YANIV BENHAMOU

BLOCAGE DE SITES WEB EN DROIT SUISSE

Des injonctions civiles et administratives au blocage pénal

Si le blocage de sites web est une mesure efficace, voire indispensable pour empêcher l'accès à certains contenus en ligne, en particulier lorsque l'hébergeur ou le fournisseur de contenu se trouve à l'étranger, elle fait l'objet d'une jurisprudence mouvante et de plusieurs controverses. La proportionnalité de la mesure revêt par ailleurs une importance particulière. Une mise à jour s'impose.

1. INTRODUCTION

Le blocage de sites web est une question importante pour le praticien et les tribunaux suisses [1]. Il s'agit d'une mesure consistant à bloquer un site, une page web ou un contenu déterminé et qui peut être ordonnée par une autorité à l'encontre d'un prestataire [2] (p. ex. il serait ordonné à Swisscom de bloquer l'accès à certains sites contenant des propos diffamatoires ou des œuvres en violation du droit d'auteur). Si une telle mesure est efficace, voire indispensable pour empêcher l'accès à certains contenus en ligne, en particulier lorsque l'hébergeur ou le fournisseur de contenu se trouve à l'étranger, elle fait l'objet d'une jurisprudence mouvante et de plusieurs controverses. Une mise à jour s'impose.

D'un point de vue technique, les *hébergeurs* peuvent généralement *retirer des contenus* déterminés mis à disposition sur leur portail (par le biais d'une action en prévention ou cessation de l'atteinte) [3], tandis que les *fournisseurs d'accès internet (FAI)* peuvent bloquer uniquement l'intégralité d'un nom de domaine par le *verrouillage des adresses IP ou DNS* [4]. Le *verrouillage des adresses IP* consiste à *bloquer l'accès à un serveur* sous une adresse IP spécifique. Une telle mesure entraîne le blocage de toutes les offres présentes sur le serveur et pas uniquement sur la page web ayant un contenu illicite. Le *verrouillage des adresses DNS* consiste à *bloquer le processus permettant de traduire* une adresse IP en un nom de domaine (forme parlante de l'adresse IP) [5]. C'est souvent le verrouillage DNS qui est utilisé pour des raisons financières et pratiques. Cela peut se faire au moyen d'un logiciel permettant de répondre à une requête DNS, soit directement (parce que le prestataire connaît l'URL) soit indirectement (en interrogeant le registre concerné). L'utilisateur voulant accéder à un site bloqué sera redirigé vers une page indiquant que le site est bloqué ou n'existe pas car le logiciel ne lui fournira pas l'adresse IP sollicitée [6]. Ces mesures ne sont que partiellement efficaces car leur *contournement* est relativement aisé. L'internaute peut contourner le verrouillage DNS en entrant l'adresse IP ou en appelant un autre serveur DNS et contourner le verrouillage de l'adresse IP en se connectant au serveur de destination via un serveur intermédiaire (serveur proxy). En outre, de nombreux sites web bloqués sont stockés sur d'autres serveurs en copie intégrale, c'est-à-dire par une mise en miroir (mirroring) ou en cache (caching) [7]. Il y aussi un risque d'*overblocking*, c'est-à-dire que soient bloqués non seulement les contenus consultables sous l'adresse IP qui doivent être supprimés, mais aussi les autres contenus (licites) consultables sous la même adresse IP [8].

D'un point de vue légal, il n'existe aujourd'hui *aucune règle spéciale ni de jurisprudence claire*. Certes la *loi sur le droit d'auteur (LDA)* est en cours de révision et fait l'objet d'un *projet de loi sur le droit d'auteur (pLDA)* [9], mais le projet final ne prévoiera certainement aucune mesure de blocage à l'égard des *fournisseurs d'accès internet (FAI)* [10]. Le pLDA est par ailleurs limité au droit d'auteur, alors que les portails touchent tous types d'atteinte (p. ex. atteintes à la personnalité, à la protection des données, violations de droit d'auteur, de droit des marques). Une telle mesure peut être envisagée en droit privé dans le cadre d'une action en cessation de l'atteinte, dans le cadre d'un séquestre ou confiscation pénal ou d'une procédure administrative à l'égard de certains contenus. Si une telle mesure est efficace, voire indispensable pour empêcher l'accès à certains contenus sur l'Internet, en particulier lorsque l'hébergeur ou fournisseur de contenu se trouve à l'étranger [11], elle fait l'objet d'une jurisprudence mouvante et de différentes controverses. Une mise à jour s'impose.

2. DROIT PRIVÉ: VERROUILLAGE DES ADRESSES IP ET DNS

Aujourd'hui, il n'existe aucune base légale expresse ni de jurisprudence autorisant le blocage (civil) des adresses IP et DNS [12]. Une telle mesure pourrait être néanmoins envisagée dans le cadre d'une action en cessation de l'atteinte. Le

YANIV BENHAMOU,
DR. IUR.,
AVOCAT, CHARGÉ
DE COURS À
L'UNIVERSITÉ DE GENÈVE,
GENÈVE,
YANIV.BENHAMOU@
UNIGE.CH

demandeur pourrait demander au juge le *blocage de l'adresse IP/DNS à l'égard des FAI* (et/ou le *retrait d'un contenu déterminé, take down, à l'égard d'un hébergeur*). Un tel *blocage pourrait être ainsi ordonné* par un juge, sans être nécessairement qualifié d'injonction de blocage, par exemple en ordonnant au prestataire d'éliminer toute possibilité d'accéder à ces contenus. Une telle mesure devra toutefois respecter le principe de proportionnalité [13].

