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 75-87

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.

BELGIQUE

Dans la version anglaise, cette partie apparaît dans les pages 75 à 87

La Belgique fait partie des Etats qui disposent d'une législation permettant de bloquer ou de retirer certaines informations illicites sur internet.

1. Sources

La Belgique a ratifié nombre de standards internationaux dans le domaine de la gouvernance d'internet. La Convention sur la cybercriminalité, conclue à Budapest le 23 novembre 2001, est entrée en vigueur en Belgique le 1er décembre 2012 en application de la loi du 3 août 2012 portant assentiment de ladite convention[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, quant à lui, été signé par la Belgique, mais n'a toujours pas été ratifié. La Belgique a également signé la Convention du Conseil de l'Europe pour la prévention du terrorisme mais celle-ci n'a pas été ratifiée. La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels est entrée en vigueur sur le territoire de la Belgique le 1er juillet 2013, suite à divers actes législatifs portant son assentiment selon les différentes sphères de compétences fédérales et régionales concernées[2]. Enfin, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel est entrée en vigueur en Belgique le 1er Septembre 1993, suite à l'adoption de plusieurs actes législatifs dans ce domaine.

Les mesures de blocage et de retrait de contenu d'internet sont, en Belgique, réglementées dans plusieurs dispositions légales, de nature différente. Toutefois, avec la récente codification de plusieurs lois dans le code de droit économique, plusieurs de ces dispositions se retrouvent dans des sections différentes du même code. Ainsi, le code de droit économique comprend, à son titre XII, les mesures ayant transposé les dispositions de la directive 2000/31/CE sur le commerce électronique, et au titre XI, les mesures spécifiques en matière de protection des droits de propriété intellectuelle. De plus, certaines prérogatives en matière de blocage et de retrait de contenu d'internet sont prévues dans des lois spéciales et par le Code d'instruction criminelle.

---

1 Loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité, M.B., 21.11.2012.

2 Loi du 7 février 2012 portant assentiment à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, faite à Lanzarote le 25 octobre 2007, M. B., 21. 06.2013 ; Décret du 28 avril 2011 portant assentiment à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, faite à Lanzarote le 25 octobre 2007, M. B., 13.05.2011 ; Décret du 28 mars 2011 portant assentiment à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, faite à Lanzarote le 25 octobre 2007, M. B., 29.04.2011 ; Décret du 12 février 2010 portant assentiment à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, faite à Lanzarote le 25 octobre 2007, M. B., 04.03.2010 ; Décret du 26 avril 2012 portant assentiment, pour ce qui concerne les matières dont l'exercice a été transféré par la Communauté française à la Région wallonne, à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, faite à Lanzarote le 25 octobre 2007, M. B., 22.05.2012 ; Ordonnance du 1er mars 2012 portant assentiment à la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, faite à Lanzarote le 25 octobre 2007, M. B., 14.03.2012.

2. Réglementation applicable en matière de blocage et/ou retrait de contenu illégal d'internet

Les mesures de blocage et de retrait sont examinées au sein d'une même section étant donné que la loi traite du régime légal applicable à ces mesures de manière jointe.

Les possibilités de blocage et/ou de retrait de contenu sur internet diffèrent selon le contenu concerné. Selon les domaines en cause, deux types de procédures différentes permettent d'appliquer le blocage et/ou le retrait de contenus sur internet : (a) un réquisitoire du Parquet, et (b) une décision de l'autorité judiciaire. Ces procédures doivent être combinées, le cas échéant, avec des règles spécifiques liées à la responsabilité des fournisseurs de services sur internet, adoptées en application de la directive 2000/31/CE relative au commerce électronique.

2.1. Atteinte à l'ordre public, à la sécurité nationale et prévention de troubles ou de crimes

Les mesures de blocage sont décidées par l'autorité compétente dans le cadre de la procédure pénale, en application des dispositions du code d'instruction criminelle en matière de saisie de données informatiques. En effet, pour pallier au fait que la saisie matérielle des choses, en ce qu'elle implique la dépossession de la chose des mains de la personne concernée par la saisie, n'est pas toujours souhaitable et/ou possible lorsqu'elle porte sur des données informatiques, le législateur a prévu la possibilité pour l'autorité compétente de procéder à une **nouvelle forme de saisie relative aux données informatiques**.

Ces mesures sont prises au **stade de la recherche des infractions pénales et de leur(s) auteur(s)**, soit avant le stade de la décision du juge pénal quant à la culpabilité de la personne concernée au regard du code pénal. Elles sont prises **par le procureur du Roi** dans le cadre d'une information en matière pénale (art. 39bis du Code d'instruction criminelle (« CIC »)) **ou par le juge d'instruction** lorsqu'une instruction est ouverte (art. 89 CIC).

L'instruction est dirigée par le juge d'instruction qui exerce ses fonctions en matière d'établissement de la vérité de manière indépendante et tant à charge qu'à décharge de la personne concernée. Elle est obligatoire en matière criminelle et facultative en matière délictuelle. Le juge d'instruction intervient généralement sur saisine du procureur du Roi.

En revanche, **l'information** est dirigée par le procureur du Roi qui relève, quant à lui, du Ministère Public. Le procureur du Roi peut poursuivre soit d'office soit à la suite d'une plainte d'un utilisateur déposée auprès des services de police compétents[3]. Jusqu'il y a peu, les services de police avaient mis à la disposition des utilisateurs une plate-forme de dénonciation de toute infraction commise sur ou par le biais d'internet (www.ecops.be). En raison du trop grand nombre de plaintes déposées, dans tous domaines, celle-ci a récemment été fermée et un nouveau système de dénonciation est en train d'être développé. D'ici là, les utilisateurs sont priés de s'adresser aux services de police de droit commun qui transmettront le cas échéant aux services de police spécialisés en matière d'informatique, la *Federal Computer Crime Unit* au niveau national au sein de la direction centrale de lutte contre la criminalité grave et organisée (FCCU) ou des *Computer Crime Unit* régionaux (CCU) au sein de chaque arrondissement judiciaire sous la direction des directeurs judiciaires.

---

[3] Pour certaines infractions, le législateur a subordonné la poursuite à une plainte préalable de la personne lésée ; comme, par exemple, la calomnie et la diffamation (art. 450 Code Pénal).

