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 679-693

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.

SUISSE

Dans la version anglaise, cette partie apparaît dans les pages 679 à 693

1. Sources juridiques

Mis-à-part deux dispositions isolées (l'une dans la loi fédérale sur la sécurité intérieure, l'autre dans l'ordonnance sur les domaines Internet)[1], **la Suisse n'a consacré aucune règle particulière en matière de blocage, de filtrage et de retrait des contenus diffusés sur Internet**. De fait, parlement et gouvernement se reposent sur le droit commun pour régir cette matière nouvelle ; partant, ils laissent le champ libre aux tribunaux pour procéder, le cas échéant, aux adaptations nécessaires. Cette absence de normes spécifiques n'est pas surprenante ; elle traduit en effet le désarroi affiché par un législateur dépassé par un processus de communication complexe, par un progrès technique fulgurant et par une mondialisation incontrôlable. Un exemple parmi d'autres, cette récente déclaration du gouvernement Suisse (le Conseil fédéral) dans son rapport concluant à l'absence de toute nécessité de réglementer les réseaux sociaux: « Comme pour d'autres domaines soumis à un rapide changement, une intervention précipitée – par exemple en édictant des dispositions sur des bases hypothétiques – risque de provoquer des effets indésirables »[2].

Le non interventionniste du législateur a toutefois créé **une grande incertitude quant au cadre juridique qui régit la communication en ligne**. Et ce pour deux raisons : d'une part, comme nous le verrons plus avant, le droit commun n'est pas toujours apte à réguler un mode de communication très différent de la communication classique ; certaines modalités d'Internet requièrent en effet des solutions particulières. D'autre part, les tribunaux ne disent le droit qu'au hasard des cas qui leur sont soumis. Autant dire que la jurisprudence topique est encore ponctuelle et fragmentaire: le Tribunal fédéral, la plus haute instance judiciaire suisse, n'a eu que sporadiquement l'occasion de se prononcer sur les aspects juridiques de la communication en ligne et bien des questions fondamentales demeurent encore non résolues. A commencer par le degré de diligence des fournisseurs de service et l'étendue de leur responsabilité.

Si cette question, qui est au cœur du présent avis de droit, n'a pas encore été spécifiquement abordée par le législateur, c'est aussi parce que la Suisse n'est pas membre de l'Espace économique européen, encore moins de l'Union européenne. Dès lors, elle n'a pas été contrainte de mettre en œuvre les textes communautaires en la matière, à savoir la directive 2000/31 CE sur le commerce électronique et la directive 2002/58 CE sur la vie privée et les communications électroniques. De même, la Suisse n'est pas non plus concernée par la jurisprudence topique de la Cour de justice de l'Union européenne (à commencer par les arrêts L'Oréal[3], Google France[4] et Scarlet Extended[5]).

En la matière qui nous intéresse, c'est donc principalement le droit commun, technologiquement neutre (et de ce fait sensé résister à l'évolution des vecteurs de communication), qui trouve (plus ou moins aisément) application. Ces règles générales, on aura l'occasion d'en présenter la substance dans les sections suivantes. On se contentera à ce stade d'en dresser sommairement la liste :

---

1 Ces dispositions seront présentée plus avant, cf. infra 2.1.5 et 2.1.6.

2 Cadre juridique pour les médias sociaux, Rapport du Conseil fédéral en réponse au postulat Amherd 11.3912 du 29 septembre 2011, Berne 2013, p. 75.

3 Arrêt du 12 juillet 2011, L'Oréal SA et autres contre eBay International AG (C-324/09).

4 Arrêt du 23 mars 2010, Google France SARL et Google Inc. Contre Louis Vuitton Malletier SA (C-236/08 à C-238/08).

5 Arrêt du 24 novembre 2011, Scarlet Extended SA contre Société belge des auteurs, compositeurs et éditeurs SCRL (C-70/10).

- Les actions en prévention ou en cessation de l'atteinte prévues par les règles sur la protection de la personnalité consacrée par le code civil, la loi sur le droit d'auteur, la loi sur la concurrence déloyale ou encore la loi sur la protection des données[6].
- Les diverses possibilités de séquestre ou de confiscation prévues par le droit pénal (code pénal ou code de procédure pénale)[7].
- Les mesures administratives destinées à protéger l'ordre public ou à mettre en œuvre des législations spéciales (loi sur les maisons jeux, loi sur l'alcool, loi sur les produits thérapeutiques, loi sur la sécurité intérieure, etc.)[8].

Si le cadre juridique de la communication en ligne en Suisse peut être qualifié de rudimentaire et de contingent, on doit tout de même relever que, ici ou là, quelques normes spécifiques ont été adoptées pour répondre à des soucis pressants (tels le spamming, la signature électronique, le vote électronique ou encore les casinos virtuels) ou pour implémenter des conventions internationales, directement ou indirectement relatives à Internet, ratifiées par la Suisse. A ce jour, celles-ci sont au nombre de cinq :

- Les deux traités de l'Organisation mondiale de la propriété intellectuelle du 20 décembre 1996 sur le droit d'auteur et sur les interprétations, exécutions et phonogrammes[9].
- La convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité (STCE 185)[10] qui consacre des mesures de droit substantiel et de droit procédural pour lutter contre la multiplication des activités criminelles en ligne[11].
- La convention du 28 janvier 1981 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE 108)[12].
- La convention du 25 octobre 2007 du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE 201)[13].

On relèvera que deux textes importants du Conseil de l'Europe n'ont pas encore été ratifiés par la Suisse : le protocole sur l'expression raciste en ligne (STCE 189)[14] et la convention pour la prévention du terrorisme (STCE 196)[15].

---

6 Cf. infra 2.1.1 à 2.1.4.

7 Cf. infra 2.1.5.

8 Cf. infra 2.1.6.

9 Respectivement Recueil systématique du droit fédéral (ci-après RS) 0.231.151 et 0.231.171.1. Ils ont été transposés en droit suisse par le biais d'une récente révision de la loi fédérale sur le droit d'auteur (Recueil officiel des lois fédérales, ci-après RO 2008 2497).

10 RS 0.311.43.

11 Pour un examen de l'impact de cette convention sur le droit suisse, voir le Message du Conseil fédéral tendant à la ratification de la convention cybercriminalité, Feuille fédérale (ci-après FF) 2010 475ss ; voir aussi Ursula Cassani, Chronique de droit pénal suisse dans le domaine international (2010), Revue Suisse de droit international et européen 2011, p. 515ss.

12 RS 0.235.1. Ce texte a été complété par le protocole additionnel du 8 novembre 2001 concernant les autorités de contrôle et les flux transfrontières de données, aussi ratifié par la Suisse (RS 0.235.11).

