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 425-444

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.

LUXEMBOURG

Dans la version anglaise, cette partie apparaît dans les pages 425 à 444

1. Cadre légal

Le Luxembourg ne s'est pas doté d'une législation spécifique en matière de filtrage, de blocage et de retrait de contenus illicites d'Internet. L'application des textes de droit commun, tant en matière civile que pénale[1], permet toutefois d'appréhender ces problématiques.

Dans un premier temps, il importe de souligner que le Luxembourg a mis en place un cadre légal qui permet d'apprécier la légalité des contenus publiés sur Internet.

Du côté des infractions informatiques, le Code pénal a été modifié dès 1993[2] pour sanctionner les atteintes aux systèmes informatiques. Tout en signant la Convention de Budapest en 2003, le Luxembourg n'a ratifié cette Convention que par une loi du 18 juillet 2014[3]. Par la même occasion, le protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination de certains actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 18 janvier 2003, a été ratifié[4]. La loi de 2014 a permis de parfaire la législation nationale en la matière[5]. En ce qui concerne la diffusion de contenus illicites, la propagation de logiciels malveillants de toutes sortes (notamment de virus, de sites de *phishing* ou de malware) est réprimée (article 509-4 du Code pénal).

Les contenus pédopornographiques (voir notamment les articles 383 et 384), violents ou de nature à porter gravement atteinte à la dignité humaine (article 383), incitant à la haine (articles 454 et suivants) ou au terrorisme[6] sont également réprimés par le Code pénal. Dans ce domaine, le Luxembourg a notamment ratifié la Convention du Conseil de l'Europe sur la prévention du terrorisme du 15 mai 2005[7], ainsi que la Convention du Conseil de l'Europe pour la protection des

---

1 Tous les textes législatifs mentionnés dans le présent avis peuvent être retrouvés sur le site Internet : www.legilux.lu; des versions coordonnées sont disponibles sous la rubrique Espace législatif \ Recherche textes coordonnés.

2 Loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique.

3 Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation 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, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

4 Les dispositions contenues dans le Protocole ayant déjà été couvertes par les dispositions législatives en vigueur, aucune modification législative n'a été nécessaire.

5 M. BRAUN, La ratification de la Convention de Budapest sur la cybercriminalité par le Luxembourg, Journal des Tribunaux Luxembourg (JTL), éd. Larcier, n° 35, p. 121 et ss.

6 Pour autant que l'infraction soit commise dans les conditions fixées par les articles 135-1 et suivants du Code pénal (législation sur le terrorisme).

7 Loi du 26 décembre 2012 portant approbation de la Convention du Conseil de l'Europe sur la prévention du terrorisme, signée à Varsovie, le 16 mai 2005, et modifiant - le Code pénal; - le Code d'instruction criminelle; - la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne; - la loi modifiée du 11 avril 1985 portant approbation de la Convention sur la protection physique des matières nucléaires, ouverte à la signature à Vienne et à New York en date du

enfants contre l'exploitation et les abus sexuels ouverte à la signature à Lanzarote les 25-26 octobre 2007[8].

La protection des droits intellectuels, ainsi que des données personnelles est encadrée par la loi[9].

En tant qu'Etat membre de l'Union Européenne, le Luxembourg applique les règlements, directives et décisions cadres communautaires, parmi lesquels la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (ci-après : la Directive sur le commerce électronique), les directives 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, et 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle, ou encore les différentes directives en matière de protection des données[10].

Du côté procédural, nous renvoyons :

- au Code d'instruction criminelle (ci-après : le CIC),
- au Nouveau Code de Procédure Civile (ci-après : le NCPC),
- à la Loi du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données (ci-après : la Loi sur les droits d'auteur) et plus précisément aux articles 76 et suivants encadrant les actions en cessation contre les atteintes aux droits d'auteur,
- à la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après : la Loi sur la protection des données).

Les relations civiles étant fondées sur la liberté contractuelle (article 1134 du Code civil)[11], les parties à une convention peuvent définir les contenus qu'elles estiment légitimes dans le cadre de l'exécution de leurs obligations. Cette liberté ne saurait toutefois être exercée en méconnaissance des droits fondamentaux, parmi lesquels figurent les libertés d'expression et d'entreprendre.

2. Réglementation applicable

Les blocages, filtrages et retraits n'étant pas définis par des dispositions spécifiques, nous tentons d'insérer ces notions dans le cadre du **droit commun luxembourgeois**.

---

3 mars 1980; et - la loi modifiée du 14 avril 1992 instituant un code disciplinaire et pénal pour la marine.

8 Loi du 16 juillet 2011 portant: 1. approbation a) de la Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels ouverte à la signature à Lanzarote les 25-26 octobre 2007 b) du Protocole facultatif à la Convention des Nations Unies relative aux droits de l'enfant concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants 2. modification de certains articles du Code pénal et du Code d'instruction criminelle.

9 Le Luxembourg a également approuvé la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg, le 28 janvier 1981, par une Loi du 19 novembre 1987.

10 Pour un relevé des directives transposées en droit luxembourgeois, voir le site Internet de la CNPD : www.cnpd.lu \ Législation \ Droit européen.

11 *« Les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites. Elles ne peuvent être révoquées que de leur consentement mutuel, ou pour les causes que la loi autorise. Elles doivent être exécutées de bonne foi »*.

A titre préliminaire, nous relevons qu'il n'existe **aucune entité centrale** ayant pour mission d'établir des « listes noires » regroupant les sites devant être bloqués. Une entité définissant des filtres à mettre en œuvre par les fournisseurs d'accès à Internet et les hébergeurs fait également défaut.

Le contrôle des contenus se fait au cas par cas. Nous faisons la distinction entre les décisions qui ordonnent l'inaccessibilité provisoire de contenus et celles qui en ordonnent la suppression définitive, après avoir analysé le fond de l'affaire. Nous qualifions les mesures prises par les premières de « blocages » et celles ordonnées par les secondes de « retraits ». La terminologie de « filtrage » ne reflète pas les procédures nationales actuelles, de sorte que nous nous limiterons à reprendre celle-ci dans le cadre de nos développements sur les droits d'auteur (voir le point 2.2.2.1 ci-dessous) et la procédure de référé (voir le point 2.1.3 ci-dessous).

L'application de mesures de blocage et de retrait se trouve encadrée par la distinction faite entre les **éditeurs** de contenus proprement dits et les **prestataires[12] intermédiaires**. Ces derniers comprennent notamment les prestataires de simple transport et d'hébergement[13]. En transposant la Directive sur le commerce électronique en droit luxembourgeois[14], le législateur a en effet repris les **régimes de responsabilité spécifiques aux prestataires intermédiaires** définis par cette directive.

Le prestataire de simple transport est celui qui transmet sur un réseau de communication, des informations fournies par un destinataire du service ou qui fournit un accès au réseau de communications. Il s'agit plus particulièrement des fournisseurs d'accès à Internet. La responsabilité de ce prestataire ne saurait être engagée pour les informations transmises, à condition qu'il ne soit pas à l'origine de la transmission, ne sélectionne pas le destinataire de la transaction ou ne modifie les informations transmises (article 60 de la Loi sur le commerce électronique).

L'hébergeur est défini comme *« le prestataire qui fournit un service de la société de l'information consistant dans le stockage des informations fournies par un destinataire du service »* (article 62).

La loi instaure un régime de limitation de responsabilité de l'hébergeur à condition que :

a) il n'ait pas effectivement connaissance que l'activité ou l'information est illicite et, en ce qui concerne une action en dommages et intérêts, qu'il n'ait pas connaissance de faits ou de circonstances selon lesquels le caractère illicite de l'activité ou de l'information est apparent; ou
b) le prestataire, dès le moment où il en a une telle connaissance, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

Ce régime ne s'applique toutefois pas *« lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire »*.

L'éditeur est en premier lieu *« toute personne physique ou morale qui, à titre d'activité principale ou régulière, conçoit et structure une publication, en assume la direction éditoriale, décide de la mettre à la disposition du public en général ou de catégories de publics par la voie d'un média et ordonne à cette fin sa reproduction ou multiplication »* (article 3, point 3 de la Loi du 8 juin 2004 sur la liberté

---

12 Définis comme : *« toute personne physique ou morale qui fournit un service de la société de l'information »* par l'article 1er de la Directive sur le commerce électronique.