En application de l'article 39bis CIC (ou de l'art. 89 CIC), il est en principe procédé à la **saisie du support matériel des données concernées**, ou si une telle saisie n'est pas souhaitable à la **copie de ces données** sur des supports appartenant à l'autorité (art. 39bis §2 CIC). En application de l'article précité, en plus de la copie des données en cause – ou au lieu d'une telle copie lorsque celle-ci n'est pas possible pour des raisons techniques ou à cause du volume des données:

«[Le procureur du Roi ou le juge d'instruction] utilise en outre les moyens techniques appropriés pour **empêcher l'accès** à ces données [qui sont utiles pour les mêmes finalités que celles prévues pour la saisie] dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité. »[4]

La mesure visant à rendre inaccessibles les données copiées ou faisant l'objet de la saisie, constitue une **mesure de blocage**. Soit elle se combine avec la copie des données prévue à l'art. 39bis §2 CIC, soit, si une telle copie n'est pas possible, elle peut être ordonnée seule en application de l'art. 39bis §4 CIC.

L'ensemble de ces mesures – la copie et/ou l'inaccessibilité des données – permet d'assurer l'établissement de la vérité et sa conservation dans le but du jugement sur le fond. La disposition laisse une marge de manœuvre au **procureur du Roi ou au juge d'instruction : il peut décider – sans y être tenu –** de les rendre inaccessibles, soit **d'en bloquer l'accès**. Ainsi, si les données et leur exploitation par la personne suspectée d'être coupable d'une infraction pénale permettent d'établir la culpabilité de ladite personne, il est probable que l'accès n'en soit pas bloqué afin de récolter les éléments de preuve nécessaires à confondre la personne en cause.

Toujours dans le cadre d'une saisie de données informatiques, le législateur est toutefois allé plus loin. L'article 39bis para. 3 al. 2 CIC prévoit en effet que :

« [S]i les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi [ou le juge d'instruction] utilise tous les moyens techniques appropriés **pour rendre ces données inaccessibles** » (nous soulignons).

Ainsi, si les données en cause présentent la caractéristique de constituer **l'objet de l'infraction** (par exemple, un contenu révélateur d'une infraction terroriste) ou ont été produites par l'infraction (par exemple, un faux informatique) **et** d'être **contraire à l'ordre public ou aux bonnes mœurs** (par exemple, les infractions de contenu), **le procureur du Roi ou le juge d'instruction est tenu de les rendre inaccessibles** par tous les moyens techniques appropriés. D'après les travaux préparatoires de la loi du 28 novembre 2000 sur la criminalité informatique, cette disposition précise se distingue des autres prévues par l'art. 39bis CIC en ce qu'elle permet au procureur du Roi ou au juge d'instruction **d'éliminer les données informatiques concernées**.

En ce qui concerne l'ensemble de ces mesures visant à rendre inaccessible des données, la loi ne donne pas plus de détails sur ce qu'il convient d'entendre par « les **moyens techniques appropriés** » pour parvenir à une telle fin. La doctrine précise que les autorités en charge de l'information ou de l'instruction consultent les services de police spécialisés dans le domaine de l'informatique, la FCCU ou les CCU. D'après les travaux préparatoires de la loi, les mesures visant à « empêcher l'accès » aux

---

4 Art. 39bis, para. 3 al. 1er CIC. Voir aussi Art. 39bis, para. 4 CIC. Le CIC est librement consultable sous : http://www.ejustice.just.fgov.be/loi/loi.htm (15.08.2015).

données informatiques, visées à l'art. 39bis §3 al.1er et §4 CIC, ne concernent **que des mesures de blocage d'accès au site internet** ne concernant dès lors que les fournisseurs d'accès à internet ; en revanche, les mesures visant à « rendre inaccessibles » lesdites données, prévues à l'art. 39bis § » al. 2 CIC, concernent **tant des mesures de blocage que des mesures de retrait des données** en cause et sont destinées aussi bien aux fournisseurs d'accès à internet qu'aux hébergeurs[5]. Ainsi, dans un arrêt du 22 octobre 2013, la Cour de Cassation a rappelé que les fournisseurs d'accès à internet pouvaient se voir contraints, en vertu de l'art. 39bis §4 CIC, de bloquer l'accès aux données en cause dans le système informatique[6]. En pratique, en ce qui concerne le retrait des données en application de l'art. 39bis §3 al. 2 CIC il sera procédé au retrait des dites données si l'hébergeur est en Belgique et au blocage des données par l'intermédiaire des fournisseurs d'accès à internet lorsque les hébergeurs sont situés à l'étranger.

Du fait qu'ils interviennent dans le cadre d'une enquête pénale, il est fait peu de publicité des cas d'application de telles mesures de blocage et/ou retrait. Il ressort toutefois de la presse que le site internet du groupuscule « Sharia4Belgium » aurait été rendu inaccessible en juin 2012 dans le cadre d'une enquête pénale pour incitation aux émeutes de Bruxelles en 2012, en réaction à l'arrestation d'une femme qui avait refusé de retirer son *niqab* dont le port en public est interdit en Belgique[7]. De telles mesures auraient, sous toute vraisemblance, été adoptées en application des articles 39bis et/ou 89 CIC.

Les mesures prises en application de l'article 39bis, para. 3 al.2 CIC ont fait l'objet de critiques, en ce sens que les mesures de blocage et/ou de retrait de contenu illicite adoptées en application de cette disposition sont d'une part destinées à être temporaires pour les besoins de l'enquête et non permanentes alors qu'en pratique, les décisions prises en application de cette disposition sont permanentes. D'autre part, on a argumenté que ces mesures de blocage et/ou de retrait devraient en réalité être destinées à l'établissement de la vérité et la conservation des preuves et non à rendre inaccessible un contenu illicite. Ceci dit, dans l'affaire The Pirate Bay, la Cour de Cassation a confirmé, dans son arrêt du 22 octobre 2013, qu'un « ordre émis par le juge d'instruction sur la base de l'article 39bis du Code d'instruction criminelle peut être délivré en vue de la recherche de la vérité, de la confiscation, de la restitution, la cessation d'agissements qui semblent constituer une infraction ou de la sauvegarde des intérêts civils ». La Cour de Cassation a également précisé que de telles mesures ne constituaient pas une obligation générale de surveillance, interdite en application de l'art. 15 de la Directive 2000/31/CE[8].