13 RS 311.040.

14 Cette lacune a été déplorée par la Commission européenne contre le racisme et l'intolérance (ECRI), laquelle a vivement recommandé à la Suisse de ratifier sans tarder ce protocole additionnel (rapport sur la Suisse 2009, p. 11, chiffre 7). En vain, jusqu'à maintenant.

15 Il est probable que la Suisse ratifiera prochainement cette convention ; une motion dans ce sens est actuellement discutée au Parlement (motion 14.4187).

Enfin, il y a lieu de signaler que de nombreux auteurs, ainsi que de plus en plus de politiciens et de représentants du secteur privé demandent au législateur d'adopter une approche plus proactive afin d'apporter enfin la sécurité juridique nécessaire[16]. Jusqu'ici sans succès : après fait procéder à une analyse approfondie de la situation par des experts internes à l'administration fédérale, le gouvernement suisse a préconisé, fin 2015, de maintenir le statu quo. Selon lui, même si tout n'est pas clair, il n'y a pas lieu de légiférer en matière de responsabilité des fournisseurs de services Internet (FSI)[17], sauf à établir quelques règles spéciales sur blocage et le retrait dans les domaines du droit d'auteur et des jeux en ligne[18]

2. Réglementation applicable

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

2.1.1. La protection de la personnalité

Aux termes de l'art. 28 al. 1 du Code civil (ci-après CC), « Celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe.». Concrètement, cette disposition permet à la victime d'une atteinte à sa personnalité (en particulier atteinte à l'honneur ou à la vie privée) de demander au juge civil de la faire cesser. Sur cette même base, la victime peut le cas échéant demander au juge de prévenir une atteinte à venir, pour autant que celle-ci soit imminente et sérieuse[19]. Pour gagner en efficacité, l'ordre du juge se double, le plus souvent, de la menace de sanctions pénales en cas d'inexécution[20].

A la différence de l'action réparatrice en dommages-intérêts - laquelle ne peut viser qu'une personne qui a commis une faute (dol ou négligence grave) -, **l'action défensive en protection de la personnalité instituée par l'art. 28 al. 1 CC peut être dirigée contre toute personne qui contribue, directement ou indirectement, à la commission de l'atteinte**. Comme le souligne la jurisprudence constante du Tribunal fédéral, « fait partie du cercle des légitimés à défendre dans les actions défensives, quiconque "participe" à l'atteinte. Cette formulation vise non seulement l'auteur originaire de l'atteinte, mais aussi toute personne dont la collaboration cause, permet ou favorise celle-ci, sans qu'il soit nécessaire qu'elle ait commis une faute (…). La seule collaboration porte (objectivement) atteinte, même si son auteur ne s'en rend pas compte ou ne peut même pas le savoir (…). En d'autres termes, peut ainsi être concerné celui qui, sans être l'auteur des propos litigieux ou même en connaître le contenu ou l'auteur, contribue à leur transmission. Le lésé peut agir contre quiconque a objectivement joué, que ce soit de près ou de loin, un rôle - fût-il secondaire - dans la création ou le développement de l'atteinte »[21]. Sur la base de cette interprétation large de la notion de « participation à l'atteinte », le Tribunal fédéral a notamment reconnu que dans le domaine de la presse classique non seulement l'auteur d'un article attentatoire à la personnalité

---

16 Pour plus de détails, voir Bertil Cottier, Le droit "suisse" du cyberespace ou le retour en force de l'insécurité juridique et de l'illégitimité, Revue de droit suisse 2015 II, p.226s.

17 Rapport du Conseil fédéral du 11 Décembre 2015, Berne 2015, p. 97s.

18 Cf. infra respectivement 2.1.3 in fine et 2.2.2 in fine, ainsi que 2.1.6.

19 Arrêt du Tribunal fédéral 128 III 100.

20 En application de l'art. 292 du code pénal qui sanctionne de l'amende celui ne se soumet pas à une décision d'une autorité.

21 Arrêt du Tribunal fédéral du 14 janvier 2014 (cons. 6), 5A_792/2011 ; dans le même sens arrêt du 6 mai 2015, 5A_658/2014 (cons. 4.2). Voir aussi Message du Conseil fédéral du 5 mai 1982 concernant la révision du code civil suisse [Protection de la personnalité: art. 28 CC et 49 CO], FF 1982 II 681.

peut être attrait en justice sur la base de l'art. 28 al. 1 CC, mais aussi l'éditeur, l'imprimeur ou encore l'exploitant d'un kiosque qui vend le journal litigieux[22].
On notera encore que **l'art. 28 CC ne prévoit pas d'ordre de priorité ; c'est au lésé de choisir librement contre qui il entend diriger son action défensive**[23].

A ce jour, le Tribunal fédéral n'a pas encore eu à se prononcer sur des cas impliquant des fournisseurs d'accès Internet (ci-après FAI). Quant à la doctrine, elle est divisée. Certains auteurs sont d'avis que les FAI peuvent être astreints à bloquer l'adresse IP de sites contenant des données attentatoires à la personnalité diffusés sur Internet, car, même s'ils ne sont pas à l'origine des communications attentatoires, ils participent à leur diffusion sur le réseau des réseaux. Reste que le blocage ne doit cibler que les seuls contenus attentatoires et ne pas empêcher l'accès aux autres communications qui elles seraient licites (interdiction de l'*overblocking*) [24]. D'autres auteurs doutent en revanche de la possibilité d'attraire les FAI, faute de lien de causalité adéquate entre leur participation et l'atteinte[25].

2.1.2. La protection des données

La loi fédérale sur la protection des données (ci-après LPD[26]), qui met en œuvre la convention 108 du Conseil de l'Europe mentionnée plus haut (cf. supra 1), consacre également des moyens de droit pour empêcher ou prévenir un traitement illicite de données personnelles. Dans la mesure où le traitement litigieux est effectué par une personne physique ou morale de droit privé[27], ces moyens sont identiques à ceux qui peuvent être mis en œuvre pour protéger la personnalité; en effet l'art. 15 LPD renvoie expressément aux actions défensives consacrées par l'art. 28 CC dont il vient d'être question dans la section précédente (cf. supra 2.1.1) [28].

En conséquence, les FAI peuvent se voir contraints par le juge civil de bloquer l'accès à des informations résultant de traitements de données illicites, même s'ils n'ont commis aucune faute.

2.1.3. La propriété intellectuelle

Tant la loi fédérale sur le droit d'auteur (ci-après LDA[29]) que la loi fédérale sur la protection des marques et des indications de provenance (ci-après LPM[30]) offrent la possibilité de requérir

---

22 Arrêt du Tribunal fédéral 131 III 26.

23 « Le principe de la proportionnalité, qui doit être respecté dans les actions défensives de l'art. 28a CC et dans les mesures provisionnelles de l'art. 28c CC (…), ne s'oppose pas à ce qu'une mesure soit prononcée à l'encontre du seul protagoniste, même secondaire, auquel le demandeur a décidé de s'en prendre », arrêt du Tribunal fédéral du 12 septembre 2002 (5P.254/2002), consid. 2.5.