2.1 Légitimation passive des prestataires en cas d'atteinte à la personnalité. Contrairement aux droits américain [14] et de l'Union européenne [15], le droit suisse se caractérise par l'*absence de règles spéciales* en matière de responsabilité civile des prestataires. La responsabilité est donc fondée sur les *règles générales*. Cette situation devrait rester inchangée (à l'exception du droit d'auteur) [16]. La *responsabilité civile* du prestataire peut être engagée si sa participation est suffisante pour lui conférer la légitimation passive. Toute la difficulté est alors de déterminer le *degré de participation,* puisque tout prestataire peut être considéré comme participant.

En cas *d'atteinte à la personnalité* (p. ex. atteinte à la vie privée ou l'honneur), le demandeur peut agir en prévention ou cessation de l'atteinte contre toute personne qui y participe (CC 28 al. 1) [17]. Une *contribution mineure* suffit. Le *Tribunal fédéral (TF)* a admis la responsabilité de la Tribune de Genève en tant qu'hébergeur d'un blog au motif qu'il est possible d'agir contre «*quiconque a objectivement joué* [...] *un rôle – fût-il secondaire – dans la création ou le développement de l'atteinte*» [18]. La légitimation passive des prestataires médias est ainsi admise *largement* par le TF [19]. Appliqué aux prestataires, cette approche permettrait d'admettre *systématiquement la légitimation passive* des prestataires puisqu'ils jouent un rôle objectif, même secondaire, dans la transmission d'informations. La responsabilité n'est toutefois pas illimitée puisqu'elle doit être ensuite restreinte par la proportionnalité [20].

2.2 Légitimation passive des prestataires en cas d'atteinte aux droits de propriété intellectuelle. En cas *d'atteinte à un droit de propriété intellectuelle* (droit d'auteur, marque, brevet, design), le demandeur peut aussi agir en prévention ou cessation contre le participant à l'atteinte (LBI 66 let. d; LDes 9 al. 2; LDA 62 al. 1; LPM 55). Il n'est pas clair si la légitimation passive est comprise de façon identique ou moins large que dans le droit de la personnalité. La jurisprudence et la doctrine tendent à limiter la légitimation passive aux actes de participations qualifiés en référence aux règles du droit des brevets et droit du design (LBI 66 let. d; LDes 9 al. 2) prévoyant la légitimation passive de toute personne qui incite, collabore, favorise ou facilite l'exécution d'une atteinte [21], ou en *référence à l'art. 50 du Code des obligations (CO),* prévoyant la légitimation de celui qui sait ou doit savoir que ses services sont aptes à violer le droit et que les clients violent effectivement le droit [22].

2.3 Appréciation. Appliqué aux prestataires, la légitimation passive en cas d'atteinte aux droits de propriété intellectuelle suppose *de rejeter la responsabilité des FAI* pour défaut d'incitation ou de connaissance du contenu et *d'admettre celle de l'hébergeur uniquement s'il a connaissance* de violations concrètes (en cas de sommation préalable ou de services fournis intentionnellement en vue de violer le droit). Cette *approche nous semble douteuse* puisque l'on conditionne les actions défensives à la faute du prestataire, laquelle s'analyse uniquement au stade d'une action en dommages-intérêts, et que l'on glisse ainsi vers une subjectivisation de l'atteinte. Selon nous, il faudrait donc admettre une solution uniforme à l'égard des prestataires, puisque les prestataires et les portails en ligne peuvent porter atteinte à tous types de droits, et que des solutions fragmentées en fonction des droits protégés apporteraient confusion et incertitude en la matière. Il convient par ailleurs d'admettre que les FAI jouent un rôle, même purement objectif et secondaire, dans le flux d'informations et donc la possibilité de réalisation des atteintes, de sorte qu'il faudrait admettre leur *légitimation passive systématiquement* puis vérifier le fondement de l'action sous l'angle de la proportionnalité.

3. DROIT PÉNAL: BLOCAGE PRÉVENTIF (SÉQUESTRE CPP 263) OU DÉFINITIF (CONFISCATION CP 69)

3.1 La controverse. Le prestataire n'engage en principe *pas sa responsabilité pénale* puisqu'il ignore généralement le type d'informations insérées par le fournisseur de contenu sur l'espace offert [23]. La responsabilité pénale des médias ne semble pas non plus engagée puisque le prestataire n'a aucun contrôle éditorial sur l'information litigieuse [24]. Le blocage pénal doit donc être envisagé sur un autre fondement, sur la base d'un séquestre (blocage préventif) ou confiscation (blocage définitif). Dans les deux cas, la *mesure est controversée:* elle ne repose sur *aucune base légale expresse* mais sur une *interprétation extensive* des dispositions procédurales relatives au séquestre (CPP 263) ou matérielles relatives à la confiscation d'objets dangereux (CP 69) [25], alors que le libellé de ces deux dispositions *vise expressément des objets* (biens corporels matériels) [26].

3.2 La jurisprudence. Cette controverse n'a *pas empêché les autorités pénales d'ordonner le blocage* sur la base du séquestre/confiscation. Certains tribunaux cantonaux ont en effet considéré que le caractère virtuel ou difficilement saisissable d'un accès à Internet ne constituait pas un obstacle au séquestre/confiscation et ont *assimilé les sites web à des objets.* Les *tribunaux cantonaux* ont ainsi validé à plusieurs reprises une ordonnance de blocage sur la base du séquestre/confiscation à l'encontre de FAI basés en Suisse pour des sites web donnant accès à des informations illicites. L'argument principal était qu'une telle interprétation tient compte des progrès techniques et est ainsi conforme à l'esprit de la loi et qu'il est *proportionnel* de bloquer l'accès plutôt que de séquestrer les serveurs en vertu de l'adage «qui peut le plus peut le moins» [27].