Ces mesures doivent être combinées avec certaines règles spéciales en matière d'exonération de responsabilité des **fournisseurs de services d'hébergement** sur internet. En application de la directive 2000/31/CE, l'article XII.19 du code de droit économique (CDE) prévoit que le fournisseur d'hébergement n'est pas tenu responsable des informations stockées à condition (a) « qu'il n'ait pas connaissance effective de l'activité ou de l'information illicite, ou, en ce qui concerne une action civile en réparation, qu'il n'ait pas connaissance de faits ou de circonstances laissant apparaître le caractère illicite de l'activité ou de l'information » ; ou (b) « qu'il agisse promptement dès le moment

---

5 Voir notamment : B. Losdyck, Les saisies et les perquisitions de matériel informatique : les « garde-fous » entourant leur mise en œuvre, RDTI, 2013/52, p. 36.

6 Cass., 22 octobre 2013, R.G. n° P.13.0550.N, Tijdschrift voor Strafrecht , note de : SCHOEFS, Raf; Noot 'Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan' 2014, nr. 2, p. 126-142.

7 Voir notamment : http://www.lesoir.be/7764/article/actualite/belgique/2012-06-07/porte-parole-sharia 4belgium-arr%C3%AAt%C3%A9 (15.08.2015).

8 Cass. 22 octobre 2013, n° P.13.0550.N, disponible sous : http://jure.juridat.just.fgov.be/JuridatSearch Combined/?lang=fr&jur=1 (15.08.2015).

où il a de telles connaissances, pour retirer les informations ou rendre l'accès à celles-ci impossible et pour autant qu'il agisse conformément à la procédure [décrite ci-dessous] ». En effet, la loi prévoit encore que « lorsque [le fournisseur d'hébergement] a une connaissance effective d'une activité ou d'une information illicite, il les communique sur le champ au procureur du Roi » et qu' « aussi longtemps que le procureur du Roi n'a pris aucune décision concernant le copiage, l'inaccessibilité et le retrait de documents stockés dans un système informatique, le [fournisseur d'hébergement] peut uniquement prendre des mesures visant à empêcher l'accès aux informations».

Ce dispositif est utilement précisé par les travaux préparatoires de la loi qui a initialement transposé la directive 2000/31/CE sur ce point. L'exposé des motifs prévoit ainsi que :

« Il conviendra de ne retenir la responsabilité du prestataire d'hébergement qu'à la triple condition qu'il ait eu **connaissance de la présence sur son serveur d'un contenu litigieux**, que ce dernier ait été **manifestement illicite** […] et qu'il ait fait preuve d'**inertie**. »[9]

L'art. XII.19 CDE fait référence au principe « ***notice and take down*** », en application duquel le fournisseur d'hébergement est tenu de retirer le contenu illicite dès le moment où il en a connaissance effective. Toutefois, le législateur précise le mécanisme de la façon suivante : dès qu'il a **connaissance** d'un contenu illicite, **l'hébergeur est tenu de prendre les mesures pour le rendre inaccessible** et d'en informer le procureur du Roi. **Tant que le procureur du Roi ou le juge d'instruction n'a pas pris les mesures de blocage ou de retrait** visées à l'article 39bis CIC ou 89 CIC, **le fournisseur d'hébergement ne peut toutefois que bloquer l'accès au site concerné (à l'exclusion des mesures de retrait).** Une fois que ces mesures sont ordonnées dans le cadre d'une enquête pénale, l'hébergeur est bien entendu obligé de les exécuter. D'après la *ratio legis* de la loi, l'hébergeur ne sera toutefois tenu responsable que si, cumulativement, il avait connaissance du contenu illicite, que ce contenu était ***manifestement* illicite**, et qu'il n'a pas pris les mesures pour le rendre inaccessible. Par « manifestement illicite », le législateur entend des contenus de type révisionniste, pédophile ou encore incontestablement outrageant[10]. Des informations plus précises ne sont pas disponibles.

2.2. Atteinte à la santé publique et aux bonnes mœurs

La situation est similaire en tous points lorsque le contenu est illicite en ce qu'il contient des **images pédopornographiques**. La pédopornographie étant pénalement punissable[11], l'information ou l'instruction permettra de prendre les **mesures de blocage ou de retrait que le procureur du Roi ou le juge d'instruction jugera utile**, et ce, en application des articles 39bis CIC ou 89 CIC (voir ci-dessus, section 2.1).

On relève que depuis la fermeture de la plate-forme de dénonciation des contenus illicites (www.ecops.be), les utilisateurs peuvent dénoncer les infractions pédopornographiques auprès de la Fondation pour Enfants Disparus et Sexuellement Exploités, fondation d'utilité publique belge, connue sous la dénomination « **Child focus** ». Cette fondation est alors chargée de transmettre l'information aux services de police spécialisés dans le domaine d'internet.

Les sites pédopornographiques sont également susceptibles de faire l'objet de mesures de blocage par l'hébergeur directement qui aurait connaissance effective du contenu illicite de ce site, et ce, en application de l'art. XII.19 CDE (voir ci-dessus, section 2.1). Une telle mesure peut donner lieu à un

---

9 Travaux Parlementaires, 2002-2003, Doc. 50/2100/01, p.48.

10 Ibidem.

11 Voir notamment: Art. 383bis Code Pénal.

contentieux devant le juge civil. Ainsi, dans une affaire où une personne a développé et exploité un site internet à partir duquel était proposé, sous le couvert de sa responsabilité et sans qu'il l'ignore, un ensemble d'hyperliens renvoyant à des sites ayant clairement un contenu pédopornographique, la Cour de Cassation a validé la décision de la Cour d'appel ayant considéré que cette personne ne pouvait pas bénéficier de l'exonération de responsabilité sous conditions dont privilégie ceux qui exercent une activité d'hébergeur.[12]

En ce qui concerne la **lutte contre les jeux de hasard en ligne**, la Commission des Jeux de Hasard a dressé une **liste noire des sites de jeux de hasard en ligne qui n'ont pas obtenu la licence nécessaire** pour leur exploitation. Cette liste est librement accessible sur le site internet de la Commission[13]. Ces sites de jeux de hasard en ligne sont bloqués à la suite d'un accord conclu par la Commission avec les divers fournisseurs d'accès à internet présents sur le marché belge[14]. Ces sanctions de blocage s'accompagnent d'un gel des transferts de capitaux depuis et vers ces sites. L'ensemble de ces sanctions présentent une nature contractuelle, mais elles peuvent également intervenir dans le cadre d'une procédure pénale en application des art. 39bis et 89 CIC.