24 Rosenthal David, Internet-Provider-Haftung – ein Sonderfall? in: Peter Jung (Ed.), Aktuelle Entwicklungen im Haftungsrecht, Bern/Zürich/Basel/Genf, 2007, p. 158.

25 Le gouvernement suisse s'est rallié à ce point de vue dans son rapport de décembre 2015 (cf. supra note 17), p. 32.

26 RS 235.1.

27 Les voies de droit à l'encontre des traitements opérés par des autorités publiques fédérales ou cantonales sont régies par des dispositions relevant respectivement du droit administratif fédéral (art.25 LPD) ou du droit administratif du canton concerné. Leur présentation dépasserait le cadre de cette étude.

28 Art. 15 al. 1 LPD : « Les actions concernant la protection de la personnalité sont régies par les art. 28, 28a et 28l du code civil. ». Ce renvoi vise aussi les mesures provisionnelles, Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, p. 592 ad 1826.

29 RS 231.1

l'intervention du juge pour faire cesser (le cas échéant pour prévenir) une violation du droit d'auteur ou du droit des marques (voir respectivement les art. 62 al. 1 LDA et art. 55 LPM). Ces actions sont en tous points semblables aux actions défensives en protection de la personnalité consacrées par le code civil (supra 2.1.1). En particulier, le cercle des personnes qui ont qualité pour défendre est tout aussi large, même si contrairement à l'art. 28 CC le libellé des deux dispositions ne mentionne pas expressément que la légitimation passive appartient à toute personne physique ou morale qui « participe » à la violation[31].

Il s'ensuit que les FAI pourraient être astreints par le juge civil à bloquer l'accès à des sites violant le droit d'auteur ou le droit des marques[32]. Le conditionnel est de rigueur vu l'absence de jurisprudence topique à l'heure actuelle ; cette absence s'explique avant tout par le fait que les ayants-droits ont jusqu'à maintenant dirigé leurs actions directement contre ceux qui violaient la propriété intellectuelle[33].

Un changement pourrait prochainement se produire, suite à la présentation par le gouvernement au parlement d'un projet de modernisation de la loi fédérale sur le droit d'auteur au décembre 2015. Ce projet de loi prévoit expressément une procédure de blocage des contenus portant atteinte au droit d'auteur (voir article 66d)[34]. On notera que le gouvernement insiste dans son rapport explicatif sur l'impérieuse nécessité d'éviter *l'overblocking* et de n'intervenir au niveau des FAI qu'en deuxième temps (à savoir seulement si une intervention au niveau des hébergeurs s'avère dénuée de succès)[35].

2.1.4. La concurrence déloyale

La loi fédérale contre la concurrence déloyale (ci-après LCD[36]) entend lutter contre les pratiques commerciales trompeuses, abusives ou de mauvaise foi ; dans cette perspective, elle s'en prend notamment au dénigrement de concurrent, aux affirmations mensongères sur la qualité d'un produit, à la publicité comparative blessante, aux indications de prix fallacieuses ou aux pourriels commerciaux (voir l'art. 3 LCD pour une liste, non exhaustive[37], des différentes pratiques litigieuses).

L'art. 9 LCD institue des actions défensives destinées à empêcher ou à faire cesser une violation de la LCD[38]. Ces actions peuvent être intentées par un concurrent ou par un consommateur (le échéant les

---

30 RS 232.11

31 Voir pour le droit d'auteur Denis Barrelet et Willy Egloff, Le nouveau droit d'auteur, Berne 2008, 3ème éd., p. 341 ad 5 et Ralph Schlosser, commentaire de l'art. 62, in : Jacques de Werra et Philippe Gilliéron, Propriété intellectuelle, Berne 2013, p. 496 ad 5 ; pour le doit des marques, Ivan Cherpillod, Le droit suisse des marques, Lausanne 2007, p. 241 et Ralph Schlosser, commentaire de l'art. 55, in : Jacques de Werra et Philippe Gilliéron, Propriété intellectuelle, Berne 2013, p. 1121 ad 4.

32 Rapport final du Groupe de travail sur le droit d'auteur AGUR12 du 28 novembre 2013 (ci-après Rapport AGUR12), Berne, p. 49 ad. 3.14, ainsi que p. 78.

33 Ibidem p. 36.

34 Voir le Rapport explicatif du Conseil fédéral du 11 décembre 2015, p 72.

35 Ibidem, p. 73

36 RS 241.

37 A son art. 2, la LCD contient en effet une clause générale dont la teneur est la suivante : « Est déloyal et illicite tout comportement ou pratique commercial qui est trompeur ou qui contrevient de toute autre manière aux règles de la bonne foi et qui influe sur les rapports entre concurrents ou entre fournisseurs et clients».

38 « Celui qui, par un acte de concurrence déloyale, subit une atteinte dans sa clientèle, son crédit ou sa réputation professionnelle, ses affaires ou ses intérêts économiques en général ou celui qui en est menacé, peut demander au juge a.de l'interdire, si elle est imminente; b.de la faire cesser, si elle dure encore ».

organisations professionnelles ou les associations de défense des consommateurs peuvent les relayer), ou encore exceptionnellement par la Confédération[39]. La légitimation passive, autrefois limitée aux seuls opérateurs économiques, est aujourd'hui beaucoup plus large et englobe toute personne qui, de près ou de loin, contribue à l'atteinte, y compris les médias[40].

Dès lors, les FAI pourraient eux aussi être astreints par le juge civil à bloquer l'accès à des sites violant le droit de la concurrence déloyale.

2.1.5. Les mesures relevant du droit pénal

Celles-ci sont de deux ordres : le blocage préventif et le blocage définitif, accessoire à la peine. Dans les deux cas, la mesure est controversée, ne reposant sur aucune disposition légale expresse, mais sur l'interprétation extensive des dispositions de la législation pénale procédurale ou substantielle qui visent le séquestre (art. 263 du code de procédure pénale, ci-après CPP[41]), respectivement la confiscation d'objets dangereux (art. 69 du code pénal, ci-après CP[42])[43]. Etant donné que le libellé de ces deux dispositions vise expressément des *objets*, autrement dit des biens corporels matériels, certains auteurs leur dénient la qualité de base légale permettant d'ordonner aux FAI de bloquer l'accès à des sites illicites ; faute de fondement légal, pareille restriction à la liberté de l'information serait anticonstitutionnelle[44]. **Cette controverse sur la constitutionnalité de la mesure de blocage semble avoir inhibé les autorités de poursuite pénale qui ont rarement prononcé cette mesure**.