Le TF ne s'est pas encore prononcé clairement sur la question. Dans un arrêt du 19 mars 2015 («Blogger»), le *TF a rejeté une ordonnance de blocage* de deux sites contenant des accusations diffamatoires qui était fondée sur CP 69 al. 2 et considérait que blocage définitif était *comparable à une destruction* au sens de l'art. 69 al. 2 CP. Le TF a rejeté l'ordonnance de blo-

cage aux motifs qu'elle était *contraire au droit de procédure* (la confiscation au sens de CP 69 al. 2 doit être ordonnée par le juge, et non au stade de l'instruction) et au *droit de fond* (le blocage vise la cessation d'un comportement, non la mise hors d'usage/destruction d'un objet dangereux). Le TF a en revanche *laissé expressément ouverte la question du blocage fondé sur CP 69 al. 1,* se bornant à renvoyer l'affaire à l'instance inférieure pour qu'elle examine si les conditions d'un blocage étaient réunies (gravité des accusations formulées et proportionnalité de la mesure devant se limiter aux seuls blocages litigieux) [28].

> *«Si l'on constate le malaise du TF pour admettre le blocage pénal de sites web vu l'absence de base légale claire, on peut aussi constater la tendance des tribunaux à l'interprétation extensive des lois pour combler certaines lacunes face aux technologies.»*

3.3 Les deux interprétations possibles. Vu l'absence de base légale expresse et de position claire du TF, *il convient d'analyser* si un *site web* peut être considéré comme un *«objet»* ou une *«valeur patrimoniale»* pouvant être séquestré/confisqué.

Selon une première approche (interprétation littérale), le libellé du séquestre/confiscation *se limite aux «objets» matériels.* Les données informatiques (ou le blocage de sites web) en tant que biens virtuels ne sont pas couvertes par le séquestre/confiscation, pas plus qu'elles ne sont couvertes par les dispositions sur le vol (art. 139 CP) et le dommage à la propriété (art. 144 CP). *Pour appréhender les données informatiques,* il a fallu édicter des *dispositions spéciales,* telles que la soustraction de données (art. 143 CP) et la détérioration de données (art. 144bis CP) [29]. Si l'on voulait prévoir le blocage pénal de sites web, il *faudrait compléter les dispositions du CPP* sur le séquestre par une disposition *ad hoc* de blocage ou, si l'on considère que le rôle du droit pénal est de sanctionner un comportement et non pas de faire cesser un trouble, compléter les mesures civiles ou administratives inspirées de l'art. 15 ODI et des art. 88 ss du projet de Loi fédérale sur les jeux d'argent (P-LJAr) [30]. D'ailleurs, le fait que le P-LJar prévoit une base légale spécifique au blocage indique bien qu'une telle possibilité de confiscation/séquestre de sites web n'existe pas et qu'une disposition spécifique est nécessaire.

Selon une deuxième approche (interprétation extensive), les données informatiques (ou le blocage de sites web) sont des objets (ou valeurs patrimoniales) couverts par le séquestre/confiscation. Dans l'arrêt «Blogger», le TF a *laissé expressément ouverte la question de l'art. 69 al. 1 CP* en renvoyant l'affaire à l'instance inférieure pour examiner si les conditions d'un blocage étaient réunies (soupçons et proportionnalité). Dans deux *arrêts récents* du 16 novembre 2016 («Facebook» et «Google»), le TF a admis que les *données informatiques* d'un compte utilisateur sont des objets (ou valeurs patrimoniales) *soumis à l'obligation de dépôt* (CPP 265) sur la base d'un arrêt assimilant les courriels à des titres électroniques (CP 110 al. 4) et d'une lacune de la loi excluant les mesures de surveillance par poste et télécommunication (CPP 269 ss) aux prestataires de messageries tels que Facebook/Gmail [31].

3.3.1 Appréciation. Si l'on constate le malaise du TF pour admettre le blocage pénal de sites web vu l'absence de base légale claire [32], on peut aussi constater la *tendance des tribunaux à l'interprétation extensive* des lois pour combler certaines lacunes face aux technologies. Il suffit de penser à l'arrêt du TF «Blogger» (assimilant les données informatiques à des objets ou valeurs patrimoniales), et aux arrêts du TPF et du Tribunal cantonal vaudois (suivant l'adage «qui peut le plus peut le moins» et visant à combler une lacune lumière des technologies) [33].

L'absence de base légale en matière de blocage de sites web est bien une *lacune proprement* dite de la loi. A supposer que l'intention du législateur était d'exclure le blocage de sites web de la norme générale (CP 69), force est de constater que même les normes spécifiques confiscatoires excluent aussi le blocage de sites web: par exemple les normes confiscatoires en matière de pornographie dure ou de représentation de la violence (CP 197 al. 6, 135 al. 2) règlent de manière analogue la confiscation de l'objet du délit [34] et portent aussi sur des objets (ou représentations) en tant que support [35]. Il paraît ainsi douteux, voire inconcevable que la mesure civile (blocage de sites web) ne puisse pas être ordonnée également au pénal, en tous les cas à l'égard de sites contenant de la pornographie dure et des représentations de violence [36]. On peut penser que le législateur a omis involontairement de prévoir de telles mesures ou d'étendre le séquestre / confiscation aux sites web. Cette lacune proprement dite doit pouvoir être comblée par le juge [37].