13 L'article 61 de la Loi sur le commerce électronique prévoit une troisième catégorie de prestataires intermédiaires – les prestataires de stockage dite *caching* – que nous n'aborderons pas dans le cadre du présent avis. A notre connaissance, le concours de ce type de prestataire n'a jamais été analysé dans la jurisprudence luxembourgeoise.

14 Par la Loi sur le commerce électronique.

d'expression dans les médias). Pour pouvoir distinguer l'éditeur de l'hébergeur – qui assure un rôle essentiellement technique – il faut étendre la définition donnée par la Loi sur la liberté d'expression dans les médias à toute personne qui édite des informations sur la toile, donc également à celle qui publie des contenus à titre privé et de façon sporadique[15].

On peut donc retenir que l'éditeur désigne la personne qui choisit de diffuser un contenu auprès du public[16]. Sous réserve des impératifs tenant aux libertés d'expression et de la presse, les éditeurs sont responsables des contenus publiés.

La distinction entre éditeur et hébergeur est cruciale pour déterminer la responsabilité de la personne concernée. Alors que la Cour de Justice de l'Union Européenne (ci-après : la CJUE)[17] a précisé ces notions dans plusieurs arrêts[18], nous mentionnons également un arrêt de la Cour Européenne des Droits de l'Homme (ci-après : la Cour EDH) du 16 juin 2015, *Delfi AS c. Estonie*, qui a statué sur les responsabilités d'un portail d'actualités sur Internet en raison des commentaires laissés par les internautes sur ce portail[19].

L'analyse de la jurisprudence des cours et tribunaux luxembourgeois montre que les régimes de responsabilité mis en place par la Directive sur le commerce électronique ont une influence pratique sur les procédures engagées par les plaideurs. D'une façon générale on peut retenir que :

- l'intervention de l'hébergeur est sollicitée pour rendre des contenus jugés illicites inaccessibles : les procédures choisies sont celles qui permettent d'obtenir rapidement une décision judiciaire,
- les responsabilités civiles et pénales de l'éditeur sont recherchées dans le cadre d'affaires au fond – ces affaires sont, le cas échéant, précédées de saisies pénales ou de procédures de référé.

Dans la mesure où nous n'avons pas pu trouver de jurisprudence ordonnant des mesures à l'égard de fournisseurs d'accès à Internet, nous nous limiterons à analyser la situation des hébergeurs dans la suite du présent avis.

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

L'obligation des hébergeurs de retirer promptement des contenus illicites de leurs systèmes, pour échapper à toute responsabilité, conduit ceux-ci à être confrontés à des demandes de blocage formulées par des personnes intéressées. Dans certaines conditions, les hébergeurs interviennent directement sur des contenus stockés sur leur infrastructure (2.1.1).

---

15 La distinction entre « éditeurs », qui tombent sous le champ d'application de la Loi sur la liberté d'expression dans les médias et les autres, a notamment son importance pour apprécier si le délai de prescription abrégé de trois mois à partir de la première mise à disposition au public du contenu critiqué s'applique (voir notamment : Tribunal d'arrondissement de Luxembourg (TA Lux.) 22.05.2008, n° 1693/2008).

16 Pour une analyse détaillée de cette question, voir notamment E. MONTEIRO, Les responsabilités liées au web 2.0, Revue du droit des technologies de l'information (RDTI) – n° 32/2008, p. 363 et ss.

17 Pour une analyse de la Jurisprudence de la CJUE rendue en relation avec Internet, voir : N. JÄÄSKINEN, Internet et la Cour de justice, dans Liber Amicorum Vassilios Skouris, Bruylant 2015, p. 253 et ss.

18 Voir notamment : CJUE, arrêts du 23.03.2010, Google France et Google, n° C-236/08 à C-238/08 ; CJUE 12.07.2011, L'Oréal c/ Ebay , n° C-324/09 ; CJUE 16.02.2012, Sabam C/ Netlog , n° C-360/10 ; CJUE 11.09. 2014, Sotiris Papasavvas c/ O Fileleftheros Dimosia Etaireia Ltd, ea., n° C-291/13.

19 CEDH 16.06.2015, Delfi AS c. Estonie , n° 64569/09 ; pour une analyse de cet arrêt, voir : D. SPIELMANN, Internet : libertés et restrictions, disponible sous : http://www.echr.coe.int/ Documents/Speech_20150626_Observatoire.pdf (17.08.2015).

Des blocages peuvent également être ordonnés dans le cadre de procédures pénales (2.1.2) ou civiles (2.1.3).

2.1.1. Le blocage décidé par l'hébergeur

La limitation de responsabilité au profit des hébergeurs, édictée par l'article 62 de la Loi sur le commerce électronique, s'accompagne de l'obligation pour ces prestataires, dès qu'ils **ont connaissance de contenus illicites** stockés sur leur infrastructure, d'**agir promptement** pour les retirer ou de rendre l'accès à celles-ci impossible.

L'application de ce texte met les hébergeurs devant une difficulté de taille : quels contenus sont à qualifier d'illicites ? La question est d'autant plus compliquée qu'Internet est accessible dans tous les pays du monde et que les mêmes contenus peuvent être parfaitement licites dans un pays et prohibés dans un autre.

D'une façon générale, on peut retenir que **les hébergeurs bloquent les contenus qui sont manifestement illicites** dans les pays de l'Union Européenne. On peut notamment citer le matériel pédopornographique, des propos qui incitent manifestement à la haine (notamment raciale)[20] ou qui appellent à des actes terroristes.

Pour augmenter leur sécurité juridique, de nombreux hébergeurs définissent les contenus illicites dans leurs **conditions générales**. Cet encadrement juridique, dans les conventions de droit privé, leur permet notamment de bloquer des œuvres artistiques mises en ligne en violation des droits d'auteur d'autrui ou des programmes malveillants distribués par leurs systèmes informatiques.

Les hébergeurs peuvent prendre connaissance des contenus illicites par des **contrôles spontanés** ou par les **dénonciations** qui leur sont faites par toute personne intéressée. Nous mentionnons le service BEE SECURE Stopline[21] par lequel tout particulier peut dénoncer des contenus relatifs à la pornographie infantile, au racisme, au révisionnisme et d´autres discriminations, ainsi qu'au terrorisme. Dans le cadre de la gestion des signalements de contenus illégaux, BEE SECURE Stopline dispose d'un accord de collaboration avec la police judiciaire[22] en vue d'agir en tant que relais et expert pour la réception, l'analyse et la transmission des renseignements aux services adéquats de la police[23]. La décision finale sur la légalité ou illégalité d'un contenu signalé à BEE SECURE Stopline et la décision d'en informer l'hébergeur en cas d'hébergement au Luxembourg appartient aux autorités de poursuite, en l'occurrence à la Police Grand-Ducale et au parquet. En général, BEE SECURE Stopline ne va pas contacter directement l'hébergeur pour le retrait de contenus illicites sauf sur demande de la Police Grand-Ducale.

Initiés dans le cadre de la **coopération entre autorités de police et le secteur privé**, les blocages sont généralement exécutés sur base des conditions générales de l'hébergeur, qui se réserve expressément le droit de retirer des contenus illicites de ses systèmes. Lorsque le caractère illicite des contenus n'est pas manifeste, l'hébergeur attend une décision de Justice statuant sur cette question[24]. Le cas échéant, le procureur peut encore ordonner le blocage des contenus sur le fondement de l'article 33, point 5) et 66, point 3) du CIC (voir point 2.1.2 ci-dessous).

---

20 Pour un exemple pratique, voir : TA Lux. 12.11.2014, n° 3019/2014.

21 https://stopline.bee-secure.lu.

22 A savoir les sections Protection Jeunesse, Nouvelles Technologies et Anti-Terroriste.

23 https://stopline.bee-secure.lu/index.php?id=8.

24 Notamment dans le cadre d'une procédure de référé, question analysée au point 2.1.3 ci-dessous.

L'article 62 de la Loi sur le commerce électronique oblige l'hébergeur à retirer les informations ou à rendre l'accès à celles-ci impossible. Sur base de cet article, le prestataire pourrait dès lors décider d'effacer définitivement les données litigieuses. En pratique, il efface les données sur l'infrastructure accessible *via* Internet, mais garde une **copie de sauvegarde** de celles-ci. Il procède dès lors à un blocage des données.