Les quelques cas en la matière proviennent, pour la plupart, du canton de Vaud. En 2009 le Tribunal cantonal a validé une ordonnance de blocage de onze adresses IP qui donnaient accès à des sites diffamatoires, hébergés à l'étranger pour contourner délibérément le droit suisse ; l'ordre de blocage était dirigé à l'encontre de tous les FAI basés en Suisse[45] . Les juges ont estimé que pareille mesure était constitutionnelle en vertu du raisonnement « a maiore minus » : dès lors que les autorités de poursuite pénale sont en droit de saisir physiquement les serveurs des FAI pour empêcher l'accès aux sites incriminés, elles sont a fortiori en droit d'ordonner la mesure moins contraignante qu'est le blocage[46]. Dans un arrêt postérieur concernant un hébergeur, cette même instance a estimé que l'assimilation du blocage à un séquestre se justifie d'autant plus que cette mesure répond à l'esprit de la loi, laquelle doit être interprétée de manière évolutive en tenant compte du progrès de la technique : « Le blocage provisoire, puis le cas échéant définitif, de l'accès à un blog contenant des

---

39 La Confédération, représentée par le Secrétariat d'Etat à l'économie, peut intervenir si des intérêts collectifs sont menacés ou subissent une atteinte (art. 10 al. 3 LCD).

40 Arrêt du Tribunal fédéral 117 IV 193 ; voir aussi Philippe Spitz, commentaire de l'article 9, in : Peter Jung et Philippe Spitz, Bundesgesetz gegen Unlauter Wettbewerb, Berne 2010, p. 695.

41 RS 312.0.

42 RS 311.0.

43 « Des objets et des valeurs patrimoniales appartenant au prévenu ou à des tiers peuvent être mis sous séquestre, lorsqu'il est probable: a. qu'ils seront utilisés comme moyens de preuves; b. qu'ils seront utilisés pour garantir le paiement des frais de procédure, des peines pécuniaires, des amendes et des indemnités; c. qu'ils devront être restitués au lésé; d. qu'ils devront être confisqués ».

44 En particulier, Christian Schwarzenegger, Sperrverfügungen gegen Access-Provider - über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Oliver Arter et Jörg Florian (éd.), Internet-Recht und Electronic Commerce Law, Bern 2003, p. 249ss. Contra Laurent Moreillon et Aude Parein-Reymond, Code de procédure pénale, Bâle 2013, p 752 ad 9.

45 Arrêt du Tribunal d'accusation du Tribunal cantonal du canton de Vaud du 26 mars 2009.

46 Ce raisonnement « a maiore minus » avait été développé pour la première fois en 2005, par le Tribunal pénal fédéral dans une affaire relative au blocage de sites internet ayant servi à la publicité et à la vente illicite de produits thérapeutiques et médicaux (arrêt du Tribunal pénal fédéral du 16 février 2005, BV 2004.26).

propos diffamatoires ne diffère pas fondamentalement du séquestre, puis le cas échéant de la confiscation et de la destruction d'un stock d'imprimés comprenant des propos diffamatoires. On ne voit donc pas ce qui justifierait de traiter la première hypothèse autrement que la seconde, dans laquelle un séquestre en vue de confiscation est indéniablement possible »[47].

Si le gouvernement suisse semble soutenir ce point de vue[48], une prise de position claire du Tribunal fédéral se fait encore attendre. Certes, la première affaire mentionnée dans le paragraphe précédent fit l'objet d'un recours ; mais les juges suprêmes se dispensèrent d'examiner la légalité du blocage, le recourant, l'un des FAI visé par l'injonction litigieuse, ayant fait appel hors-délais[49]. En mars 2015, le Tribunal fédéral, saisi d'un recours contre le blocage par la justice pénale valaisanne de deux sites contenant des accusations diffamatoires, laissa la question ouverte, se bornant à renvoyer l'affaire à l'instance inférieure pour qu'elle examine si les conditions d'un blocage étaient réunies (notamment celle de la gravité des accusations formulées) et, si tel était le cas, s'il est possible, eu égard au principe de proportionnalité, de limiter le blocage aux seuls propos litigieux[50].

Cela dit, on relèvera qu'en matière de lutte contre la cybercriminalité, il est possible d'ordonner administrativement le blocage du nom de domaine d'un site malveillant. L'ordonnance sur les domaines Internet du 5 novembre 2014 (ci-après ODI[51]) autorise en effet le blocage par le « registre »[52] d'un nom de domaine de son ressort, en cas de soupçons sérieux que le site y afférant est utilisé pour accéder, illicitement, à des données « critiques » de tiers (hameçonnage) ou pour diffuser des logiciels malveillants (maliciels)[53] ; la mesure doit être requise par un service de lutte contre la cybercriminalité reconnu par l'Office fédéral de la communication. Le blocage a une validité de 30 jours ; passé ce délai, il doit être confirmé par l'Office fédéral de la police (art. 15 ODI). La confirmation a valeur de décision administrative, susceptible d'un recours administratif suivant les règles usuelles en la matière[54].

2.1.6. Les mesures relevant du droit administratif (sécurité nationale, bonnes mœurs etc.)

Faute de toute jurisprudence topique, il paraît douteux que les autorités administratives soient en droit de contraindre les FAI à bloquer des sites internet sans pouvoir se fonder sur une base légale spécifique.

---

47 Arrêt du Tribunal cantonal vaudois du 18 juin 2014, forumpoenale 3/2015, p. 149s, en particulier cons.4d.

48 Voir la réponse du Conseil fédéral à la question Schwaab (12.1128), du 13 février 2013 : « Si un contenu interdit par la loi devait avoir un lien quelconque avec la Suisse, l'autorité de poursuite pénale peut, par le biais d'une décision, ordonner la mise sous séquestre (art. 263 CPP) et son blocage ou sa suppression, pour autant que les contenus servent de moyens de preuve dans la procédure pénale ou soient confisqués d'une autre manière. ».

49 Arrêt du Tribunal fédéral du 11 octobre 2009 (1B_242/2009).

50 Arrêt du Tribunal fédéral du 19 mars 2015 (1B 294/2014), cons. 4.

51 RS 784.104.2. Ce texte se fonde sur une délégation de compétences du Parlement au Conseil fédéral contenue à l'art. 48a de la loi fédérale sur les télécommunications (RS 784.10), délégation qui a la teneur suivante : « Le Conseil fédéral peut édicter des prescriptions techniques et administratives sur la sécurité et la disponibilité des infrastructures et des services de télécommunication ».

52 L'expression, définie dans l'annexe à l'ODI, vise l'« entité chargée de l'organisation, de l'administration et de la gestion centrales d'un domaine de premier niveau, ainsi que de l'attribution et de la révocation des droits d'utilisation sur les noms de domaine qui lui sont subordonnés ».