L'interprétation extensive suppose le *raisonnement suivant.* Les données informatiques peuvent être séquestrées/confisquées en tant qu'objets dangereux ayant servi à commettre des infractions et compromettant la morale ou l'ordre public (CP 69 al. 1). L'*analogie* entre les *objets* et les *données informatiques* a été confirmée par le TF dans l'arrêt «Blogger» assimilant les données d'un compte utilisateur gmail/facebook à un objet ainsi qu'un arrêt antérieur assimilant l'e-mail à une lettre [38]. Les données informatiques peuvent être considérées comme ayant «servi à commettre des infractions et compromettent la morale ou l'ordre public» (p. ex. des propos négationnistes ou diffamatoires) [39]. L'approche «qui peut le plus peut le moins» adoptée par la jurisprudence cantonale et le Tribunal pénal fédéral semble enfin pertinente puisque l'autorité pénale pourrait effectivement ordonner le séquestre/confiscation des serveurs physiques (et ce même s'ils sont à l'étranger) et choisir le blocage du site web (i. e. du flux de données transitant par les serveurs du FAI) semble bien proportionnel.

Le *blocage de sites web semble donc possible* selon une interprétation extensive du séquestre/confiscation pour combler une lacune proprement dite et faire face aux technologies. Ce résultat est toutefois *discutable* sous l'angle de la légalité des

peines et de la sécurité du droit (le malaise et l'absence de position claire du TF en sont la preuve), et il est *souhaitable* que le législateur prévoie à terme une disposition *ad hoc* de blocage, ou des mesures administratives inspirées de l'art. 15 ODI et des art. 88 ss P-LJAr.

4. DROIT ADMINISTRATIF: DÉCISION OU COOPÉRATION EN VUE DU BLOCAGE DE CERTAINS CONTENUS

Les autorités administratives ont aussi dans certains cas la compétence d'ordonner le blocage de sites.

4.1 Décision administrative de blocage (ODI, P-LJAr). *L'Ordonnance sur les domaines Internet (ODI)* permet le blocage de *sites malveillants* par le biais d'une décision administrative. Le «registre» [40] doit bloquer un nom de domaine de son ressort en cas de soupçons sérieux que le site correspondant est utilisé pour accéder illictement à des données critiques de tiers *(hameçonnage)* ou pour diffuser des logiciels malveillants *(maliciels)* (ODI 15 al. 1 let. a). La mesure est d'abord demandée par un service de lutte contre la cybercriminalité reconnu par *l'Office fédéral de la communication, OFCOM* (ODI 15 al. 1 let. b) puis confirmée par *l'Office fédéral de la police (fedpol)* qui rend une décision administrative de blocage (ODI 15 al. 4).

Le *projet de loi sur les jeux d'argent (P-LJAr)* prévoit l'insertion d'une nouvelle mesure de blocage. Après des pourparlers infructueux entre les principaux FAI suisses et la Commission fédérale des jeux, le projet prévoit que cette Commission pourra ordonner le *blocage de sites de jeux d'argent en ligne non autorisés dont l'exploitant a son siège à l'étranger. Une liste noire des offres non autorisées* sera régulièrement tenue à jour, transmise aux FAI pour blocage puis officiellement publiée (P-LJAr 84).

A ce titre, on mentionnera également le *pLDA* prévoyant une mesure de blocage par le biais d'une liste établie par l'IGE et d'une décision administrative. Cette mesure risque toutefois d'être supprimée du projet final [41].

4.2 Coopération visant à bloquer certains contenus (LSMI, SCOCI). La *loi fédérale sur la sécurité intérieure (LMSI)* prévoit une possibilité de *blocage sur une base volontaire.* L'Office fédéral de la police peut recommander aux FAI suisses de bloquer l'accès à des sites dont les serveurs se trouvent à l'étranger et contenant du *matériel d'incitation à la violence* (p. ex. propagande djihadiste) (LMSI 13*e*, ch. 5). Comme le relève Cottier, cette démarche codifie la pratique administrative en matière de blocage consistant à privilégier le dialogue avec les FAI réticents à toute instrumentalisation mais repose sur une base de recommandation et de coopération volontaire [42].

On mentionnera enfin le *Service de coordination de la lutte contre la criminalité sur Internet (SCOCI),* créé fin 2001 et rattaché à fedpol qui permet à toute personne de lui *signaler l'existence de sites ou contenus en ligne suspects:* les contenus signalés font l'objet d'un premier examen, puis transmis aux autorités de poursuite pénale en Suisse ou à l'étranger. Le SCOCI parcourt aussi internet à la recherche de contenus illicites et soutient les FAI en matière de lutte contre la pornographie, en leur transmettant une liste des sites Internet étrangers offrant certains types de pornographie.

4.3 Appréciation. Les mesures administratives sont efficaces, et ont porté leurs fruits dans certains domaines, en tant qu'elles reposent sur le droit administratif permettant aux autorités d'investiguer et d'agir d'office soit sur le dialogue avec les FAI. Le revers de la médaille est qu'elles ne tiennent pas compte des mêmes droits de procédure que les mesures civiles et pénales et limitées à certains domaines, conduisant ainsi à une fragmentation des solutions, voire à une incertitude des autres domaines dépourvus de base légale expresse.

«A propos du droit des internautes, il convient d'éviter de bloquer des sites offrant du contenu légal et illégal à la fois (overblocking).»