En ce qui concerne les services de médias audiovisuels, les communautés sont les seules compétentes pour les réguler. Le Décret flamand des médias du 27 mars 2009[15], qui fournit le cadre juridique flamand, offre la possibilité de bloquer certains types de contenus audiovisuels en passant par Internet. L'article 44 de ce texte permet au *Vlaamse Regulator voor de Media* (l'autorité flamande de régulation des médias) de forcer un fournisseur de services ou un opérateur de réseau à suspendre temporairement la transmission de programmes de télévision linéaires d'une chaîne de télévision lorsqu'il s'agit d'une violation de l'art. 38 et/ou 42 du même décret, à savoir les programmes incitant à la haine et ces dont le contenu est préjudiciable au développement physique, mental ou moral des mineurs. Par conséquent, si ces programmes de télévision linéaires devaient être transmis par Internet, le régulateur pourrait forcer l'opérateur du réseau ou le fournisseur de bloquer ~~la~~ leur transmission. Cette législation se base sur l'article 3 de la Directive 2010/13/UE du 10 mars 2010 sur les services de médias audiovisuels. Pour la Communauté française de Belgique, les articles pertinents sont les articles 9 et 159 du Décret coordonné sur les services de médias audiovisuels du 26 mars 2009.

2.3. Atteinte aux droits d'autrui

La **lutte contre la discrimination** fait l'objet de plusieurs législations, tant au niveau fédéral qu'au niveau des communautaire et régional[16]. Au niveau fédéral, la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination et la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie, octroient un rôle important au **Centre interfédéral**

---

12 Cass. 03.02.2004, P.03.1427.N, disponible sous : http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1 (15.08.2015).

13 Voir : https://www.gamingcommission.be/opencms/opencms/jhksweb_fr/establishments/Online/blacklist/index.html (15.08.2015).

14 Ibidem.

15 Une version anglaise de ce texte peut être consultée via http://www.vlaamseregulatormedia.be/sites/default/files/act_on_radio_and_television_broadcasting.pdf.

16 Pour un aperçu de l'ensemble de la législation applicable sur le territoire belge en matière de lutte contre la discrimination, voir : http://www.diversite.be/photographie-des-legislations-antidiscrimination (15.08.2015).

pour l'égalité des chances qui est une administration publique indépendante compétente dans le domaine (le « Centre »).

Le Centre est tout d'abord l'interlocuteur privilégié des victimes qui peuvent s'adresser au Centre pour un premier conseil sur les situations discriminatoires rencontrées par celle-ci mais aussi pour la gestion d'un conflit. Ainsi, le Centre peut donner diverses suites à un signalement entrant dans sa compétence : tout d'abord, la négociation et la conciliation des parties sera privilégiée ; ensuite, le Centre peut adresser à la personne ou à l'institution mise en cause une mise en garde et un rappel de la loi ; il peut aussi saisir l'autorité hiérarchique ou disciplinaire de la personne mise en cause ; le Centre est également compétent pour donner des avis dans le cadre de procédures judiciaires sans être partie au procès ; enfin, le Centre peut initier ou se joindre à une action en justice, que celle-ci soit pénale ou civile. Lorsqu'il agit en justice, le Centre agit toujours en son nom propre et pour son propre compte et non pour ceux de la victime.

En matière d'action civile, les lois précitées octroient toutes deux la possibilité au **juge civil** de constater l'existence d'un acte constitutif d'une violation des dispositions légales précitées et d'en ordonner la cessation, même si cet acte est aussi pénalement réprimé. **L'action en cessation** est formée et instruite selon les formes du référé, par le président du tribunal de première instance, ou, selon la nature de l'acte, par le président du tribunal du travail ou celui du tribunal de commerce[17]. Sur internet, la cessation comprend l'obligation éventuelle de l'hébergeur ou d'autres acteurs de **retirer le contenu illicite d'internet ou de le rendre autrement inaccessible**. Ces lois prévoient encore que lorsque les faits qui font l'objet de l'action en cessation sont également soumis à un juge pénal, celui-ci ne peut statuer sur l'action pénale qu'après qu'une décision coulée en force de chose jugée ait été rendue en ce qui concerne l'action en cessation[18]. L'action en cessation est introduite par l'utilisateur victime mais elle peut aussi l'être par le Centre, par l'un des groupements d'intérêts, par le ministère public, ou selon la nature de l'acte, par l'auditorat du travail.

S'il y a matière à infraction pénale, le Centre ou l'utilisateur victime peut déposer une **plainte pénale** auprès du Parquet ou de la police qui prendra, s'il estime qu'elles sont justifiées, les mêmes mesures en matière de blocage et/ou retrait que celles exposées à la section 2.1.

La procédure et les **mesures de blocage et/ou de retrait** exposées à la section 2.1 sont également applicables lorsque les actes portant atteinte aux droits d'autrui sur internet constituent des **infractions de diffamation ou d'atteinte à l'honneur**, infractions pénalement réprimées.

On relève encore un règlement spécifique en matière de **protection de la vie privée**. En application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[19], le **fournisseur de services sur internet peut être tenu**, en application d'une décision rendue **par le président du tribunal de première instance**, **de supprimer des données à caractère personnel** qui n'auraient pas été traitées dans certaines conditions prévues par la loi[20].

---

17 Voir : Art. 20 Loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination (M.B., 30.05.2007) et art. 18 Loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie, modifiée par la loi du 10 mai 2007 (MB 30.05.07) et la loi du 17 août 2013 (M.B. 05.03.2014).

18 Ibidem.

19 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B., 18 mars 1993.

20 Voir art. 12 et 14 Loi du 8 décembre 1992.

De plus, la loi précitée prévoit certaines **infractions pénales** en matière de protection de la vie privée[21]. Lorsque ces infractions sont reconnues établies, **le juge pénal peut ordonner l'effacement des données** à caractère personnel concernées[22].

De tels ordres en matière de protection de la vie privée pourront s'adresser, le cas échéant, au fournisseur de services internet qualifié de «responsable de traitement »[23] ou de « tiers »[24] exécutant le « traitement des données personnelles »[25] pour le compte du responsable de traitement.