Dans le cas de contenus à caractère pédopornographique hébergés dans d'autrespays, les procédures opérationnelles de BEE SECURE Stopline prévoient d'en informer la Police Grand-Ducale et de transmettre les liens à une hotline partenaire, membre du réseau INHOPE (International Association of Internet Hotlines). A noter dans ce contexte que INHOPE bannit le terme de « pédopornographie » et lui préfère les terminologies de "matériel d'abus sexuel contre mineurs" (ou de "contenus ayant trait à la violence sexuelle exercée contre des enfants"), resp. de "Child sexual abuse material" en anglais.

Le but du travail de BEE SECURE Stopline et des membres du réseau INHOPE est le retrait le plus rapidement possible des contenus d'abus sexuels sur mineur afin d'éviter la révictimisation des enfants et adolescents représentés sur les images et vidéos (Notice and Takedown).

2.1.2. Les mesures pénales

Le CIC ne contient pas de dispositions spécifiques sur le blocage, le filtrage ou le retrait de contenus illicites. Ces mesures peuvent toutefois être ordonnées sur le fondement des **règles de droit commun relatives à la saisie des biens** qui *« ont servi à commettre le crime ou qui étaient destinés à le commettre et ceux qui ont formé l'objet du crime »* (voir notamment l'article 31 du CIC).

Les saisies pénales sont possibles pour tous les crimes et délits. Les types d'infractions suivantes tombent notamment sous ces catégories : le terrorisme (articles 135-1 et suivants du Code pénal), la pédopornographie (voir notamment les articles 383 et 384 du Code pénal), le *grooming* (article 385-2 du Code pénal)[25], de même que l'incitation à la haine contre différents groupes de personnes (articles 454 et suivants du Code pénal) ou les menaces contre l'intégrité physique (articles 327 et suivants du Code pénal).

En matière de **protection de la vie privée**, l'article 1er de la Loi du 11 août 1982 concernant la protection de la vie privée pose comme principe que *« les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, 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 »*. Les atteintes à la vie privée prévues par la loi, dont notamment les enregistrements audio et vidéo non-autorisés (articles 2 à 4), les montages réalisés avec les paroles ou les images d'une personne sans le consentement de celle-ci (article 5) ou encore les harcèlements intempestifs (article 6), constituent par ailleurs des délits.

Les atteintes aux droits d'auteur sont sanctionnées pénalement de peines délictuelles par l'article 82 de la Loi sur les droits d'auteur.

---

[25] Pour des applications pratiques de ce texte, introduit en droit luxembourgeois par une loi du 16 juillet 2011, voir : TA Lux. 19.03.2015, n° 914/2015 ; TA Lux. 30.04.2015, n° 1311/2015 ; TA Lux. 28.05.2015, n° 1571/2015

Il en va de même pour certaines infractions en matière de protection des données[26]. En effet, rien que dans la Loi sur la protection des données, sur un total de 45 articles, pas moins de 19 prévoient des sanctions pénales en cas de violation de ces dispositions.
En appréhendant la saisie pénale dans sa conception classique, à savoir mettre un bien sous-main de Justice[27], on peut aboutir à un blocage de contenus illicites en saisissant le matériel informatique les hébergeant. En retirant ce matériel du centre de données et en le déconnectant d'Internet, tous les contenus et services se trouvant sur ce matériel deviennent inaccessibles.

Cette solution pragmatique se heurte essentiellement à deux problèmes :
- les données litigieuses peuvent être stockées sur un serveur qui abrite les données d'autres personnes que celle visée par l'enquête ou l'instruction judiciaire. Tel est notamment le cas des hébergements mutualisés, où un serveur accueille les sites Internet d'une multitude de clients. La saisie touche non seulement la personne visée par l'enquête ou l'instruction, mais encore l'hébergeur et toutes les autres personnes abritant légitimement leur site sur le serveur en question[28] ;
- la saisie du matériel informatique aboutit à un blocage total de tous les contenus y stockés. La mesure n'étant pas ciblée, des contenus parfaitement licites mis en ligne par la personne visée par l'enquête ou l'instruction sont également bloqués.

La **saisie physique du matériel informatique** peut notamment être une solution en matière d'échanges de contenus à caractère pédopornographique par des connexions *peer-to-peer* initiées par des particuliers[29].

Par une Loi du 18 juillet 2014[30], le législateur est intervenu pour encadrer plus spécifiquement la saisie de *« données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données »*[31]. Les articles 31, 33 (crimes et délits flagrants) et 66 (saisies ordonnées par un juge d'instruction) prévoient désormais expressément la **saisie de données**

---

26 Infractions prévues par la Loi sur la protection des données, ainsi que par la Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

27 G. CORNU, Vocabulaire juridique, Presses Universitaires de France (PUF), 4ème éd. 2003, v° saisie.

28 Sur ces aspects, voir également B. LOSDYCK, Les saisies et perquisitions de matériel informatique : les « garde-fous » entourant leur mise en œuvre, RDTI n° 52, 3/2013, p. 36.

29 Voir notamment TA Lux. 23.03.2011, n° 1059/2011 ; TA Lux. 07.10.2008, n° 2822/2008 ; TA Lux. 24.06.2008, n° 2126/2008 ; TA Lux. 06.11.2008, n° 3150/2008.

30 Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation 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, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

31 Depuis la Loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique, ayant introduit les infractions en matière informatique dans le Code pénal, le législateur se réfère aux termes « système de traitement ou de transmission automatisé de données » pour désigner les « systèmes informatiques » (terminologie employée par la Convention de Budapest) dans les différents textes répressifs.

informatiques « *soit par la saisie du support physique de ces données, soit par une copie de ces données* » (article 33, point 5 ; article 66, point 3)[32].

Dans une première phase, la preuve du contenu prétendument illicite est recueillie par la saisie des données.

Les articles 33, point 5) et 66, point 3) du CIC autorisent par la suite **la suppression et donc le blocage de ces données** de leur support d'origine, à condition que :

- une copie des données ait été préalablement établie,
- le support physique des données n'ait pas été saisi[33],
- la mesure de suppression soit ordonnée par un **juge d'instruction**, respectivement par le **procureur d'Etat** (en cas de flagrant délit),
- la détention ou l'usage des données soit illégal ou dangereux pour la sécurité des personnes ou des biens,
- le support physique (p.ex. l'ordinateur ou le serveur) abritant les données se situe au Grand-Duché de Luxembourg.

A côté des impératifs en matière de preuve, la condition qu'une copie des données effacées ait été préalablement établie, permet de rétablir celles-ci en cas d'annulation de la décision d'effacement par la chambre du conseil[34] ou par les juridictions du fond, ainsi qu'en cas de non-lieu ou d'acquittement prononcé sur le fond de l'affaire[35]. Tel que l'explique le législateur *« la décision d'effacement ne peut pas être assimilée à une sanction de confiscation anticipée. Il s'agit soit d'une protection des personnes et des biens contre de nouvelles infractions (en cas de malware notamment), soit d'une mesure tendant à éviter la propagation de matériel illégal (telle que la pédopornographie). En cas d'acquittement ou de décision de ne pas procéder à des poursuites, les données saisies (leur copie) pourront être restituées. En cas de poursuites, en revanche, les données seront confisquées »*[36].

A la lecture des travaux parlementaires, on constate que l'idée du législateur était de rendre des données illicites ou dangereuses inaccessibles, en attendant une décision au fond. La mesure d'effacement produit les effets d'un blocage.

Les contenus pouvant être bloqués sont notamment « la pédopornographie, la malware ou encore l'incitation à la haine, voire le terrorisme ».

La mesure est entourée d'importantes garanties, en ce qu'elle doit être ordonnée par le procureur d'Etat en cas de flagrant crime ou délit et par un juge d'instruction dans toutes les autres hypothèses. Ces décisions peuvent faire l'objet de **recours en annulation et en restitution**[37].

---

32 Pour une saisie de données avant l'adoption de ce texte, voir notamment : Cour d'appel (CA) 09.07.2013, n° 375/13 ; 16.11.2012, n° 752/12 ; CA 21.12.2011, n° 931/11.