5. PROPORTIONNALITÉ

La mesure du blocage doit respecter le principe de proportionnalité, autrement dit le juge devra tenir compte de tous les intérêts en présence qui risquent d'être lésés par la mesure [43]. La proportionnalité est particulièrement délicate à l'égard des prestataires vu leur manque de contrôle et d'influence sur le contenu [44]. Un FAI pourrait ainsi invoquer le fait que, dans un cas concret, il ne lui est pas raisonnable, d'un point de vue technique, d'empêcher l'accès à certains contenus et que la mesure est disproportionnée. La mesure doit par ailleurs cibler uniquement les informations illicites et éviter l'accès aux autres communications licites (interdiction de l'*overblocking*).

5.1 Droits fondamentaux. En cas de blocage, la proportionnalité suppose de *tenir compte des autres droits en présence.* En droit suisse, il existe peu de jurisprudence sur cette question, à l'exception de quelques décisions cantonales pénales reconnaissant la primauté de la paix publique, de l'honneur ou du secret sur l'intérêt financier du FAI à ne pas prendre des mesures techniques de contrôle ou de blocage [45]. Vu l'absence de jurisprudence en droit suisse, il est utile de s'inspirer du droit européen [46].

A propos du *droit des titulaires,* la *Cour de justice de l'Union européenne (CJUE)* a estimé dans l'arrêt The Pirate Bay que la transmission d'information légale méritait davantage de protection que la transmission d'information illégale [47].

A propos du *droit des FAI,* la CJUE a estimé dans l'arrêt kino.to que le blocage ne porte pas atteinte au fondement même de la liberté d'entreprise des FAI puisqu'ils *peuvent continuer d'exercer leurs activités* malgré une mesure de blocage. La mesure de blocage *ne doit toutefois pas* obliger le FAI à faire des *sacrifices insupportables* (solutions techniques difficiles et complexes entravant ses activités), et doit *laisser au FAI le choix* de la mesure qui convient le mieux à ses ressources [48].

A propos du *droit des internautes,* il convient *d'éviter de bloquer* des sites offrant du *contenu légal* et illégal à la fois *(overblocking).* Cet argument n'a généralement pas été retenu par les tribunaux puisque la plupart des cas concernaient des sites conçus principalement pour permettre le partage de fichiers illégaux (p. ex. *The Pirate Bay*) [49]. Il conviendra toutefois de prendre garde à ce que la mesure de blocage soit strictement ciblée [50].

A propos du *droit des exploitants* de plateforme, la *Cour européenne des droits de l'homme (CEDH)* a considéré dans l'arrêt The Pirate Bay que la condamnation pénale des exploitants du site était une restriction à leur liberté d'expression mais qu'une telle restriction était justifiée notamment du fait que les informations en question ne bénéficient pas du même niveau de protection que le débat politique [51].

5.2 Proportionnalité quant aux sites visés. Pour respecter le test de proportionnalité, la mesure de blocage doit *cibler les sites ayant des informations principalement illicites* [52]. Pour déterminer quels sont les sites à cibler, on proposera de tenir compte de *plusieurs critères,* tels que la quantité d'informations illégales, de l'objectif poursuivi par le portail et de la nature des informations (commerciale, politique ou créative).

S'agissant de la *quantité d'informations,* il faudra cibler les sites offrant du contenu principalement illicite, par opposition aux sites ayant des informations essentiellement licites et sur lesquels seules quelques informations illicites isolées sont accessibles [53].

S'agissant de *l'objectif poursuivi* par le portail, on peut s'inspirer de la jurisprudence étrangère, en particulier l'affaire américaine Grokster et l'affaire européenne TPB. Dans *l'arrêt Grokster,* la Cour suprême américaine a admis la responsabilité indirecte *(contributory infringement)* pour incitation à la contrefaçon *(inducement of infringement)* sur la base de trois éléments: (i) l'exploitant *tentait d'attirer les anciens utilisateurs du réseau Napster* (par le nom donné aux produits, la publicité adressée aux utilisateurs de Napster et l'aménagement du réseau qui a été rendu compatible avec Napster), (ii) profitait directement des violations de droit d'auteur par la *vente d'espace publicitaire* et (iii) était *conscient* que la plupart des utilisateurs du logiciel utilisait ce dernier pour échanger des œuvres en *violation du droit d'auteur* (environ 90% des fichiers échangés sur le réseau) sans prendre de mesure à cet égard [54]. Dans *l'arrêt The Pirate Bay,* la CJUE a retenu que les exploitants de la plateforme avaient un objectif de mettre à disposition des œuvres en violation du droit d'auteur (via l'indexation des fichiers torrents, la mise à disposition d'un moteur de recherche classant les œuvres par catégories de genre et de popularité) et d'en *retirer un bénéfice* (via des recettes publicitaires) et avaient été *informés du caractère illicite* de nombreux fichiers échangés (via les blogs et forums disponibles sur la plateforme). On peut enfin s'inspirer de la loi sur le droit d'auteur canadienne définissant l'acte de participation accessoire des exploitants de plateformes. Cette participation est établie selon la *promotion* des activités de mise à disposition d'œuvres en violation du droit d'auteur, la *connaissance* de l'exploitant quant aux échanges illcites et les *mesures prises pour lutter* contre celles-ci, les *revenus* tirés de ces échanges illicites et la viabilité économique de la plateforme en l'absence des échanges illicites [55].