La Commission de la vie privée, instituée par la loi du 8 décembre 1992, peut enfin dénoncer certains actes constitutifs **d'infractions pénales** dans le domaine de sa compétence auprès du Parquet – ce qui pourra, le cas échéant, aboutir à des **mesures de blocage et/ou de retrait** de contenu illicite sur internet (voir ci-dessus, section 2.1).

Enfin, il convient de relever qu'en toutes matières, le droit judiciaire connaît la procédure en référé qui permet de solliciter au président du tribunal de commerce ou du tribunal de première instance que des mesures provisoires soient prises en attendant le règlement du litige au fond lorsque l'urgence de la situation le justifie. Dans le cadre de cette procédure, le président peut « ordonner **toutes mesures nécessaires à la sauvegarde des droits de ceux qui ne peuvent y pourvoir**»[26]. En cas d'absolue nécessité, ledit président peut même être saisi par simple requête de la partie intéressée.

2.4. Atteinte aux droits de propriété intellectuelle

Les droits de propriété intellectuelle bénéficient également d'une protection efficace devant le juge civil, qu'il s'agisse du président du tribunal de première instance ou celui du tribunal de commerce (selon la nature des faits de la cause)[27]. Dans le cadre d'une **action dite en cessation**, celui-ci peut en effet **ordonner, une fois qu'il a constaté une atteinte aux droits de propriété intellectuelle, aux intermédiaires de cesser les services qu'ils mettent à disposition et qui sont utilisés par les tiers pour violer les droits de propriété intellectuelle**[28].

---

21 Voir en particulier : Art. 39 Loi du 8 décembre 1992.

22 Art. 41 Loi du 8 décembre 1992.

23 Par «responsable du traitement», on entend la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel (Art. 1er, par. 4, al. 1er Loi 8 décembre 1992).

24 Par «tiers», on entend la personne physique, la personne morale, l'association de fait ou l'administration publique, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données (Art. 1er, par. 6 Loi 8 décembre 1992).

25 Par «traitement», on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que 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 de données à caractère personnel (Art. 1er, par. 2 Loi 8 décembre 1992) ; on entend par «données à caractère personnel» toute information concernant une personne physique identifiée ou identifiable, désignée ci-après «personne concernée»; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale (Art. 1er, par. 1er Loi 8 décembre 1992).

26 Art. 584 Code judiciaire

27 Art. XVII.14 CDE.

28 Art. XI.334 para. 1er al. 2 CDE et art. XVII.14 para. 4 CDE.

Il en va ainsi en application de l'art. XI. 334 CDE en ce qui concerne les atteinte à un brevet d'invention, à un certificat complémentaire de protection, à un droit d'obtenteur, à un droit d'auteur, à un droit voisin, au droit d'un producteur de bases de données ou au droit sur une topographie d'un produit semi-conducteur. Pour d'autres types de droits de propriété intellectuelle, dont la **protection des marques**, l'art. XVII.14 par. 1er et 4 CDE prévoit que les titulaires de droits de propriété intellectuelle, dont les titulaires de marques, disposent d'une action en cessation à l'égard du responsable de l'atteinte et que le tribunal compétent peut également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit.

L'action en cessation en matière de protection des droits de propriété intellectuelle a été appliquée à plusieurs reprises par les tribunaux.

Dans une affaire concernant des atteintes aux droits d'auteurs rendues possibles par l'utilisation du site internet « **thepiratebay.org** » en Belgique, la Cour d'appel d'Anvers a ordonné, sur le plan civil et en application de l'action en cessation visée à l'art. XI.334 CDE, à deux fournisseurs d'accès à internet, de bloquer l'accès pour leurs abonnés au site The Pirate Bay, par la mise en place d'un blocage par DNS, et ce, sur demande de la *Belgian anti-piracy federation* (B.A.F.). L'arrêt vient en opposition de la décision du tribunal de commerce d'Anvers qui avait refusé d'imposer aux fournisseurs d'accès à internet une telle mesure de blocage, jugée disproportionnée selon lui par rapport à l'infraction, en remettant en question la pertinence et l'efficacité de la mesure demandée[29]. Suite à l'arrêt de la Cour d'Appel, la B.A.F. a adressé un courrier à d'autres fournisseurs d'accès à internet, les mettant en demeure de les poursuivre en justice s'ils ne bloquaient pas également l'accès au site concerné. Une telle démarche a été vivement critiquée car elle force la prise de mesures de blocage par les fournisseurs d'accès à internet, en dehors d'une intervention judiciaire et sans que la société civile ni les utilisateurs finaux ne soient consultés[30]. Il résulte des faits de la cause que la mesure de blocage du site internet a ensuite été contournée. La B.A.F. a alors décidé de porter plainte au pénal pour les infractions de contrefaçon en matière de droits d'auteur commises par le biais dudit site internet (cf. ci-dessous).
Dans une autre affaire ayant opposé la société de produits de parfumerie et de cosmétiques, Lancôme, la société de vente de biens et services en ligne, eBay, à propos de la mise en ligne sur le site de vente en ligne de eBay, de contrefaçons de produits de la marque Lancôme. La demande en justice de Lancôme visait à obtenir qu'eBay soit tenu d'empêcher l'affichage en ligne de tels produits et de payer à Lancôme des dommages-et-intérêts. La société eBay, quant à elle, faisait valoir son statut d'hébergeur et l'irresponsabilité sous conditions qui en découle. Dans son jugement, le tribunal de commerce précise tout d'abord le type d'activité exercée par eBay dans le cadre de l'affichage des ventes proposées par ces clients, et en déduit qu'il s'agit, pour cette activité concernée d'eBay, d'une **activité d'hébergement**, bénéficiant d'une exonération de responsabilité dans les conditions prévues par la loi belge (cf. section 2.1. ci-dessus). Le tribunal précise encore qu'**eBay a toujours veillé à répondre aux demandes de Lancôme de retirer d'internet certains contenus** qui étaient reconnus comme illicites, mais qu'il est légitime de considérer qu'**eBay doit pouvoir vérifier le bien-fondé des prétentions de Lancôme** au sujet de chaque contenu visé et qu'il ne peut être ordonné à eBay de prendre des **mesures pour éviter que pareille illicéité ne se**

---

29 Anvers (1re ch.) n° 2010/AR/2541, 26 septembre 2011, AM 2012, liv. 2-3, 216; Computerr. (Pays-Bas) 2013, liv. 4, 217, note TSHIANANGA, B., SOMERS, G.; ICIP 2011, liv. 5-6, 731; RABG 2011, liv. 18, 1269, note VAN EECKE, P., FIERENS, A.