33 Ce qui engendre nécessairement un blocage total de toutes les données enregistrées sur le serveur et exclut ainsi toute suppression sélective des données.

34 Pour les questions de procédure, voir le point 3.2 ci-dessous.

35 Cette problématique a notamment été soulevée par le Conseil d'Etat dans son premier avis du 16.04.2013, Documents parlementaires (doc. parl.) 6514-2, p. 6, point 4.

36 Doc. parl. 6514-7, p. 12.

37 Nous renvoyons à nos développements exposés au point 3.2.1 ci-dessous.

2.1.3. Les mesures civiles / le référé

Les actions en référé sont prévues par le titre XV du NCPC. Le **juge des référés** peut notamment, dans les situations d'urgence, ordonner toutes les mesures qui ne se heurtent **à aucune contestation sérieuse**[38] ou que justifie l'existence d'un différend (le **référé urgence** – article 932). Il peut également prescrire les **mesures conservatoires** ou de remise en état qui s'imposent, soit pour **prévenir un dommage imminent**, soit pour **faire cesser un trouble manifestement illicite** (le référé voie de fait – article 933).

L'avantage du référé est la **célérité** avec laquelle les ordonnances sont rendues. Le juge peut même permettre d'assigner, *« à heure indiquée, même les jours fériés ou habituellement chômés, soit à l'audience, soit à son domicile portes ouvertes »* (article 934, alinéa 2).

L'ordonnance de référé n'a toutefois pas, au principal, l'autorité de la chose jugée (article 938, alinéa 1er). Les décisions prises par le juge des référés n'ont dès lors qu'un **caractère provisoire**, jusqu'à ce que l'affaire soit toisée au fond.

Afin de garantir l'exécution de la décision prise par le juge des référés, celle-ci peut être assortie d'une **astreinte**[39]. Celle-ci peut être définie comme *« une condamnation au paiement d'une somme d'argent prononcée à titre accessoire par le juge, pour exercer une pression sur le débiteur de manière que ce dernier exécute la condamnation mise à sa charge »*[40]. En principe, toute condamnation est susceptible d'être assortie d'une astreinte, à l'exclusion des condamnations au paiement d'une somme d'argent.

Un point fondamental du référé est l'**exécution provisoire** des ordonnances rendues (article 938, alinéa 3), qui peuvent être exécutées nonobstant appel, au risque toutefois de la personne qui les exécute[41].

La célérité avec laquelle les ordonnances de référé peuvent être rendues, rend cette procédure particulièrement adaptée aux contenus publiés en ligne. Elle permet non seulement d'obtenir rapidement un titre exécutoire contre l'éditeur de contenus illicites, mais également d'imposer le blocage de contenus à un **hébergeur**. Pour ce dernier, l'ordre donné par une autorité judiciaire lui donne la sécurité juridique nécessaire pour retirer le contenu litigieux de ses systèmes[42]. Bien que nous n'ayons pas pu trouver de décision sur ce point, nous estimons qu'une mesure de filtrage pourrait également être ordonnée à l'encontre d'un fournisseur d'accès à Internet dans le cadre d'une procédure de référé.

---

38 Dès qu'il y a une contestation sérieuse sur une question de fait ou de droit, le juge des référés n'est plus compétent pour connaître de l'affaire. Pour un exemple pratique d'une prétendue atteinte à la réputation et à l'honneur d'une personne, voir : TA Lux. 22.05.2012, n° 363/2012.

39 Pour une analyse détaillée de l'astreinte, voir M. THEWES, L'astreinte en droit luxembourgeois, Annales du Droit luxembourgeois 1999, n° 9, p. 119 et ss.

40 P. VAN OMMESLAGHE, Les obligations – examen de jurisprudence (1974 – 1982), Revue critique de jurisprudence belge 1986, p. 198, n° 94, cité dans M. THEWES, L'astreinte en droit luxembourgeois, op. cit., n° 9, p. 119.

41 Jurisprudence constante, voir notamment : CA 16.04.1915, Pasicrisie 10, p. 510.

42 Pour une analyse de cette question, voir A. PRUM, Le commerce électronique en droit luxembourgeois, éd. Larcier 2005, p. 562, n° 680.

Les procédures de référé peuvent notamment être intentées par des personnes s'estimant victimes d'atteintes à leur vie privée[43] ou à leur réputation. Nous pouvons également citer une affaire, dans laquelle un père divorcé avait mis en ligne des photos de sa fille mineure, sans l'autorisation de la mère. Au moment où le juge a été appelé à statuer, le père avait déjà retiré les photos des réseaux sociaux. Le juge des référés lui a néanmoins interdit, sous peine d'astreinte, la publication future de toute photo sur Internet représentant l'enfant mineur en question[44].

2.2. Retrait de contenu illégal d'internet

Dans la présente partie nous analysons les mesures de retrait prises par des juridictions qui statuent sur le fond du litige. Tout en revenant sur les procédures pénales (2.2.1) et civiles (2.2.2), nous abordons les procédures spécifiques pouvant être engagées en matière de protection des données (2.2.3).

2.2.1. Les retraits ordonnés par les juridictions pénales

La législation luxembourgeoise ne contient pas de disposition spécifique sur le retrait de contenus en ligne. Dans la continuation des développements exposés au point 2.1.2 ci-dessus, la situation peut se résumer comme suit : Le procureur d'Etat ou le juge d'instruction ordonne la saisie des données litigieuses sous forme d'une copie sur un support numérique, ainsi que leur suppression sur l'infrastructure informatique d'origine. Le contenu est donc bloqué. A l'issue de l'enquête préliminaire ou de l'instruction judiciaire, le fond de l'affaire est porté devant les juridictions répressives.

En cas de condamnation pour crime ou délit, ces juridictions prononcent la **confiscation du contenu illicite**. Ce bien incorporel forme en effet l'objet direct de l'infraction sanctionnée. La mesure de suppression du contenu est validée par la condamnation intervenue[45].

Nous signalons également un arrêt qui a ordonné la **fermeture judiciaire d'un site Internet**[46].

Dans les affaires de pédopornographie, les juridictions confisquent naturellement le matériel illicite[47]. Ils le retirent ainsi non seulement à la personne condamnée, mais l'enlèvent également des canaux de diffusion utilisés par celle-ci[48].

Une difficulté d'ordre pratique peut se poser lorsque la personne condamnée opère un site Internet à l'étranger. L'exécution pratique de la décision de justice peut s'avérer difficile. D'autant plus que la législation nationale ne prévoit actuellement pas d'astreinte pénale[49]. Une solution peut être une condamnation avec sursis probatoire (articles 629 et suivants du CIC), prévoyant l'obligation de retirer le contenu litigieux endéans un certain délai.

2.2.2. Les retraits ordonnés par les juridictions civiles

---

43 Voir notamment : CA 10.07.2013, n° 39634 du rôle.

44 TA Lux. 29.07.2014, n° 463/2014.

45 Doc. parl. 6514-7, p. 12.

46 CA 14.02.2012, n° 101/12 V.

47 Voir notamment : TA Lux. 05.03.2014, n° 715/2014 ; TA Lux. 07.11.2013, n° 2921/2013 ; TA Lux. 09.10.2013, n° 2574/2013.

48 Pour les échanges *peer-to-peer*, voir notamment TA Lux. 23.03.2011, n° 1059/2011 ; TA Lux. 07.10.2008, n° 2822/2008 ; TA Lux. 24.06.2008, n° 2126/2008 ; TA Lux. 06.11.2008, n° 3150/2008.

49 Le juge pénal peut toutefois assortir le volet civil de sa décision d'une astreinte ; voir à ce sujet : CA 14.12.1970, Pasicrisie 21, p. 434.

Dans la présente partie, nous esquissons les procédures civiles classiques (2.2.2.2), pour aborder plus en détail l'action en cessation prévue en matière d'atteintes aux droits d'auteur (2.2.2.1).