S'agissant de la *nature des informations,* sur la base de la jurisprudence européenne, on relèvera que des informations contenant des copies d'œuvres de droit d'auteur sont moins protégées que les *informations à débat politique* [56] et que les discours d'incitation à la haine et à la violence ne sont pas protégés [57].

En *résumé,* on peut considérer qu'un exploitant est une offre manifestement illicite justifiant une mesure de blocage en fonction de la quantité d'échanges illicites, des revenus générés par ces échanges illicites et l'incitation à utiliser les services pour les échanges illicites.

5.3 Proportionnalité quant à la technique visée. La proportionnalité suppose également d'adapter les mesures en fonction du système utilisé par le FAI (p. ex. automatisé ou non) et de l'évolution des technologies [58]. Une injonction serait par exemple disproportionnée si elle ordonnait à un FAI ayant des services automatisés la mise en œuvre de *mesures non automatisables,* et pouvait ainsi conduire à la cessation complète des activités du FAI [59]. L'état actuel technique conduira certainement les FAI à mettre en œuvre le blocage principalement sous forme de verrouillage des adresses IP ou DNS [60]. Le *verrouillage des adresses IP* paraît disproportionné à l'égard de grands exploitants ouvrant accès à des milliers de contenus différents (cela entraîne le blocage de toutes les offres présentes sur le serveur, et pas seulement la page web ayant un contenu illicite), tandis qu'il paraît proportionnel pour les offres illicites disposant de leur propre serveur ou pour les adresses IP offrant uniquement des contenus illicites similaires (p. ex. racistes, pornographiques ou illégaux dans leur quasi-totalité) [61]. Le verrouillage DNS paraît donc plus proportionnel, et ce sera même souvent préféré en raison des coûts maîtrisables pour les FAI [62].

5.4 Proportionnalité quant au coût. La question du coût de la mesure de blocage est débattue dans de nombreuses juridictions qui admettent généralement que les FAI doivent prendre en charge ces coûts même s'ils ne sont pas directement responsables des violations [63].

En droit suisse, sous l'angle du *blocage pénal* de sites, le *FAI peut réclamer remboursement à l'Etat,* soit une indemnisation pour le dommage causé par la mesure de blocage (CPP 434) [64]. Sous l'angle du *blocage civil* de sites, le tribunal met en général les *frais à la charge de la partie succombante* (CPC 106 al. 1) mais peut s'en écarter lorsque des circonstances particulières rendent la répartition en fonction du sort de la cause inéquitable (art. 107 al. 1 let. f CPC). Le prestataire pourrait tenter de convaincre le juge de mettre à la charge du demandeur les coûts de mise en œuvre du blocage. Il s'exposera toutefois à la libre appréciation du juge qui pourrait refuser en considérant que de tels coûts sont proportionnels, par exemple parce qu'il est préférable de les laisser à la charge du FAI pouvant choisir la mesure la moins onéreuse, qu'il a déjà bénéficié de revenus grâce au contenu illicite (via l'augmentation des visites et/ou les annonceurs) et qu'un demandeur obtenant gain de cause ne doit pas supporter de coûts additionnels de

mise en œuvre. Enfin les coûts semblent maîtrisables et non excessifs [65].

5.5 Subsidiarité du blocage par rapport aux actions directes ou à la désindexation. Selon le principe de subsidiarité, il faudrait agir directement contre le contrevenant ou autres intervenants (annonceurs, fournisseurs de services de paiement ou registraires) et, uniquement subsidiairement, contre les FAI avec le blocage, au motif que les premiers seraient plus proches de la violation que les seconds.

Le principe de *subsidiarité a été suivi par certains tribunaux.* En Allemagne et en Autriche, le blocage est admis uniquement lorsque les actions directes s'avéraient impossibles (p. ex. parce que le contrevenant est introuvable) ou inefficaces (p. ex. parce que la mise en œuvre est trop lente et coûteuse) [66]. En Suisse, ce principe a été proposé dans le pLDA [67].

Le principe de subsidiarité est *criticable* car il n'a *aucun fondement légal* et rend souvent le *blocage inefficace* (les serveurs sont souvent localisés dans des juridictions n'offrant pas de mise en œuvre efficace des droits ou une mise en œuvre lente et coûteuse) [68]. En effet, le blocage est nécessaire précisément pour les situations où il n'est pas possible d'agir contre ces opérateurs. Ces motifs expliquent pourquoi ce principe n'a pas été suivi par la CJUE ni la plupart des juridictions voisines. Le blocage devrait donc être admis *indépendamment des autres mesures* possibles (ou en tout cas lorsque les autres mesures paraissent lentes et coûteuses) et *cumulativement* à d'autres actions, telles qu'une demande en *désindexation* de sites web [69]. Cette approche est d'autant plus justifiée du fait que la désindexation n'est pas un droit clairement établi, en tous les cas à l'égard des droits de PI, et que les sites web continuent à être accessibles malgré la désindexation [70].

5.6 Mise en œuvre effective: possibilité de contournement. On reproche parfois à la mesure de blocage le fait qu'elle puisse être contournée. Parmi les techniques utilisées pour contourner le blocage, on mentionnera l'utilisation de proxys ou le changement régulier d'adresses IP/URL hébergeant le site litigieux: certains FAI utilisent en effet plusieurs noms de domaine et adresses IP qu'ils changent régulièrement en fonction des mesures de blocage ciblant certains noms de domaine spécifiques [71].