30 Voir notamment : https://www.eff.org/fr/deeplinks/2011/12/belgian-isps-vs-internet-freedom (15.08.2015).

reproduise, car cela **constituerait une obligation générale de surveillance interdite** par la directive 2000/31/CE[31].

On relève encore l'affaire ayant opposé la Société belge des auteurs, compositeurs et éditeurs (**SABAM**) à Scarlet (anciennement Tiscali), un fournisseur d'accès à internet, dans un litige dans lequel la SABAM cherchait, sur base de l'action en cessation visée à l'art. XI.334 CDE (anciennement art. 87 de la loi du 30 juin 1994 relative aux droits d'auteur et droits voisins), à contraindre judiciairement Scarlet à prendre des mesures pour faire cesser les atteintes aux droits d'auteur commises par les clients de celle-ci. La Cour d'appel de Bruxelles a, dans son arrêt du 28 janvier 2010, décidé de poser à la Cour de Justice de l'Union européenne (CJUE) deux questions préjudicielles. La CJUE a répondu à ces deux questions après les avoir reformulées, dans son arrêt du 24 novembre 2011[32]. Elle estime que si les obligations générales de surveillance sont interdites, **un juge peut enjoindre à un** fournisseur d'accès à internet ou à tout autre **intermédiaire technique**, de prendre des **mesures visant à mettre fin à des atteintes à des droits de propriété intellectuelle, ou visant à prévenir de nouvelles atteintes**. Selon la CJUE, de telles mesures peuvent être prises à l'encontre d'un fournisseur d'accès à internet **pour autant qu'elles respectent les limitations prévues dans les directives** 2001/29, 2004/48 et 2000/31. Les mesures prises doivent être **effectives et dissuasives**, **ne pas consister en une obligation générale de surveillance** et assurer un **juste équilibre entre les droits et libertés**. **La mesure souhaitée par la SABAM**, qui obligerait le fournisseur d'accès à internet à procéder à une surveillance active de l'ensemble des communications électroniques de tous ses clients pour y identifier celles qui sont illicites, **correspondrait à une surveillance généralisée**, incompatible avec l'art. 15 de la directive 2000/31/CE ainsi que l'art. 3 de la directive 2004/48/CE. De l'avis de la CJUE, la mise en place d'un système de filtrage, pour un temps illimité, aux seuls frais du fournisseur d'accès à internet, en vue de faire cesser les atteintes actuelles et de prévenir des atteintes futures, et impliquant une analyse systématique de tous les contenus échangés avec collecte des adresses IP des clients dudit fournisseur, **ne préserve pas l'équilibre que le juge doit rechercher entre la protection des droits des titulaires de droits d'auteur et d'autres droits fondamentaux, dont la liberté d'expression**. Ainsi, en ce qui concerne cette dernière, la mesure en cause est jugée contraire au droit communautaire étant donné qu'elle **ne distingue pas suffisamment entre un contenu illicite et un contenu licite**, et que, partant, sa **mise en place risquerait d'entraîner le blocage de communications à contenu licite**.

En application des dispositions du livre XI ainsi que du livre XV du Code de droit économique, certaines atteintes aux droits de propriété intellectuelle sont constitutives d'**infraction pénale**[33]. Dans un tel cas, les mesures de blocage sont décidées par le Procureur du Roi ou le juge d'instruction en application des dispositions du code d'instruction criminelle en matière de **saisie de données informatiques** (voir ci-dessus la section 2.1). Dans les hypothèses où les éléments du dossier font apparaître l'existence d'une infraction pénale, le Parquet ou le juge d'instruction peut décider de rendre les données informatiques inaccessibles, en application des art. 39bis CIC ou 89 CIC. Nous renvoyons sur ce point aux détails exposés ci-dessus (section 2.1). Il convient toutefois de noter qu'une contrariété à l'ordre public ou aux bonnes mœurs sera plus difficilement démontrable en ce qui concerne une violation de droits de propriété intellectuelle. Le Parquet est saisi soit d'initiative soit par une plainte d'un utilisateur, le cas échéant par l'intermédiaire des services du service public fédéral pour l'économie.

---

31 Comm. Bruxelles (7è Ch.), 31 juillet 2008, RDTI, 2008, n°33, p. 521 et s.

32 CJUE, 24 novembre 2011, Scarlet extended SA c. Sabam, aff. C-70/10.

33 Sont ainsi notamment prévus par le CDE, le délit de contrefaçon en matière de droits d'auteur et droits voisins (art. XI.293 CDE et art. XV.104 CDE), le délit de contrefaçon en matière de droits d'auteur sur un programme d'ordinateur (art. XI.304 CDE et art. XV.105 CDE) ou encore le délit en matière de marque (art. XV.103 et s. CDE).

En lien avec l'action en cessation précitée dans l'affaire relative à *The Pirate Bay*, et suite au contournement de la mesure de blocage de site internet ordonnée au civil, des mesures de blocage ont été mises en œuvre au niveau pénal, dans le cadre de l'enquête pénale sur les atteintes aux droits d'auteurs résultant de l'utilisation sur internet depuis la Belgique du site « **thepiratebay.org** ». Dans cette affaire, le juge d'instruction avait rendu une ordonnance ordonnant à tous les opérateurs et fournisseurs d'accès à internet de rendre l'accès au site « thepiratebay.org » inaccessible. Plus précisément, l'ordonnance indiquait que le contenu hébergé par le serveur couplé au nom de domaine « thepiratebay.org » devait être rendu inaccessible. De plus, il était exigé des opérateurs qu'ils mettent en œuvre tous les moyens techniques possibles pour bloquer l'accès aux noms de domaines qui renvoyaient vers ce serveur. **L'ordonnance** précisait les moyens techniques qui pouvaient être mis en œuvre pour déterminer les noms de domaines concernés. De cette manière, le juge d'instruction entendait empêcher les mesures de contournement de l'ordre de blocage. L'ordre rendu restait en effet « ouvert » et **permettait le blocage de certains noms de domaine non expressément mentionnés dans l'ordre mais suffisamment identifiés**. Plusieurs opérateurs ont fait appel de cette décision. La Cour de Cassation a cependant refusé de sanctionner la Chambre du conseil qui avait confirmé cette ordonnance, estimant que des mesures adoptées en application des articles 39bis et 89 CIC pouvaient valablement être adoptées dans le but de contribuer à l'établissement de la vérité, de procéder à la confiscation, la remise, la cessation de comportements paraissant constitutifs de crime ou la protection d'intérêts civils. Elle a également précisé qu'une telle ordonnance ne violait pas l'interdiction d'obliger les fournisseurs de services sur internet à effectuer une surveillance générale d'internet.[34]