53 RS 784.104.2.

54 Voir les articles 44 et ss. de la loi fédérale sur la procédure administrative (RS 172.021).

Reste qu'à ce jour une seule norme envisage expressément le blocage administratif d'adresses IP: l'art. 13 e, al. 5 de la loi fédérale sur la sécurité intérieure (ci-après LMSI[55]). Et encore, l'injonction de blocage est privée d'effet contraignant. En effet, l'Office fédéral de la police ne peut que « recommander » aux FAI de bloquer l'accès à des sites qui contiendraient du matériel de propagande[56]. La démarche a été entreprise notamment pour obtenir le blocage de l'accès à des sites Internet utilisés pour diffuser depuis l'étranger de la propagande djihadiste[57].

Le dit art. 13 LMSI codifie d'ailleurs la pratique administrative générale en matière de blocage : le dialogue avec les FAI est privilégié. L'objectif est d'inciter des FAI, réticents à toute instrumentalisation, à coopérer volontairement ; avec plus ou moins de succès selon les domaines : la lutte contre la pédopornographie est certainement celui où cette coopération fonctionne le mieux[58].

Emblématique de cette approche prudente et conciliante des autorités administratives est le cas de la Commission fédérale des jeux, laquelle veut depuis longtemps empêcher l'accès des internautes suisses à des casinos en ligne opérant depuis l'étranger et offrant des prestations interdites en Suisse. En l'absence d'une base légale l'habilitant expressément d'exiger des FAI qu'ils bloquent l'accès à ces sites[59], elle a entamé des discussions à cet effet avec les principaux FAI du pays. Ces pourparlers s'avérant infructueux, le gouvernement a décidé, dans le cadre de la révision totale de la loi fédérale sur les maisons de jeux actuellement en cours, d'insérer une disposition spécifique donnant compétence à la Commission fédérale des jeux d'ordonner le blocage de sites de jeux situés à l'étranger. Une liste noire des sites litigieux sera ainsi régulièrement tenue à jour, transmise aux FAI pour blocage, puis officiellement publiée[60].

Au demeurant, il convient de noter que sur la base de la clause générale de police (art. 36 al. 1 (3) de la constitution fédérale), les autorités peuvent intervenir sans base légale à l'encontre de quiconque menace la sécurité publique. La menace doit toutefois être imminente, sérieuse et grave[61] ; en outre, par respect pour le principe de proportionnalité consacré par l'alinéa 3 de ce même article 36 de la

---

55 RS 120.

56 Aux termes de l'13 e al. 1 LMSI, cette expression vise les sites « dont le contenu incite, d'une manière concrète et sérieuse, à faire usage de la violence contre des personnes ou des objets ».

57 Voir la réponse du Conseil fédéral du 8 mai 2015 à la question van Singer (15.1027, Quelles actions préventives le Conseil fédéral entend-il mener pour éviter l'implantation d'extrémismes violents en Suisse?).

58 Cf. infra 2.2.5

59 Absence que la Commission fédérale des jeux a toujours déploré, cf. son Rapport annuel 2014, p. 19.

60 Art. 84 du-projet de loi sur les jeux d'argent (transmis au Parlement en octobre 2015, FF 2015 7769) : « 1 L'accès à une offre de jeux d'argent en ligne doit être bloqué lorsque celle-ci n'est pas autorisée en Suisse. 2 Seul est bloqué l'accès aux offres de jeux accessibles en Suisse dont l'exploitant a son siège ou son domicile à l'étranger ou qui dissimule son siège. 3 La CFMJ et l'autorité intercantonale tiennent chacune une liste des offres de jeux relevant de leur compétence dont l'accès est bloqué et actualisent cette liste régulièrement. 4 Les fournisseurs de services de télécommunication bloquent l'accès aux offres de jeux figurant dans l'une ou l'autre de ces listes. »
5 La CFMJ et l'autorité intercantonale peuvent autoriser un utilisateur à accéder aux offres de jeux bloquées à des fins de surveillance ou de recherche.».

61 L'art. 36 de la Constitution fédérale dispose que « Toute restriction d'un droit fondamental doit être fondée sur une base légale. (…) Les cas de danger sérieux, direct et imminent sont réservés. ». Pour un cas pratique, voir l'arrêt du Tribunal fédéral 126 I 118 (soins médicaux imposés à un patient en l'absence de base légale formelle).

constitution[62], il ne doit pas exister de moyen moins intrusif pour parer au danger[63]. A notre connaissance, aucun ordre de blocage n'a encore été émis sur la base de la clause générale de police.

2.2. Retrait de contenu illégal

2.2.1. La protection de la personnalité et la protection des données

Les actions défensives fondées sur l'art. 28 CC, soit directement (protection de la personnalité, cf. supra 2.1.1) soit par l'effet d'un renvoi (protection des données, cf. 2.1.4) permettent également d'obtenir le retrait de contenus illicites. Ces actions pouvant être dirigées contre toute personne qui « participe » à l'atteinte, le cercle des personnes qui ont qualité pour défendre s'étend à l'hébergeur ou aux exploitants de plateformes sociales.

Ce point de vue a été confirmé par le Tribunal fédéral, lequel a ordonné en 2011 le retrait, d'un blog exploité par un quotidien genevois, de contributions attentatoires à l'honneur émanant d'un tiers[64]. Dans leurs considérants, les juges ont clairement rejeté l'argumentation de la partie défenderesse (le journal) qui exigeait que la victime s'en prenne directement à l'auteur des propos litigieux et non à l'intermédiaire qui ne fait que procéder à leur diffusion : « De même, elle (la défenderesse) tombe à faux lorsqu'elle se prévaut du fait qu'il lui serait impossible de contrôler constamment le contenu de tous les blogs hébergés. Ces éléments, en particulier le devoir d'attention et de contrôle requis de chacun, ressortissent à la question de la faute qui n'est pas pertinente dans le cadre des actions défensives du droit de la personnalité »[65].

L'action défensive peut également être dirigée contre le fournisseur de liens. Celui-ci peut être contraint de supprimer un lien vers un site attentatoire à la personnalité, pour autant qu'il s'agisse d'un lien profond, qui donne directement accès aux informations litigieuses ; un lien qui pointerait généralement sur le portail d'un site où se trouverait, entre autres des informations attentatoires, n'est pas suffisant[66].

2.2.2. Propriété intellectuelle et concurrence déloyale.

Les actions défensives ressortissant tant au droit d'auteur, au droit des marques qu'à la concurrence déloyale sont également applicables à l'encontre de l'hébergeur ou de l'exploitant d'un réseau social. Et ce, du fait de l'étendue très large des personnes qui ont qualité pour défendre à ces actions[67]. En l'absence de jurisprudence topique, nous renvoyons à ce qui a été dit sous chiffre 2.1.3 et 2.1.4.