Cela étant, le blocage ne doit *pas nécessairement conduire à la cessation complète* des violations; il suffit que la mesure soit *raisonnablement efficace pour stopper ou prévenir* des violations [72] et, selon plusieurs études, elle réduit substantiellement (de 70 à 90%) la visite des sites bloqués par les internautes [73]. Le fait qu'il soit possible de contourner des mesures techniques ne saurait constituer un argument pour y renoncer. Dans de nombreux domaines, il est possible d'éluder les règles de contrôle (p. ex. lutte contre le blanchiment). De même, dans le cadre de la circulation routière, il n'est pas rare que certains contrevenants ne puissent pas être identifiés. Cela ne signifie pas pour autant qu'il faille renoncer aux mesures de contrôle utiles sur les flux financiers ou de la vitesse [74].

La mise en œuvre judiciaire est donc un enjeu pour les titulaires et les autorités. Pour pallier les modes opératoires précités (p. ex. changement régulier de noms de domaines), certains tribunaux ordonnent des *injonctions de blocage dynamiques.* Au Royaume-Uni et en Irlande, le blocage porte sur des sites web *(location online)* sans se référer à un nom de domaine/adresses IP spécifique et prévoit un mécanisme selon

«La mise en œuvre judiciaire est donc un enjeu pour les titulaires et les autorités. Pour pallier les modes opératoires précités (p. ex. changement régulier de noms de domaines), certains tribunaux ordonnent des injonctions de blocage dynamiques.»

lequel le titulaire peut notifier aux FAI tout changement ou nouveau de nom de domaine hébergeant le site litigieux pour que le FAI l'ajoute aux mesures de blocage [75]. Un Tribunal a même récemment adopté une injonction de blocage live *(live blocking)* contre une retransmission streaming illégale suite à une action déposée par la *Football Association Premier League* qui n'avait d'effet que lors de la rediffusion du match de première ligue et uniquement pendant la saison (i. e. du 18 mars 2017 au 22 mai 2017) [76]. En Australie, bien que la mesure ne prévoie pas un mécanisme de notification de nouvelles adresses IP/URL, elle peut être modifiée pour inclure de nouvelles adresses. D'autres juridictions ne prévoient pas d'injonction dynamique (notamment Argentine, Autriche, Finlande, France, Italie, Espagne). Un changement d'adresses requiert une nouvelle demande de blocage au Tribunal.

En *droit suisse,* une telle *injonction dynamique* semble contraire au droit de procédure. Le demandeur doit formuler des conclusions de manière à pouvoir être, le cas échéant reprises à l'identique dans la décision et à permettre une exécution forcée sans qu'il soit nécessaire de se référer aux motifs [77]. On peut alors envisager deux solutions: (i) solliciter *l'exécution directe* [78] et, à chaque nouveau changement d'adresses IP/URL de l'exploitant, refaire une nouvelle demande ou (ii) solliciter *l'exécution indirecte,* en présentant une requête au tribunal d'exécution accompagnée de tous les documents utiles, y compris l'attestation du caractère exécutoire de la demande [79].

5.7 Appréciation. La proportionnalité permet d'encadrer la mesure: après avoir admis son fondement légal sous l'angle civil, pénal et administratif, l'autorité en charge de la mesure devra apprécier strictement la proportionnalité de la mesure. Elle devra en particulier tenir compte de tous les intérêts en présence qui risquent d'être lésés par la mesure [80]. Un tel exercice est délicat, non seulement vu le manque de contrôle et d'influence sur le contenu de la part des prestataires [81] mais également vu la diversité des techniques de blocage, la variété des types d'atteintes et sites web et le risque d'*overblocking.* Dans ce contexte, l'autorégulation (p. ex. recommandations pratiques émises par les différents groupes d'in-

térêts, si possibles associées et approuvées par une autorité) permettrait d'apporter plus de transparence et de clarté aux prestataires et d'être adaptée au fur et à mesure de l'évolution des technologies de façon plus légère qu'une base légale.

6. CONCLUSION

Alors qu'à l'étranger la mesure de blocage semble être efficace et que la question porte surtout sur les modalités d'une telle mesure (p. ex. coûts et caractère dynamique de la mesure), la Suisse n'offre toujours *pas de base légale claire* pour la fonder.

> *«Alors qu'à l'étranger la mesure de blocage semble être efficace et que la question porte surtout sur les modalités d'une telle mesure la Suisse n'offre toujours pas de base légale claire pour la fonder.»*

Une telle mesure peut pourtant se baser sur *différents fondements légaux* mais fait l'objet de différentes *controverses*. En *droit civil,* la controverse est d'admettre la *légitimation passive* des FAI. A notre avis, elle devrait être admise systématiquement en référence à la jurisprudence en matière d'atteinte à la personnalité. En *droit pénal,* la controverse est d'admettre une *interprétation extensive* de la mesure de blocage/confiscation malgré un libellé limité aux objets. Une telle interprétation extensive semble possible, voire requise pour combler une lacune proprement dite et faire face aux technologies. Ce résultat est toutefois discutable sous l'angle de la légalité des peines et de la sécurité du droit et il est souhaitable que le législateur prévoie à terme une disposition générale *ad hoc* de blocage, ou des mesures administratives inspirées de l'art. 15 ODI et des art. 88 ss P-LJAr. Une telle disposition *ad hoc* devrait être applicable de manière transversale sans être sectorielle/limitée à certains domaines particuliers. En *droit administratif,* certaines mesures permettent le blocage et ont prouvé être efficaces. Elles sont toutefois *limitées à certains domaines,* conduisant à une fragmentation des solutions, voire à une incertitude dans les autres domaines dépourvus de base légale expresse.