2.5 Codes de conduite

L'association des fournisseurs de services internet a conclu au sein de ses membres un code de conduite, qui prévoit que les fournisseurs de services internet ajoutent dans les conditions générales de fourniture de leurs services auprès des utilisateurs ou client une rubrique « bonne conduite », comportant une mention de la conduite correcte sur Internet. De manière générale, cette mention est formulée dans des termes très vagues, sans autre précision, donnant ainsi au fournisseur de services internet la possibilité – du point de vue contractuel – de prendre toute mesure utile, notamment les mesures de blocage, vis-à-vis de leur client.[35] Les conditions de la « conduite correcte sur Internet » et les conséquences concrètes de son absence sont précisées dans les conditions générales des fournisseurs de services internet et dépendent donc de chaque fournisseur.

3. Questions de procédure

Si la Belgique avait mis en place une plateforme centralisée pour les signalements relatifs à internet, accessible sur le site www.ecops.be, celle-ci a été fermée récemment, du fait du trop grand nombre de signalements et de l'impossibilité de traiter l'ensemble de ces signalements dans un délai raisonnable. Les acteurs concernés par ces signalements, le Service Public Fédéral Economie ainsi que les services de police et les organisations actives dans le domaine, se concertent afin de développer un nouveau mécanisme de signalement et de traitement des plaintes relatives à internet. Dans l'intervalle, comme déjà indiqué à la section 2, les utilisateurs sont priés de signaler les contenus illicites qu'ils rencontrent directement auprès des autorités compétentes selon la nature dudit contenu : Service Public Fédéral Economie, services de police, Child Focus et Parquet.

---

34 Cass. 22 octobre 2013, n° P.13.0550.N, disponible sous : http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1 (15.08.2015).

35 ISPA, code de conduite, disponible sous : www.ispa.be

Lorsque les mesures de blocage et/ou de retrait sont ordonnées dans le cadre d'une instruction ou information au pénal en application des dispositions relatives à la saisie des données informatiques prévues aux art. 39bis et 89 CIC, ces mêmes dispositions prévoient que le procureur du Roi ou le juge d'instruction informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées[36]. Cette obligation de communication n'est ni soumise à un délai dans le temps ni prévue à peine de nullité, ce qui peut conduire le procureur du Roi ou le juge d'instruction à attendre un moment opportun dans l'enquête pénale pour communiquer l'information visée au responsable du système informatique. De plus, il n'est pas toujours aisé d'identifier le responsable du système informatique, surtout lorsque celui-ci prend des dispositions pour ne pas pouvoir être identifié.

De plus, les personnes visées par la mesure de saisie peuvent, dans certains circonstances, solliciter la levée desdites mesures. L'art. 28sexies et 61quater CIC prévoient que toute personne lésée par un acte d'information ou d'instruction relatif à ses biens peut en demander la levée au procureur du Roi ou au juge d'instruction. Celui-ci se prononce dans les 15 jours du dépôt de la requête. Le procureur du Roi ou le juge d'instruction peut rejeter la requête « s'il estime que les nécessités de l'information le requièrent, lorsque la levée de l'acte compromet la sauvegarde des droits des parties ou des tiers, lorsque la levée de l'acte présente un danger pour les personnes ou les biens, ou dans les cas où la loi prévoit la restitution ou la confiscation desdits biens ». Il peut aussi accorder une levée totale, partielle ou assortie de conditions. Un appel contre la décision du procureur du Roi ou du juge d'instruction peut être interjeté auprès de la chambre des mises en accusation, au sein du tribunal de première instance. Celle-ci se prononce sur le dossier dans un délai de 15 jours. Il reste alors encore le pourvoi en cassation contre la décision de la chambre des mises en accusation, pour autant qu'un défaut quant au droit puisse être argumenté.

Lorsqu'en revanche, les mesures de blocage et/ou de retrait sont ordonnées par le juge en matière civile, ce sont les recours de droit commun qui s'appliquent. Ainsi, la décision du président du tribunal de première instance ou du tribunal de commerce peut être revue par la Cour d'appel ; le pourvoi en cassation contre la décision de la cour d'appel est également ouvert pour autant qu'un défaut quant au droit puisse être argumenté.

4. Surveillance générale d'Internet

En application de la directive 2000/31/CE et de l'art. XII.20 CDE, les fournisseurs de services internet n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. Ceci n'empêche pas les autorités judiciaires compétentes d'imposer une obligation temporaire de surveillance dans un cas spécifique lorsque cette possibilité est prévue par une loi[37]. En outre, les fournisseurs de services internet ont l'obligation d'informer sans délai les autorités judiciaires ou administratives compétentes des activités illicites alléguées qu'exerceraient les destinataires de leurs services, ou des informations illicites alléguées que ces derniers fourniraient. Ils sont également tenus de communiquer aux autorités judiciaires ou administratives compétentes, à

---

36 Art. 39bis par. 5 CIC et art. 89 CIC.

37 Le code d'instruction criminelle prévoit notamment des mesures de repérage et localisation de télécommunications et d'enregistrement de communications et télécommunications privées (art. 87 et s. CIC).

leur demande, toutes les informations dont ils disposent et utiles pour la recherche et la constatation des infractions commises par leur intermédiaire.[38]

Comme déjà exposé, les acteurs concernés par les signalements de contenus illicites sur internet, le Service Public Fédéral Economie ainsi que les services de police et les organisations actives dans le domaine, se concertent, depuis la fermeture de la plate-forme www.ecops.be, afin de développer un nouveau mécanisme de signalement et de traitement des plaintes relatives à internet. A ce titre, il nous a été indiqué que les possibilités d'une surveillance d'internet par les services de police spécialisés dans le futur n'étaient pas, à ce stade, à exclure.

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

Les conditions dans lesquelles il peut être procédé au blocage ou au retrait d'informations sur internet sont généralement **prévues par la loi**. Au pénal, elles entrent dans le cadre d'une procédure spécifique de **saisie des données informatiques** qui relève de l'autorité du juge d'instruction ou du procureur du Roi. Ce cadre légal a toutefois été critiqué.