Cela dit, il y lieu de préciser que le projet de modernisation de la loi fédérale sur le droit d'auteur de décembre 2015, déjà mentionné (cf. supra 2.1.3 in fine), introduit une procédure de notification et de retrait pour les contenus portant atteinte au droit d'auteur (voir article 66b)[68] . En substance, l'hébergeur qui apprend du titulaire des droits que, sans son consentement, il donne accès à des

---

62 « Toute restriction d'un droit fondamental doit être proportionnée au but visé ».

63 Pour plus de détails, voir Regina Kiener et Walter Kälin, Grundrechte, Berne 2013, p. 110s.

64 Arrêt du Tribunal fédéral du 14 janvier 2013 (5A_792/2011).

65 Voir aussi arrêt du Tribunal fédéral du 28 octobre 2003 (5P.308/2003), retrait d'articles de journaux diffamatoires du site personnel d'un tiers.

66 Arrêt du Tribunal fédéral du 4 mai 2015 (5A_658/2014), cons. 4.2.

67 Voir en particulier Ralph Schlosser, commentaire de l'art. 62, in : Jacques de Werra et Philippe Gilliéron, Propriété intellectuelle, Berne 2013, p. 497 ad 6 ; l'auteur mentionne expressément le cas de l'hébergeur d'un site reproduisant des œuvres en violation du droit d'auteur.

68 Voir le Rapport explicatif du Conseil fédéral du 11 décembre 2015, p 71.

œuvres protégées, doit les retirer. Ce faisant, l'hébergeur informe du retrait le fournisseur des contenus litigieux, lequel peut faire opposition. En cas d'opposition, l'hébergeur doit rétablir l'accès ; il appartient alors au titulaire des droits de faire valoir ses prétentions devant le juge civil.

2.2.3. Le droit pénal

L'autorité de poursuite pénale peut ordonner la suppression de contenus pénalement répréhensibles soit à titre préventif par le biais du séquestre, soit à titre définitif par le biais d'une mesure de confiscation.

Cette suppression se fonde sur les dispositions du code de procédure pénale et du code pénal sur le séquestre et la confiscation d'objets matériels (cf. supra 2.1.5). On rappellera que cette interprétation évolutive de la loi est le fait d'instances judiciaires inférieures ; sa confirmation de la part du Tribunal fédéral est encore attendue, ce d'autant qu'une partie de la doctrine est d'avis qu'une base légale expresse doit être adoptée.

2.2.4. Le droit administratif

La seule habilitation spécifique d'ordonner le retrait de contenus illicites est contenue dans loi sur la sécurité intérieure. L'Office fédéral de la police, peut, après avoir consulté le Service de renseignement de la Confédération, ordonner la suppression d'un site hébergé en Suisse qui contiendrait du matériel de propagande (art. 13e litt. al.5 LMSI). Contrairement à ce qui prévaut à l'encontre des FAI (cf. supra 2.1.6), l'injonction à l'encontre des hébergeurs ou des exploitants de plateformes est de nature contraignante (et non simplement volontaire).

Vu la proximité physique des hébergeurs avec les contenus litigieux, la question du droit ou non à faire supprimer des contenus illicites en dehors de toute habilitation légale spécifique est moins controversée que celle du droit de faire bloquer. Dès lors, certaines autorités administratives n'ont pas hésité à ordonner des retraits sur la simple base d'autorisations générales de s'en prendre à des communications illicites. Ainsi, par exemple, la Régie fédérale des alcools a obtenu la suppression de publicités en ligne contraire à la loi sur l'alcool[69] ; de même, Swissmedic, l'organe national de contrôle des médicaments, est intervenu à plusieurs reprises contre des hébergeurs qui contribuaient à la diffusion de publicités interdites pour des médicaments[70].

2.2.5. Autorégulation

Sur une base purement volontaire, la SIMSA (*Swiss Internet Industry Association*), l'association faitière des fournisseurs suisses de services Internet[71], a mis en vigueur, le 1er février 2013, son *Code de conduite Hébergement* (ci-après CCH). L'objectif de ce texte est de pallier l'absence de toute réglementation de droit dur sur la responsabilité des hébergeurs en matière civile et pénale, en mettant sur pied une procédure de notification et de retrait de contenu illicite. Sur le modèle de la

---

69 Voir Cadre juridique pour les médias sociaux**,** Rapport du Conseil fédéral en réponse au postulat Amherd 11.3912 du 29 septembre 2011, Berne 2013, p.65 ad 5.4.1.

70 Voir notamment l'arrêt du Tribunal pénal fédéral du 16 février 2005, BV 2004.26 ; voir aussi Valérie Junod, Publicité pour les médicaments: La santé publique l'emporte sur la liberté d'expression, medialex 2010, p. 10, note 24.

71 Les exploitants de plateformes Internet ne sont pas membres de la SIMSA et par conséquent ne sont pas concernés par ces mesures d'auto-discipline.

procédure de « notice and take down », consacrée depuis plus d'une dizaine d'années par le droit américain[72], les membres de la SIMSA se réservent, dans les conditions générales qui les lient à leurs clients, le droit de supprimer les contenus illicites portés à leur connaissance.

Pour être admissible, la notification doit contenir au moins les indications suivantes: (a) nom et adresse de l'auteur de la notification; (b) justification de la manière dont la personne est concernée par le contenu (sauf délits poursuivis d'office comme la pédopornographie); (c) adresse URL de la page ou de la rubrique litigieuse; (d) désignation précise des contenus illicites; (e) justification du caractère illicite des contenus[73]. Si la notification reçue remplit ces conditions et s'il est très probable[74] qu'elle concerne des contenus illicites l'hébergeur peut bloquer l'accès au site[75]. Le client est informé du blocage et des raisons qui l'ont motivé[76]. On notera enfin que le non-respect du code Hébergement ne conduit qu'à une sanction symbolique : l'hébergeur ne pourra plus afficher le label de qualité *Swiss quality hosting*.

3. Questions de procédure

3.1. Les actions défensives fondées sur le droit civil

Ces actions sont régies par le code de procédure civile (ci-après CPC[77]). Il s'en suit qu'elles ne peuvent être ordonnées que par un juge qui statue dans le cadre d'un procès contradictoire ; la décision du juge peut ensuite faire l'objet d'un recours à une instance supérieure. On signalera que contrairement à nombre de pays européens, l'autorité nationale de protection des données (en Suisse, le Préposé fédéral à la protection des données et à la transparence) ne dispose d'aucun pouvoir de décision. Si des moyens défensifs sont envisagés, la victime doit s'adresser au juge civil, seul compétent en la matière (15 LPD).