2.2.2.1. L'action en cessation en matière d'atteintes aux droits d'auteur

Les articles 76 et suivants de la Loi sur les droits d'auteur prévoient une **action en cessation**[50] contre toute atteinte à un droit d'auteur, à un droit voisin ou à un droit *sui generis* sur des bases de données. Le législateur a pu définir cette action comme une *« action rapide au fond, introduite et jugée comme en référé, qui permet de demander la cessation de toute violation d'un droit d'auteur ou d'un droit voisin. Le tribunal civil demeure compétent pour prononcer l'indemnisation du ou des titulaires de droits dont les droits ont été violés »*[51]. Il importe de noter que cette action est une action au fond, mais dans laquelle le tribunal statue *« comme en matière de référé »*[52]. Par opposition aux procédures de référé prévues par les articles 932 et suivants du NCPC, l'exécution provisoire est facultative.

L'injonction prononcée peut être assortie d'une **astreinte**.

Tout intéressé (y compris les organismes de gestion collective) peut demander devant le Tribunal la cessation d'une atteinte aux droits d'auteur. Cette action peut être dirigée contre toute personne, la loi ne limitant pas le cercle des potentiels défendeurs aux seuls auteurs directs et principaux de l'atteinte.

Conformément à l'article 76 de la Loi sur les droits d'auteur, qui reprend sur ce point l'article 8, point 3 de la directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, la juridiction saisie peut également rendre une injonction de cessation à l'encontre des **intermédiaires** dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur.

L'action en cessation contre les intermédiaires n'est soumise à aucune formalité préalable et peut être intentée sans avoir été dirigée préalablement contre l'auteur de l'atteinte aux droits d'auteur[53].

Pour ce qui est de la notion d' « intermédiaire », les juges nationaux, tout en appliquant la jurisprudence de la CJUE[54], confient ce statut aux prestataires intermédiaires au sens de la Loi sur le commerce électronique, parmi lesquels les **fournisseurs d'accès à Internet** et les **hébergeurs**.

Dans deux affaires opposant un organisme de gestion collective des droits d'auteur à un hébergeur[55], le tribunal a ordonné la cessation des atteintes constatées sur des sites Internet stockés sur l'infrastructure informatique de l'hébergeur. Le tribunal n'a pas détaillé cette injonction, en constatant que la Loi sur les droits d'auteur ne permettait pas au juge d'ordonner des mesures techniques concrètes. Il incombe à la partie qui se voit ordonner de cesser des atteintes aux droits d'auteur de se conformer à la décision en prenant toutes les mesures appropriées.

---

50 Pour plus de précision sur cette action, voir J-L. PUTZ, Le droit d'auteur, éd. Promoculture-Larcier 2013, p. 281 et ss.

51 Doc. parl. n° 4431, Exposé des motifs, « Renforcement des sanctions de la contrefaçon ».

52 CA 25.04.2012, n° 38033 du rôle.

53 J-L. PUTZ, Le droit d'auteur, op. cit., p. 304, n° 701a.

54 Voir notamment les arrêts CJUE 24.11.2011, Scarlet Extended, n° C-70/10 et CJUE 16.02.2012, Netlog NV, n° C-360/10.

55 Voir notamment TA Lux. 11.05.2011, n° 349/2011 et TA Lux. 11.03.2014, n° 54/2014.

Afin de faire respecter sa décision, le tribunal a ordonné la cessation des atteintes constatées endéans les trois jours ouvrables à dater de la signification de la décision, sous peine d'une astreinte de 2.000 euros par violation constatée et par jour[56].

Nous n'avons pas pu trouver de décision ayant ordonné une mesure de filtrage ou de blocage à l'encontre d'un fournisseur d'accès à Internet. Au regard de la jurisprudence de la CJUE[57], nous estimons toutefois qu'une telle action pourrait être intentée sur base des articles 76 et suivants de la Loi sur les droits d'auteur.

56 Pour ce qui est de la notion d'astreinte, voir le point 2.1.3 ci-dessous.

57 CJUE 24.11.2011, Scarlet Extended, n° C-70/10.

2.2.2.2. Les procédures de droit commun

Le retrait de contenus illicites peut naturellement être demandé devant les **juridictions civiles statuant au fond**. Au regard de la célérité avec laquelle les informations sont diffusées sur Internet, cette procédure s'avère toutefois peu adaptée.

Elle se conçoit essentiellement en parallèle à une procédure de référé, pour asseoir la décision prise par cette juridiction. Une autre hypothèse est celle d'une victime qui réclame des dommages et intérêts devant la juridiction du fond et demande également le retrait des contenus litigieux.

Nous précisons que les décisions rendues au fond peuvent également être assorties d'une **astreinte** (article 2059 du Code civil).

2.2.3. La protection des données

La protection des données **à caractère personnel** est réglementée par la Loi sur la protection des données, ainsi que par la Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

Les textes instaurent un cadre normatif et procédural strict encadrant tout traitement de données à caractère personnel. Le non-respect des obligations imposées aux responsables du traitement de données ainsi que les manquements sont assortis de sanctions pénales et administratives[58].
Après avoir analysé l'action en cessation – comparable à celle prévue en matière de protection des droits d'auteur – nous abordons les sanctions administratives pouvant être prononcées par l'établissement public Commission nationale pour la protection des données (ci-après : la CNPD)[59].

2.2.3.1. L'action en cessation

L'action en cessation consiste à saisir le juge afin de voir ordonner la cessation d'actes contraires à la Loi sur la protection des données[60]. Une particularité de la procédure instaurée par l'article 39 de la loi est qu'elle est réservée

- au **Procureur d'Etat** qui a déclenché une action publique pour violation de la Loi sur la protection des données,
- à la **CNPD**, dans l'hypothèse où une sanction disciplinaire prononcée en application de l'article 33 de la loi n'a pas été respectée,
- à une **personne lésée**, mais uniquement si celle-ci a préalablement saisi la CNPD d'une demande relative au respect de ses droits et libertés fondamentaux par le responsable du traitement ou d'une demande de vérification de la licéité du traitement suite à un refus ou une limitation de l'exercice de son droit d'accès.

Le champ d'application de cette action se trouve limité, en ce qu'elle concerne seulement le « **responsable de traitement** », défini comme *« la personne physique ou morale, l'autorité publique,*

---

58 Voir le tableau reprenant les différentes infractions en la matière, dans C. PIERRE-BEAUSSE, La protection des données personnelles, éd. Promoculture 2005, p. 287.

59 Pour plus d'informations, voir le site Internet de la CNPD : www.cnpd.lu.

60 Pour plus d'informations sur cette procédure, voir C. PIERRE-BEAUSSE, La protection des données personnelles, op.cit., p. 282 et ss.

le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales » (article 2 de la loi) et son sous-traitant (défini comme *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement »* - article 2)

L'action en cessation prévue par la Loi sur la protection des données peut dès lors uniquement être dirigée contre les personnes qui sont à qualifier de « responsable de traitement » ou de « **sous-traitant** » et qui ont effectué des traitements de données jugés illicites. En principe, cette qualification ne s'applique pas à l'hébergeur ou au fournisseur d'accès à Internet. L'hébergeur – au sens classique du terme – se limite en effet à stocker les données de son client. S'il traite ces données pour des finalités qui lui sont propres,, il peut tomber sous la qualification de « responsable de traitement ». Dans son arrêt Google Spain, la CJUE retient ainsi que *« l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de «traitement de données à caractère personnel», au sens de cet article 2, sous b), lorsque ces informations contiennent des données à caractère personnel et, d'autre part, l'exploitant de ce moteur de recherche doit être considéré comme le «responsable» dudit traitement, au sens dudit article 2, sous d) »*[61].

2.2.3.2. La procédure administrative devant la CNPD

La Loi sur la protection des données accorde un pouvoir disciplinaire à la CNPD, lui permettant notamment de *« **verrouiller, effacer ou détruire** »* des données faisant l'objet d'un traitement contraire aux dispositions de ladite loi ou de ses règlements d'exécution (article 33)[62].

Une telle mesure peut notamment être prise à l'encontre d'un responsable de traitement qui procède à des traitements de données personnelles illicites.

Nous n'avons pas pu trouver de jurisprudence ayant appliqué ce texte.

En cas de violation des dispositions relatives aux mesures de sécurité, la CNPD peux prescrire un avertissement ou une admonestation (articles 21 à 24), ainsi que l'interdiction temporaire ou définitive d'un traitement de données. Cette décision d'interdiction de traitement peut être publiée. La CNPD a aussi la possibilité de prononcer des amendes d'ordre ne pouvant excéder 50.000 EUR en vertu de l'article 3 de la loi du 28 juillet 2011 relative à la protection des données dans le secteur des communications électroniques.