La principale critique consiste à dire que les mesures de blocage et/ou retrait ordonnées en application du CIC sont destinées à être des **mesures temporaires ordonnées dans le cadre d'une enquête pénale**, et donc **pas une mesure légale permettant de bloquer les sites internet sans limite de temps**. En laissant la question du blocage et/ou retrait des informations visées par l'enquête aux seules mains du juge d'instruction ou du procureur du Roi, **cette question est retirée du contrôle judiciaire**.

D'autres critiques relèvent qu'il n'était pas adéquat de placer ces mesures dans le cadre de la saisie de données informatique, car elles n'ont rien à faire avec l'établissement de la vérité. Nonobstant, la Cour de Cassation n'a pas jugé nécessaire de sanctionner l'arrêt de la chambre des mises en accusation, estimant, dans son arrêt du 22 octobre 2013, qu'un « ordre émis par le juge d'instruction sur la base de l'article 39bis du Code d'instruction criminelle peut être délivré en vue de la recherche de la vérité, de la confiscation, de la restitution, la cessation d'agissements qui semblent constituer une infraction ou de la sauvegarde des intérêts civils »[39]. Ainsi, des mesures de blocage et de retrait d'un contenu illicite sur internet peuvent être ordonnées tant dans le but d'établir la vérité que de mettre fin à un contenu illicite.

Enfin, en ce qui concerne les obligations d'information des personnes saisies, en ne prévoyant pas un délai pour informer le responsable du système informatique visé par la mesure de blocage et/ou de retrait ni en en sanctionnant le défaut d'information par la nullité, le législateur a octroyé une marge de manœuvre au juge d'instruction ou au procureur du Roi en fonction des besoins de l'enquête, ce qui, d'un point de vue des droits fondamentaux, pourrait poser problème. Ceci dit, il convient de relever qu'en application du titre préliminaire du CIC, une trop grande flexibilité dans le cadre de l'exécution de cette obligation d'information peut conduire à des problèmes de recevabilité des preuves dans le procès pénal, en particulier si «**l'irrégularité commise a entaché la fiabilité de la preuve** » ou « **si l'usage de la preuve est contraire au droit à un procès équitable** » (art. 32 titre préliminaire du CIC).

---

38 Art. XII.20 CDE.

39 Cass. 22 octobre 2013, n° P.13.0550.N, disponible sous : http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1 (15.08.2015).

Au civil, les conditions dans lesquelles le juge peut ordonner aux intermédiaires de cesser les services qui permettent aux tiers de commettre des atteintes, en particulier, aux droits de propriété intellectuelle, sont clairement définies par la loi. Elles apparaissent donc faire preuve d'une prévisibilité suffisante. En particulier, la lecture des travaux préparatoires permet de nuancer le régime légal de responsabilité en la matière s'imposant aux hébergeurs. D'après ceux-ci, en cas de connaissance effective du caractère illicite d'un contenu hébergé, l'hébergeur ne risque d'encourir la mise en cause de sa responsabilité que si le contenu visé est « **manifestement illicite** » et qu'il n'a à son égard pas pris de mesures visant à le rendre inaccessible. Ainsi, en ce qui concerne le contenu qui n'est pas *manifestement* illicite, la *ratio legis* de l'art. XII.19 CDE indique que l'hébergeur n'est pas tenu de le bloquer sauf en exécution d'une obligation ordonnée dans le cadre d'une enquête pénale. S'il n'y est pas tenu, il pourra toutefois décider volontairement de mettre en place une mesure de blocage dudit contenu mais il s'expose alors à d'éventuelles poursuites judiciaires de la personne victime de la mesure de blocage injustifiée. Le dispositif ainsi mis en place apparaît comme assurant une suffisante prévisibilité du système au bénéfice des hébergeurs. Il apparaît comme respectueux de la liberté d'expression, en ce qu'il n'encourage pas les hébergeurs à bloquer trop facilement les sites internet à contenu probablement illicite, par crainte de voir leur responsabilité mise en cause pour ne pas l'avoir fait.

En ce qui concerne les mesures de blocage, une certaine pratique a été relatée qui consiste pour le demandeur de ladite mesure de mettre les fournisseurs d'accès à internet ou les hébergeurs en demeure de bloquer le ou les sites concernés, sous peine de les poursuivre en justice. Une telle démarche avait été adoptée par la *Belgian anti-piracy Federation* (B.A.F.) dans le cadre de l'affaire *The Pirate Bay* : après avoir obtenu une décision judiciaire ordonnant une mesure de blocage dudit site internet par certains fournisseurs d'accès à internet, la BAF a adressé une mise en demeure à plusieurs autres fournisseurs d'accès à internet, afin que ceux-ci se conforment à la décision judiciaire, et ce, alors qu'ils n'y sont pas partie, leur indiquant qu'à défaut, la BAF initierait une procédure judiciaire à leur encontre. Une telle démarche a été vivement critiquée car elle force la prise de mesures de blocage volontaires par les fournisseurs d'accès à internet, et donc en dehors d'une intervention judiciaire censée garantir un équilibre entre l'impact des mesures de blocage sur la liberté d'expression et les atteintes portées aux droits de propriété intellectuelle[40].

On relève enfin qu'il a été proposé que le contenu d'ordre raciste, et plus largement discriminatoire, puisse faire l'objet de mesures de blocage et/ou de retrait d'ordre administratif, par le Centre interfédéral de l'Egalité des chances, et ce, sans intervention judiciaire préalable. Selon cet auteur, un tel dispositif aurait pour avantage de permettre un règlement plus rapide que l'intervention de l'appareil répressif et lent de la machine judiciaire et permettrait de décharger les hébergeurs d'une tâche – celle de décider ce qui est illicite de ce qui ne l'est pas – qui, en la matière, peut s'avérer délicate et qui serait mieux remplie si elle résultait de l'intervention d'une autorité indépendante et spécialisée dans la question, ce que le Centre représente[41].

Stéphanie De Dycker - 15.08.2015

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

---

40 Voir notamment : https://www.eff.org/fr/deeplinks/2011/12/belgian-isps-vs-internet-freedom (15.08.2015).

41 Y. Poullet, La lutte contre le racisme et la xénophobie sur internet, J.T., 2006/23, n°6229, p. 401-412.