On relèvera encore que le blocage peut être ordonné à titre provisionnel. Aux termes des art. 261ss CPC, le juge peut en effet prendre des mesures, urgentes mais temporaires, contre les personnes qui contribuent à l'atteinte. Ces mesures provisionnelles sont cependant soumises à des conditions strictes pour éviter les abus : en particulier il doit apparaître vraisemblable que la victime subira un préjudice difficilement réparable. Les mesures provisionnelles pouvant s'assimiler à une forme de censure préalable qui menacerait la liberté de l'information, le législateur en a limité le recours à l'encontre des médias *à caractère périodique*, tels (mais pas exclusivement) la presse, la radio et la télévision: le juge n'est dans ce cas habilité à ordonner une mesure provisionnelle (par exemple une interdiction immédiate de diffuser une émission) que si le préjudice encouru par la victime est *particulièrement grave* et si l'intérêt à la publication ou à la diffusion n'est pas évident (art. 266 CPC). S'il fait peu de doutes qu'un FAI ou un hébergeur ne saurait être considéré comme un média, car ni l'un ni l'autre n'exercent de contrôle éditorial sur l'information, il n'en va pas de même des opérateurs de plateforme en ligne. Le Tribunal fédéral a toutefois refusé le bénéfice de l'art. 266 CPC

---

72 Voir l'art. 512 (c) du Digital Millenium Act.

73 Chiffre 4.3 CCH.

74 « Le point de vue d'une personne non spécialisée en droit est suffisant pour l'évaluation de la notification et la prise de décision en matière de blocage et de dénonciation. » (chiffre 7.3 CCH).

75 Chiffre 7.1. CCH.

76 Le blocage non seulement est prévu par le CCH, mais en plus est expressément mentionné dans le contrat qui lie l'hébergeur et son client (e.g. la procédure de blocage est décrite dans les conditions générales annexées au contrat). En revanche, ni le CCH, ni les dispositions contractuelles applicables ne font référence à la liberté d'expression et à ses conditions de restrictions.

77 RS 272.

à un exploitant d'un réseau social[78]. On relèvera encore qu'en règle générale, le juge entend le défendeur avant d'ordonner les mesures provisionnelles ; il peut cependant se passer de l'auditionner, « en cas d'urgence particulière, notamment s'il y a risque d'entrave à leur exécution, » (mesures dites superprovisionnelles, art. 265 CPC).

3.2. Les mesures de droit pénal

Le blocage (ou le retrait) provisoire (dont on rappellera qu'il est controversé, car il se base sur une interprétation évolutive de l'institution procédurale du séquestre, art. 263 CPP[79]) est une mesure de contrainte qui est ordonnée par l'autorité qui conduit l'enquête (le Ministère public) ; la personne visée par la mesure n'est pas entendue au préalable. L'ordonnance de séquestre peut faire l'objet d'un recours à un tribunal (le Tribunal des mesures de contraintes) conformément aux art. 393ss CPP. On soulignera encore que le séquestre est soumis aux principes généraux régissant les mesures de contraintes ; aux termes de l'art. 197 du CPP, celles-ci ne peuvent être prises qu'aux conditions suivantes: « a) elles sont prévues par la loi, b) des soupçons suffisants laissent présumer une infraction, c) les buts poursuivis ne peuvent pas être atteints par des mesures moins sévères et d) elles apparaissent justifiées au regard de la gravité de l'infraction. ».

Tout aussi controversé que le blocage provisoire (il se fonde sur une interprétation, elle aussi évolutive, de l'institution de la confiscation), le blocage (ou le retrait) définitif est une mesure accessoire à la peine, prononcée par l'instance de jugement. Pour autant que l'objet confisqué ait servi à commettre l'infraction, la confiscation peut être prononcée à l'encontre de tiers qui n'ont pas été partie au procès[80] (ce qui est l'hypothèse la plus courante en cas de blocage définitif visant un FAI ou un hébergeur). Par respect du droit à être entendu, le juge doit, dans ce cas, interpeller le destinataire de la mesure[81]. Le blocage définitif peut faire l'objet d'un recours à l'instance pénale supérieure.

3.3. Les mesures de droit administratif

Dans les (rares) cas où le blocage ou le retrait sont le fait d'une autorité administrative, ils sont ordonnés en la forme d'une décision administrative[82], soumise aux conditions formelles et matérielles posée par la loi de procédure administrative (fédérale, ou, le cas échéant, cantonale), et susceptible de recours. En particulier, le destinataire de la mesure a le droit d'être entendu. A cet égard on notera que la loi sur la sécurité intérieure prévoit expressément que les décisions de suppression de matériel de propagande (cf. supra 2.2.4) sont régies par la loi sur la procédure administrative fédérale (art. 13e al. 2 in fine LMSI).

---

78 Arrêt du Tribunal fédéral du 4 mai 2011 (5A 790/2010 cons. 5.2), refus de considérer un réseau social comme un média périodique ; le Tribunal fédéral n'a cependant pas expliqué en quoi un réseau social n'est pas un média périodique. Voir aussi l'arrêt du Tribunal fédéral du 10 octobre 2013 (1C_335/2013), bloggeur interdit de filmer les séances publiques d'une assemblée de commune, faute de compétence journalistique.

79 Cf. supra 2.1.5.

80 Madeleine Hirsig-Vouilloz, commentaire à l'art. 69 CP, in : Robert Roth et Laurent Moreillon, Code pénal I, Bâle 2009, p. 722 ad 36.

81 Madeleine Hirsig-Vouilloz, ibidem, p. 737 ad 43 et la jurisprudence citée en note 100. Si la confiscation a lieu indépendamment d'une procédure pénale, l'ordonnance de confiscation sera rendue par le Ministère public qui doit donner à la personne concernée l'occasion de s'exprimer (art. 377 CPP). L'ordonnance est susceptible de recours (art. 393sCPP).

82 Cadre juridique pour les médias sociaux**,** Rapport du Conseil fédéral en réponse au postulat Amherd 11.3912 du 29 septembre 2011, Berne 2013, p.53 ad 4.5.7.2 et p. 65 ad 5.4.1.

On notera que le blocage du nom de domaine par le « registre » (cf. supra 2.1.5) suit une procédure particulière. Le blocage en tant que tel s'opère sur simple requête d'un service de lutte contre la cybercriminalité reconnu ; en vertu de l'art. 15 al. 4 ODI, le titulaire du domaine (et non le registre) peut saisir l'Office fédéral de la police ; ce dernier confirmera (ou non) le blocage par le biais d'une décision administrative, susceptible de recours.

4. Surveillance générale d'internet

4.1. Monitorage par des autorités publiques

Il n'existe en Suisse aucune entité publique chargée de monitorer les contenus d'Internet de façon générale et systématique.