3. Questions de procédure

Les blocages, filtrages et retraits de contenus illicites n'étant pas encadrés par des règles spécifiques, les procédures de droit commun s'appliquent. Un exposé détaillé de celles-ci dépasserait le cadre du présent avis, de sorte que nous nous limitons à esquisser les aspects essentiels de ces procédures.

---

[61] CJUE 13.05.2014, Google Spain c/ Agencia Española de Protección de Datos (AEPD), n° C-131/12.

[62] Voir également : C. PIERRE-BEAUSSE, La protection des données personnelles, op. cit., p. 289 et ss.

3.1. Les recours contre les décisions de blocage ou de retrait prises par l'hébergeur

Nous rappelons que l'hébergeur est tenu de retirer promptement les contenus illicites, dont il a connaissance, de ses systèmes. A côté des injonctions judiciaires qui lui sont faites, l'hébergeur peut aussi retirer des contenus de sa propre initiative. La prise de connaissance peut avoir été acquise soit en raison de contrôles diligentés périodiquement ou de la dénonciation qui lui a été faite par toute personne intéressée.

L'éditeur des contenus bloqués peut naturellement contester la décision de l'hébergeur.

Il peut notamment agir en référé pour demander la remise en ligne des contenus litigieux[63].

3.2. Les procédures pénales

Nous faisons la différence entre les procédures pendant la phase de l'enquête ou de l'instruction judiciaire – où les blocages n'ont pas encore de caractère définitif – et les procédures au fond, dans le cadre desquelles un retrait définitif peut être ordonné.

3.2.1. Les procédures au cours de l'enquête ou de l'instruction judiciaire

Tel qu'exposé au point 2.1.2 ci-dessus, des mesures de blocage peuvent être prises à l'encontre de l'hébergeur, tiers par rapport à l'éditeur du contenu litigieux, ou contre l'éditeur responsable du contenu.

Hormis le cas du flagrant crime ou délit[64], où un **officier de police judiciaire** peut procéder à des saisies, toute saisie opérée sans le consentement de la personne visée nécessite une ordonnance émise par un juge d'instruction. Celle-ci peut être émise dans le cadre d'une **instruction judiciaire** ou à l'issue d'une **mini-instruction** sur base de l'article 24-1 du CIC. Cette dernière procédure permet au procureur d'Etat de requérir du juge d'instruction d'ordonner une perquisition, une saisie, l'audition d'un témoin ou une expertise sans qu'une instruction judiciaire ne soit ouverte.

En pratique, les décisions du procureur d'Etat et du juge d'instruction sont notifiées et exécutées par des officiers de police judiciaire.

Le prévenu (lors de l'enquête), l'inculpé (lors de l'instruction), ainsi que « tout tiers intéressé » peuvent contester la légalité de la décision prise à leur encontre et en demander l'annulation. Le CIC distingue entre le **recours en annulation** contre les actes posés lors de l'enquête (articles 48-2 du CIC) et ceux accomplis au cours de l'instruction judiciaire (article 126 du CIC). Nous mentionnons également le recours contre les ordonnances du juge d'instruction, prises en application de l'article 24-1 du CIC (procédure prévue audit article).

Les recours sont présentés – par voie de simple requête – devant la **chambre du conseil** du tribunal d'arrondissement territorialement compétent.

---

63 Nous renvoyons notamment à nos développements exposés au point 2.1.3 ci-dessus.

64 Est qualifié crime ou délit flagrant, le crime ou le délit qui se commet actuellement ou qui vient de se commettre (article 30, alinéa 1er du Code pénal). D'une façon générale, la situation de flagrance est donnée dans les 24 heures suivant la commission de l'infraction.

La notion de « **tout tiers intéressé** » étant très large, l'**hébergeur** qui a agi comme intermédiaire, peut également exercer ces recours.
Les recours en annulation doivent toutefois être exercés endéans des **délais de forclusion très stricts** :

- pour les actes accomplis au cours de l'enquête, « toute personne concernée » dispose d'un délai de deux mois suivant l'exécution de l'acte, pour demander l'annulation de celui-ci, qu'une instruction préparatoire ait ou non été ouverte à la suite de l'acte contesté,
- pour les actes accomplis au cours de l'enquête
  - l'inculpé dispose de cinq jours à partir de son inculpation, si une instruction préparatoire a été ouverte sur la base de l'enquête,
  - si aucune instruction préparatoire n'a été ouverte sur la base de l'enquête, le prévenu peut présenter sa demande en annulation devant la juridiction du fond, avant toute demande, défense ou exception autre que les exceptions d'incompétence.

Les mêmes règles s'appliquent pour les actes pris sur base de l'article 24-1 du CIC.

Pour les actes ordonnés par un juge d'instruction dans le cadre d'une instruction judiciaire, la demande doit être produite, à peine de forclusion, au cours même de l'instruction, dans un délai de cinq jours à partir de la connaissance de l'acte (article 126 du CIC).

Les ordonnances rendues par la chambre du conseil peuvent faire l'objet d'un **appel** devant la chambre du conseil de la Cour d'appel (article 133 du CIC).

Nous mentionnons finalement les **demandes en restitution**, qui se conçoivent essentiellement en cas de saisie du matériel informatique hébergeant le contenu litigieux (article 68 du CIC).

3.2.2. Les procédures au fond

Dans une première hypothèse, le contenu litigieux a déjà été bloqué au cours de l'enquête ou de l'instruction (voir le point 2.1.2 ci-dessus). Si ce blocage s'est fait au moyen de la saisie du matériel informatique, celui-ci est confisqué en cas de condamnation et restitué en cas d'acquittement.

En se basant sur les travaux parlementaires sur les articles 33, point 5) et 66, point 3)[65], on peut retenir que la **suppression du contenu est validée en cas de condamnation**. La copie du contenu effacé du matériel informatique originaire est **confisquée**. En cas d'acquittement, cette copie est **restituée** au prévenu.

Toutes les décisions pénales rendues en matière criminelle et délictuelle sont **appelables** (articles 199 et 221 du CIC). Elles peuvent également faire d'objet d'un **pourvoi en cassation** (article 407 du CIC)[66].

3.3. Les procédures civiles

Dans tous les cas de figure analysés au point 2 ci-dessus, nous sommes partis du postulat que le demandeur dirigeait son action contre l'éditeur du contenu critiqué et/ou contre l'hébergeur. Pour pouvoir valablement engager l'instance, le demandeur doit faire signifier son **acte d'assignation par**

---

65 Doc. parl. 6514-7, p. 12.

66 Voir également la Loi du 18 février 1885 sur les pourvois et la procédure en cassation.

voie d'huissier. En fonction de la procédure choisie, l'acte doit indiquer soit une date fixe de comparution, soit un délai endéans lequel le défendeur doit avoir constitué avocat[67].

En cas de comparution du défendeur, la **procédure se déroule contradictoirement**.

A supposer que la mesure de blocage ou de retrait soit prononcée par la juridiction saisie, il appartient au demandeur de faire **signifier la décision au défendeur**. Ce n'est qu'à partir de la signification de la décision que le défendeur est obligé de s'exécuter et qu'une **exécution forcée** de la décision devient possible.

Nous rappelons que les ordonnances de **référé** (voir le point 2.1.3 ci-dessus) sont **exécutoires par provision**, nonobstant appel ou opposition. Pour toutes les décisions rendues au fond, qui ne prévoient pas expressément leur exécution provisoire, le demandeur doit attendre l'écoulement du délai d'appel pour que la décision acquière force de chose jugée.

Toutes les décisions civiles ayant statué sur une demande de blocage ou de retrait sont **appelables** (voir notamment les articles 571 et 939 du NCPC) et peuvent faire l'objet d'un **pourvoi en cassation** (article 1er de la Loi du 18 février 1885 sur les pourvois et la procédure en cassation).

3.4. Les procédures en matière de protection des données

L'action en cessation prévue par l'article 38 de la Loi sur la protection des données obéit aux règles de procédure énoncées au point 3.3 ci-dessous.

