Internet, sécurité et liberté d'expression: bis repetita placent, Gaz. Palais, 25 septembre 2014, n°268, p. 3; F. Tréguer, La LCEN, le juge et l'urgence d'une réforme, 27.04.2013, disponible sous: www.wethenet.eu (30.04.2015); G. Champeau, 10 problèmes posés par la censure d'Islamic-News.info, 16 mars 2015, disponible sous: www.numerama.com (30.04.2015).

> destinée à prévenir la provocation à des actes de terrorisme ou l'apologie de ceux-ci. Les nouvelles dispositions relèvent indéniablement du domaine de la police judiciaire dont la direction et le contrôle sont dévolus à l'autorité judiciaire, seule compétente pour la poursuite et la répression des infractions. Il est donc porté atteinte au principe de la séparation des pouvoirs».[60]

Enfin, il convient ici de relever que, dans une décision plus ancienne, le Conseil Constitutionnel avait censuré une disposition légale autorisant une autorité administrative indépendante à suspendre l'abonnement à internet d'un abonné en raison de l'utilisation illicite qui avait été faite de cet accès, au motif qu'une telle restriction à la liberté d'expression nécessite l'intervention d'un juge[61]. Ce dispositif était proposé dans le cadre de la protection des droits d'auteurs et des droits voisins, pour sanctionner le comportement d'utilisateurs d'internet violant cette protection. Le changement de position du Conseil Constitutionnel dans le cadre de sa décision relative aux sites pédopornographique de 2011 s'explique essentiellement par la gravité des violations sanctionnées ou l'importance des droits protégés: Plus les intérêts et valeurs à protéger par la mesure restrictive sont importants, plus la restriction à la liberté d'expression semble admissible. Cela apparaît d'autant plus pertinent à présent que la France a déclaré, depuis quelques temps, être **en guerre contre le terrorisme** et qu'elle a déclaré l'**état d'urgence**[62] après les attaques terroristes du 13 novembre 2015.

En conclusion, en l'attente de la décision du Conseil d'Etat sur les recours contre le décret du 5 février 2015 et du décret du 4 mars 2015, **la compatibilité du dispositif de blocage administratif des sites internet incitant à commettre des actes terroristes ou en faisant l'apologie avec la jurisprudence naissante de la Cour européenne des droits de l'homme en la matière n'est pas acquise**. L'interprétation des notions de provocation à d'actes terroristes ou d'apologie au terrorisme est réalisée sur la base de règles de droit et sous le double contrôle de la personnalité qualifiée au sein de la CNIL d'abord et du juge ensuite dans le cadre d'un recours judiciaire contre la décision administrative de blocage ou retrait. De telles possibilités de contrôle semblent assurer des protections suffisantes du point de vue de la liberté d'expression. Cependant, si la possibilité de restreindre la liberté d'expression sans intervention préalable d'un juge semble acquise pour le Conseil Constitutionnel dans le cadre de sites internet qui «diffusent des images de pornographie infantile», il n'en reste pas moins que ce blocage sur ordre administratif repose sur un constat objectif, c'est-à-dire la présence d'images de pornographie impliquant des enfants. La qualification des notions de provocation à des actes terroristes et d'apologie du terrorisme peut toutefois s'avérer nettement plus délicate en ce qu'elle constitue un sujet beaucoup plus subjectif.

Enfin, en ce qui concerne la lutte contre les discours de haine sur Internet, il convient de mentionner l'Avis de la Commission nationale consultative des droits de l'homme qui a été adopté le 12 février 2015. Dans cet avis, la CNCDH fait plusieurs recommandations, parmi lesquelles l'amendement de la LCEN en vue d'identifier les intermédiaires de l'Internet qui jouent un «rôle actif» et d'imposer à ces intermédiaires une obligation de détecter de manière proactive le contenu considéré comme du discours de haine ainsi que l'obligation d'informer les autorités compétentes de l'existence de ce contenu. La CNCDH propose également la création d'une autorité administrative indépendante

---

60 Ibidem. Voir aussi : E. Dreyer, Le blocage de l'accès aux sites terroristes ou pédopornographiques, Semaines Juridique ; Ed. Générale, 6 avril 2015, n° 14, doctr. 423.

61 Conseil Constitutionnel, 2009-580 DC, 10 juin 2009, par. 16 et suivants, disponible sous: www.conseil-constitutionnel.fr (30.04.2015).

62 Décrets n° 2015-1475, 1476 et 1478 du 14 novembre 2015 portant application de la loi n° 55-385 du 3 avril 1955 modifiée instituant un état d'urgence, J.O. 14-15.11.2015.

spécifique chargée notamment d'accompagner les hébergeurs et des fournisseurs d'accès à Internet dans leur tâche d'identification des discours de haine sur internet.[63]

Stéphanie De Dycker, LL.M.
Conseillère juridique, Institut suisse de droit comparé
30.04.2015 – révisé le 15.11.2015

Révisé le 3/5/2016 en tenant compte des commentaires de la France sur ce rapport.

63 Commission nationale consultative des droits de l'homme, Avis sur la lutte contre les discours de haine sur internet, 12 février 2015, disponible sous : http://www.cncdh.fr/fr/publications/avis-sur-la-lutte-contre-les-discours-de-haine-sur-internet (15.11.2015).