Dans le domaine pénal, on signalera toutefois l'existence, depuis 2001, du Service national de Coordination de la lutte contre la Criminalité sur Internet (SCOCI), un organisme rattaché à l'Office fédéral de la police, dont la tâche est de procéder à des analyses approfondies sur l'évolution de la criminalité en ligne, et pour ce faire, de conduire des recherches de contenus pénalement répréhensibles ; en pratique, l'accent est mis sur la pédopornographie, la propagande raciale et le discours haineux, ainsi que la criminalité économique. Il importe de souligner que le SCOCI n'est nullement une autorité de poursuite pénale, partant il ne dispose d'aucune compétence répressive. S'il vient à constater une infraction, il transmet le cas aux autorités compétentes (cantonales ou fédérales selon le type d'infractions) de poursuite pénale pour ouverture d'une enquête formelle. On notera que le SCOCI tient une liste des principaux sites criminels étrangers ; cette liste est transmise aux FAI avec la recommandation d'en bloquer l'accès. Ce mode de collaboration volontaire avec les FAI est jugé positif[83]. En matière de lutte contre la pédopornographie, les FAI se sont même engagés à bloquer l'accès sur requête du SCOCI[84] : leurs conditions générales de vente prévoient expressément cette mesure. Chaque année plusieurs centaines de milliers de requêtes de pages contenant des communications illicites ont ainsi été bloquées[85], le plus souvent suite à des notifications provenant des internautes (à cet effet, le SCOCI met à leur disposition un formulaire d'annonce de contenus douteux).

4.2. Monitorage par les fournisseurs de service Internet

A ce jour, aucune disposition légale n'oblige les fournisseurs de services Internet de monitorer les contenus qu'ils hébergent et/ou les sites auxquelles ils donnent accès. Peut-on en déduire que les fournisseurs de service sont dispensés de tout contrôle ? la doctrine dans sa grande majorité répond par l'affirmative[86] . La jurisprudence aussi, à en croire le seul arrêt du Tribunal fédéral en la matière, lequel concernait l'exploitant d'un forum de discussion ; il ne lui pas été reproché de n'avoir pas continuellement surveillé les contributions haineuses des tiers qui s'exprimaient sur son forum: « L'exploitation d'un forum de discussion est indissociable du risque que des contenus illégaux y soient déposés et, partant, que des intérêts juridiquement protégés par une norme pénale soient lésés. Si, en lui-même, ce risque n'excède pas ce qui peut être admis en société (Sozialadäquanz) et **ne permet vraisemblablement pas de fonder une obligation de surveillance permanente**, la

---

83 Rapport annuel du SCOCI 2014 p. 111.

84 Accord entre le SCOCI et les principaux fournisseurs d'accès suisses de 2007.

85 Cadre juridique pour les médias sociaux**,** Rapport du Conseil fédéral en réponse au postulat Amherd 11.3912 du 29 septembre 2011, Berne 2013, p.66 ad 5.4.2.

86 Voir en particulier Christiana Fountoulakis et Julien Francey, La diligence d'un hébergeur sur Internet et la réparation du préjudice, Medialex 2014, p. 181.

situation est cependant différente lorsque l'exploitant du forum a effectivement connaissance de la présence de ce contenu illégal sur son site [87] ».

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

Comme on aura pu le constater, le régime juridique du blocage et du retrait des contenus illicites ressortit en Suisse essentiellement au droit commun, ce qui ne manque pas de susciter interrogations et doutes quant à sa comptabilité avec les standards posés par le Cour européenne des droits de l'Homme en matière de restriction à la liberté de l'information. Faute de base légale spécifique, le respect des exigences de **clarté et de prévisibilité de la norme** appelée à fonder l'ingérence laisse beaucoup à désirer. Il est à espérer que le parlement, qui a enfin décidé de s'atteler à la tâche de définir les responsabilités des fournisseurs de services Internet (cf. supra 1 in fine) apportera sans tarder les éclaircissements nécessaires, comme le lui demande instamment, entre autres, le Tribunal fédéral, lequel s'est jusqu'à maintenant refusé à se substituer à un législateur défaillant: «il n'appartient pas à la justice, mais au législateur, de réparer les "graves conséquences" pour Internet et pour les hébergeurs de blogs auxquelles pourrait conduire l'application du droit actuel »[88].

En particulier, il importe de lever la grande incertitude qui règne quant à la possibilité ou non d'ordonner aux FAI, lesquels ne contrôlent ni directement ni indirectement les informations qu'ils font transiter, de bloquer l'accès à des contenus illicites. Les clarifications requises ne concernent pas seulement le blocage pénal ou administratif, mais aussi le blocage civil. Les dispositions générales qui le fondent (art. 28 CC, art. 62 LDA, art. 15 LPM et 9 LCD[89]) datent de l'ère pré-Internet ; leur portée doit être révisée en fonction du rôle joué par les différents types d'intermédiaires qui contribuent à la communication sur le réseau des réseaux.

Reste que l'on doit mettre en exergue le fait que les autorités administratives ainsi que les organes de poursuite pénale ont conscience de la précarité du régime actuel : dans leur rapport avec les FAI, elles n'ont que très rarement cherché à imposer des mesures de blocage, mais plutôt se sont engagées dans la voie du **dialogue**, tentant de persuader les FAI d'empêcher volontairement l'accès. Si cette approche souple doit être saluée, on ne peut s'empêcher d'émettre des réserves sur son adéquation avec les exigences de la Cour européenne des droits de l'Homme en matière de justiciabilité des mesures restreignant les libertés fondamentales : faute de toute décision formelle, il devient impossible de recourir contre un blocage abusif.

On notera enfin que, comme toutes les libertés fondamentales, la liberté d'expression ne peut être restreinte qu'à trois conditions précises, définies expressément par la constitution fédérale à son article 36 : **la mesure restrictive doit être prévue par une loi, elle doit répondre à un intérêt public et elle doit être proportionnée**. Cette dernière condition, en particulier, est très attentivement examinée par les tribunaux ; et témoigne leur volonté constante d'éviter l'*overblocking* ou de ne procéder au blocage que lorsqu'il est impossible d'agir en Suisse contre l'auteur ou l'hébergeur [90]. Il en va de même du législateur ; ainsi le code de procédure pénale souligne à son article 197 que les mesures de contrainte (catégorie à laquelle appartient le blocage ou le retrait préventif[91]) qui doivent

87 Arrêt du Tribunal fédéral du 2 mai 2008 (6B 645/2007), en particulier cons. 7.3.4.4.2 :

88 Arrêt du Tribunal fédéral du 14 janvier 2013 (5A_792/2011, cons. 6.3).

89 Cf. supra 2.

90 Cf supra 2.1.1.

91 Cf. supra 2.1.5

être appliquées non seulement en dernier ressort (priorité sera donnée à une mesure moins sévère si elle est envisageable), mais encore seront appliquées « avec une retenue particulière » à l'encontre des personnes qui n'ont pas le statut prévenu, tels les hébergeurs ou les FAI.

Bertil Cottier / 15 décembre 2015

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