Les sanctions disciplinaires prononcées par la CNPD sur base de l'article 33 de la Loi sur la protection des données peuvent être mises en cause par un **recours en réformation** devant les juridictions administratives[68]. Dans le cadre d'un recours en réformation *« le juge non seulement déclarera l'acte illégal, mais en plus se mettra en lieu et place de l'administration pour redresser les défauts initiaux de l'acte. Il agira donc comme juge tout en se substituant au pouvoir de l'entité administrative dont la décision a été soumise à son contrôle »*[69].

Les décisions rendues par le Tribunal administratif sont appelables devant la **Cour administrative** (article 8, 2 de la loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif).

4. Surveillance générale d'Internet

L'article 63 (1) de la Loi sur le commerce électronique[70] dispose que :

> *« pour la fourniture des services visés aux articles 60 à 62, les prestataires ne sont pas tenus d'une obligation générale de surveiller les informations qu'ils transmettent ou*

---

67 Pour une analyse très détaillée des procédures civiles en droit luxembourgeois : T. HOSCHEIT, Le droit judiciaire privé au Grand-Duché de Luxembourg, éd. Paul Bauler 2012.

68 Recours défini par l'article 3 de la loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif.

69 M. FEYEREISEN, J. GUILLOT, S. SALVADOR, Procédure administrative contentieuse, éd. Promoculture 2006, p. 78, n° 86.

70 Reprenant sur ce point l'article 15, paragraphe 1er, de la Directive sur le commerce électronique.

stockent, ni d'une obligation générale de rechercher des faits ou circonstances indiquant des activités illicites ».

Sur base de ce texte, **aucune obligation de surveillance générale**[71] à charge des fournisseurs d'accès à Internet et des hébergeurs ne saurait être instaurée[72]. Ce texte ne porte toutefois pas préjudice à leur devoir de coopération avec les autorités de poursuite. Tel que décrit au point 2.1.1 ci-dessus, les autorités de police peuvent notamment dénoncer des contenus qu'elles jugent illicites aux hébergeurs. A ce sujet, nous relevons que la section nouvelles technologies, ainsi que les officiers chargés de la lutte contre le terrorisme de la police judiciaire analysent et enquêtent sur les contenus illicites qu'ils constant eux-mêmes ou qui leur sont rapportés.

La CJUE a été appelée à préciser le champ d'application de l'article 63 (1) de la Loi sur le commerce électronique, notamment par rapport à des demandes de blocage formulées par les ayants droit d'œuvres protégées par les droits d'auteur.

Dans une première décision, L'Oréal c/ Ebay, les Juges européens ont retenu qu'

il résulte de l'article 15, paragraphe 1, de la directive 2000/31, lu en combinaison avec l'article 2, paragraphe 3, de la directive 2004/48, que les mesures exigées de la part du prestataire du service en ligne concerné ne peuvent consister en une surveillance active de l'ensemble des données de chacun de ses clients afin de prévenir toute atteinte future à des droits de propriété intellectuelle via le site de ce prestataire. Par ailleurs, une telle obligation de surveillance générale serait incompatible avec l'article 3 de la directive 2004/48, qui énonce que les mesures visées par cette directive doivent être équitables et proportionnées et ne doivent pas être excessivement coûteuses[73].

Dans sa décision numéro C‑360/10, Sabam C/ Netlog[74], la Cour de justice rappelle également que la protection du **droit fondamental de propriété**, dont font partie les droits liés à la propriété intellectuelle, doit être mise en balance avec celle d'autres droits fondamentaux. Ainsi, il incombe aux autorités et aux juridictions nationales, dans le cadre des mesures adoptées pour protéger les titulaires de droits d'auteur, d'assurer un **juste équilibre** entre la protection de ce droit et celle des **droits fondamentaux** de personnes qui sont affectées par de telles mesures. Parmi ces droits fondamentaux à mettre en balance figure notamment la **liberté d'expression**, ainsi que la **liberté d'entreprise** des prestataires intermédiaires.

Les Juges de la Cour de Justice concluent que les dispositions de la Directive sur le commerce électronique, de même que les directives 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, et 2004/48/CE du Parlement européen et du Conseil, du 29 avril 2004, relative au respect des droits de propriété intellectuelle,

doivent être interprétées en ce sens qu'elles s'opposent à une injonction faite par un juge national à un prestataire de services d'hébergement de mettre en place un système de filtrage:

---

71 L'article 88-1 CIC prévoit un cadre légal strict pour des mesures de surveillance spéciales ordonnées par un Juge d'instruction.

72 Sur cette question, voir également : T. REISCH, Internet et les nouvelles technologies de la communication face au droit luxembourgeois, éd. Mike Koedinger 2008, p. 75.

73 CJUE 12.07.2011, L'Oréal c/ Ebay n° C-324/09, par. 139.

74 CJUE 16.02.2012, Sabam C/ Netlog n° C-360/10.

- *des informations stockées sur ses serveurs par les utilisateurs de ses services;*
- *qui s'applique indistinctement à l'égard de l'ensemble de ces utilisateurs;*
- *à titre préventif;*
- *à ses frais exclusifs, et*
- *sans limitation dans le temps,*

capable d'identifier des fichiers électroniques contenant des œuvres musicales, cinématographiques ou audiovisuelles sur lesquelles le demandeur prétend détenir des droits de propriété intellectuelle, en vue de bloquer la mise à disposition du public desdites œuvres qui porte atteinte au droit d'auteur.[75]

La solution retenue par les juges européens n'a pas encore fait l'objet d'applications pratiques dans la jurisprudence luxembourgeoise.

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

La **liberté d'expression**, telle que prévue par l'article 10 de la Convention Européenne des Droits de l'Homme (ci-après : la Convention EDH)[76] est également garantie par l'**article 24 de la Constitution** luxembourgeoise[77], ainsi que par la Loi du 8 juin 2004 sur la liberté d'expression dans les médias. Les juridictions nationales suivent la jurisprudence de la Cour EDH[78] et procèdent à une interprétation très large de la liberté d'expression. La satire et la caricature[79], un droit de critique plus étendu à l'égard d'hommes politiques[80] ou encore la liberté d'exprimer des opinions politiques, même susceptibles de choquer les esprits[81], sont notamment consacrés.

Tel qu'exposé ci-dessus, la législation luxembourgeoise ne prévoit pas de procédure spécifique pour le blocage, le filtrage et le retrait de contenus illicites. Ces mesures sont prises dans le cadre de procédures civiles et pénales sur le fondement des règles de **droit commun**[82]. Le défi consiste à appliquer ces règles de nature législative (5.1) à des situations de fait, en se laissant guider par les critères de « poursuite d'un but légitime » (5.2) et de « nécessité dans une société démocratique » (5.3.) prévues par l'article 10, alinéa 2 de la Convention EDH.

---

75 Ibid., par. 26.

76 Nous renvoyons également au texte de l'article 11 de la Charte des Droits Fondamentaux de l'Union Européenne.

77 L'art. 24 de la Constitution prévoit : *« La liberté de manifester ses opinions par la parole en toutes matières, et la liberté de la presse sont garanties, sauf la répression des délits commis à l'occasion de l'exercice de ces libertés.*
La censure ne pourra jamais être établie ».

78 Pour une analyse des décisions de la Cour Européenne ayant vérifié l'application de l'article 10 par les juridictions luxembourgeoises, voir C. HIRSCH, Le Luxembourg et la Cour Européenne des Droits de l'Homme, éd. Larcier 2015, p. 325 et ss.

79 CA 21.06.2011, n° 325/11 V.

80 Voir notamment : CA 24.05.2011, n° 274/11 V.

81 Voir notamment : CA 09.03.2011, n° 126/11 X.

82 Nous rappelons également l'existence d'une procédure administrative devant la CNPD pour des blocages ou retraits liés à la protection des données personnelles – voir le point 2.2.3.2 ci-dessus.

5.1. L'exigence d'une base légale

L'intégralité des mesures décrites au point 2 ci-dessus sont prévues par une loi. Les règles de procédure sont transcrites dans le CIC pour ce qui est des procédures pénales, respectivement dans le NCPC pour ce qui est du domaine civil. Les autres lois spéciales sont regroupées dans un recueil des lois spéciales, librement accessible sur le site internet www.legilux.lu. Ce site met désormais tous les codes, recueils de législation, textes législatifs, avec leurs travaux préparatoires et les règlements d'exécution, à la disposition du grand public.

Les blocages, filtrages et retraits ne sont pas décidés par des organes spécialement créés à cet effet, mais sont mis en œuvre par des juridictions.

Dans les **affaires pénales**, les blocages – fondés sur la saisie du contenu illicite – s'inscrivent dans une **tradition juridique constante**. La saisie du produit de l'infraction, respectivement du moyen pour le commettre, constitue une règle de droit profondément ancrée dans le système juridique.

Il en va de même pour le retrait du contenu, qui s'analyse comme une confiscation.

Les **mesures civiles** peuvent uniquement être prises par un tribunal, qui statue après une **procédure contradictoire**. Le fait de devoir retirer provisoirement ou définitivement des contenus jugés illicites de serveurs liés à Internet s'analyse en une obligation de faire pour la partie qui a succombé à l'instance. Le caractère de prévisibilité nous paraît rempli.

Un autre facteur de taille est que **toutes les décisions** prises par les autorités judiciaires en la matière **peuvent faire l'objet d'un recours**.

En matière pénale, la chambre du conseil contrôle non seulement la conformité de la décision par rapport au droit national, mais également par rapport à la Convention EDH[83]. Des prétendues violations de la liberté d'expression ou du principe de proportionnalité peuvent dès lors être avancées à l'appui d'une demande en annulation d'une décision, dès le moment où celle-ci aura été prise.

Les procédures de référé permettent d'obtenir rapidement une décision d'un juge pour toutes les contestations d'ordre civil.

5.2. La poursuite d'un but légitime

L'article 10, alinéa 2 de la Convention EDH prévoit notamment que la liberté d'expression ne peut faire l'objet d'autres restrictions que celles que *« constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. Le présent article n'interdit pas que des restrictions légitimes soient imposées à l'exercice de ces droits par les membres des forces armées, de la police ou de l'administration de l'Etat »*.

---

83 Voir notamment : CA 22.10.2012, n° 674/12 ; CA 21.01.2014, n°44/14 ; CA 28.01.2014, n° 69/14.

Il appartient aux autorités – et notamment au procureur d'Etat et au juge d'instruction – de vérifier que leur action s'inscrit strictement dans le cadre dressé par cet article[84]. En pratique, des mesures de blocage sont **prises dans le cadre des infractions les plus graves** :

- pédopornographie,
- incitation à la haine raciale[85],
- propagation de logiciels malveillants,
- publication de données à caractère personnel qui ont été exfiltrées d'un système informatique lors d'une cyberattaque,
- atteintes manifestes à la vie privée.

Les choix deviennent plus délicats en matière de diffamations, calomnies et injures. L'infraction de calomnie n'est en effet pas donnée si son auteur prouve la véracité des faits affirmés. Elle n'est encore pas remplie à l'égard de l'éditeur, au sens de la Loi sur la liberté de la presse, s'il prouve, sous réserve d'avoir accompli les diligences nécessaires, qu'il avait des raisons suffisantes pour conclure à la véracité des faits rapportés ainsi que l'existence d'un intérêt prépondérant du public à connaître l'information litigieuse (article 443 du Code pénal).

L'absence d'une atteinte manifeste aux droits de la personnalité d'autrui fragilise la base légale pour pouvoir prendre une mesure de blocage. La prise d'une telle mesure peut encore se heurter au test de proportionnalité, abordé au point 5.3 ci-dessous.

Pour ce qui est des mesures de blocage et de retrait prises par les hébergeurs sur base de l'article 62 de la Loi sur le commerce électronique, nous estimons que celles-ci doivent uniquement être prises – sans autorisation d'un juge – si les contenus sont manifestement illicites[86]. Tel est naturellement le cas pour les contenus à caractère pédopornographique, terroriste, contraire à la dignité humaine ou incitant à la haine. Des considérations techniques, telles que la suppression de virus ou de malware propagés à partir des serveurs de l'hébergeur, nous semble également constituer un but légitime.

La question devient plus complexe pour ce qui est des violations de droits d'auteur, où la qualité à agir de la personne qui en demande la suppression peut notamment poser problème, ou pour les atteintes à la réputation des personnes. Sur ce dernier point, les législations nationales diffèrent fortement, de sorte que la qualification comme licite ou illicite des contenus peut s'avérer difficile pour l'hébergeur. Il peut également être confronté à des problèmes de qualification de contenus (nous renvoyons notamment à l'exemple de la calomnie repris ci-dessus).

Au stade des mesures de blocage[87], nous estimons dès lors qu'une certaine **prudence** doit guider les intervenants.

Cette problématique se pose sous un autre angle pour les mesures de retrait – décidées par des juridictions au fond. Ces mesures s'analysent en effet comme la conséquence d'une condamnation définitive pour une infraction déterminée ou un comportement civilement répréhensible.

---

84 Pour une application rigoureuse de ce texte : Cour administrative 11.12.2012, n° 31148C du rôle, JTL n° 28, p. 107, avec les observations de T. CHEVRIER.

85 Voir notamment : TA Lux. 10.05.2012, n° 1754/2012.

86 Problématique abordée dans A. PRUM, Le commerce électronique en droit luxembourgeois, op. cit., p. 560 et ss.

87 Analysées comme des mesures provisoires conformément à nos développements exposés au point 2 ci-dessus.

5.3. La nécessité des mesures dans une société démocratique

Internet ne constitue pas un monde virtuel, mais un moyen de communication. Les mêmes règles que celles encadrant les relations physiques entre personnes doivent dès lors s'appliquer. Certains types de contenus – tel que le matériel pédopornographique – ne sauraient être acceptés. Leur blocage et retrait s'imposent.

Les réseaux de l'information ne sauraient également devenir des **zones de non-droit** où tout à chacun – sous le couvert de l'**anonymat** – peut porter atteinte aux droits d'autrui. Des restrictions à des abus de la liberté d'expression doivent pouvoir être imposées sur Internet.
Avec l'importance des communications en ligne, des blocages et retraits de contenus illicites sont une nécessité. Ces **mesures sont légalement encadrées**. Leur application se fait sous le **contrôle d'autorités judiciaires** et des **recours sont très largement ouverts à toutes les personnes concernées** (voir notamment les points 2 et 3 ci-dessus).

Vu comme un correctif dans l'application des règles de droit, le **principe de proportionnalité** permet encore de vérifier l'adéquation entre la mesure prononcée avec d'autres règles de droit.

D'un côté, l'application de ce principe peut montrer une disproportion entre la mesure de blocage ou de retrait envisagée pour faire face à une certaine infraction, avec d'autres droits fondamentaux, tels que la liberté d'expression. De l'autre côté, le principe de proportionnalité impose un encadrement de la mesure au strict nécessaire.

Avant la modification législative du 18 juillet 2014[88], la saisie et la suppression des données informatiques n'était pas encadrée par des dispositions spécifiques. Pour bloquer des contenus, les autorités saisissaient physiquement le matériel informatique hébergeant les données litigieuses. Cette mesure pouvait poser problème au regard du principe de proportionnalité, chaque fois qu'elle affectait également des contenus parfaitement licites.
Avec la réforme intervenue en 2014, la législation nationale permet désormais la saisie de données informatiques sous forme d'une copie des données, avec la suppression des données jugées illicites sur leur support d'origine. Un **blocage et un retrait ciblés** sont dès lors possibles.

La conformité de la mesure de blocage par rapport aux principes consacrés et dégagés par la Convention EDH peut être contrôlée par la chambre du conseil[89]. Des violations du principe de proportionnalité peuvent dès lors être reconnues dans un temps très proche de l'exécution de la mesure critiquée.

Du côté des procédures civiles, le juge peut désigner avec précision les contenus devant être bloqués. Le contrôle du principe de proportionnalité peut se faire à tous les stades de la procédure[90].

17 août 2015
Max BRAUN
Révisé le 3/5/2016 en tenant compte des commentaires du Luxembourg sur ce rapport.

---

88 Pour les nouveautés apportées par cette réforme, voir le point 2.1.2. ci-dessus.

89 Voir notamment : CA 16.05.2012, n° 301/12 ; CA 22.10.2012, n° 674/12.

90 Pour un exemple pratique, voir : TA Lux. 11.05.2011, n° 349/2011 et TA Lux. 11.03.2014, n° 54/2014.