Il faudrait donc admettre clairement une telle mesure, en tous les cas sur le *fondement civil et pénal général,* plutôt que sur des règles spéciales sectorielles (p. ex. pLDA), ce afin *d'éviter une fragmentation* des solutions. Cette question de blocage de sites web concerne en effet tous types d'atteintes, sans se limiter au droit d'auteur ou autre domaine. Après avoir admis le principe d'une telle mesure, celle-ci devra être proportionnelle et tenir compte de tous les intérêts en présence. Cette contribution tente ainsi de *proposer différentes solutions,* soit d'abord d'admettre la mesure sous l'angle des différents fondements et ensuite de *donner les critères applicables à la proportionnalité* de la mesure.

Alternativement ou cumulativement aux mesures de blocage, il serait important de bien *considérer d'autres méthodes dont la désindexation de sites web et/ou l'approche follow the money,* dont l'idée est d'associer les services payants, les sociétés émettrices de cartes de crédit (p. ex. *PayPal*) et les acteurs de la publicité en ligne, pour faire en sorte que l'exploitation de sites pirate devienne moins lucrative. Cette dernière approche *follow the money* n'est pas suffisamment mûrie aujourd'hui et devra respecter tous les intérêts et droits fondamentaux en présence (dont la protection des données des internautes) mais constituerait certainement une mesure efficace [82].

En plus des mesures judiciaires, il serait par ailleurs utile de *favoriser l'autorégulation*. Cela apporterait de la *transparence* aux FAI qui pourraient s'appuyer sur des lignes directrices (p. ex. en matière de proportionnalité). À titre d'exemples, on peut songer aux lignes directrices émises par le Conseil de l'Europe, en coopération avec l'Association européenne des fournisseurs de service Internet (EuroISPA), visant à aider les FAI (en particulier sous l'angle de la proportionnalité) ou à la liste établie par le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) et répertoriant les sites qui sont accessibles depuis le site et contenant selon toute vraisemblance de la pornographie enfantine. L'autorégulation offrirait en outre la *souplesse nécessaire pour tenir compte de l'évolution des technologies* en recommandant de manière dynamique/évolutive les mesures de blocage qui devraient être techniquement mises en place par les FAI. ■

Notes: 1) Cette contribution est une version courte d'un article plus détaillé à paraître dans la collection pi-ip en 2017 suite à une présentation sur le «Droit d'auteur & numérique: défis et développements du droit suisse» dans le cadre de la journée de droit de la propriété intellectuelle (JDPI) du 22 février 2017 organisée par l'Université de Genève. **2)** Par «prestataire», on entend tout intermédiaire internet offrant à ses utilisateurs une prestation (souvent automatisée), sans contrôle éditorial sur l'information et couvre tant les hébergeurs (i. e. prestataires mettant à disposition un espace sur lequel l'utilisateur peut enregistrer son contenu) que les fournisseurs d'accès internet (i. e. permettant aux utilisateurs d'accéder à Internet via un téléphone ou un accès à large bande). Cf. Rapport du Conseil fédéral du 11 décembre 2015, La responsabilité civile des fournisseurs de services internet, 20, soulignant que les frontières entre ces rôles sont souvent poreuses car les formes mixtes ou particulières de prestataires sont nombreuses. **3)** Cottier Bertil, Etude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, Etude du Conseil de l'Europe préparée par l'Institut suisse de droit comparé, Lausanne 2015, 681 ss; Rapport (n. 2), 46. **4)** Rapport (n. 2), 20, 46, indiquant que l'hébergeur ne peut parfois pas supprimer des contenus isolés sur un serveur qu'il loue mais uniquement mettre hors service le serveur loué dans son intégralité. **5)** Rapport (n. 2), 47, comparant le fait d'effacer le numéro de téléphone d'une personne dans un exemplaire d'annuaire. **6)** Equey David, La responsabilité pénale des fournisseurs de services internet, Stämpfli 2016, 339. **7)** Equey, 332, évoque aussi le fait qu'il existe plusieurs résolveurs DNS en libre d'accès (p. ex. Google Public DNS, OpenDNS ou French Data Network). **8)** Cf. Equey, 331, évoque aussi le fait que ces mesures entraînent des problèmes de performance (p. ex. ralentissement du temps de connexion ou interruptions de l'infrastructure du fournisseur d'accès pour des adresses qui ne seraient pas concernées par les mesures de blocage). **9)** Projet de révision de la loi sur le droit d'auteur (LDA) du 11 décembre 2015, basé sur les recommandations du

groupe de travail sur le droit d'auteur (AGUR12). **10)** AGUR 12 II, communiqué aux médias du 2 mars 217, Modernisation du droit d'auteur: compromis au sein de l'AGUR12 II («Les propositions de compromis n'incluent pas les mesures prévoyant le blocage par les fournisseurs d'accès, ni l'envoi de messages d'information en cas de violations graves de droits d'auteur par le biais de réseaux pair-à-pair»). **11)** Il existe différents sites web permettant de géolocaliser les noms de domaine, p. ex. http://fr.geoipview.com. **12)** Un changement pourrait se produire suite à une demande de blocage déposée par le distributeur de film zurichois (Praesenz-Film) contre Swisscom auprès du Handelsgericht de Berne, cf. Tagesanzeiger du 15 mars 2017, Ein Filmverleih zerrt die Swisscom vor Gericht. Cf. Cottier (n. 3), expliquant que les titulaires préféraient agir contre les responsables directs de l'atteinte. **13)** Infra 5. **14)** 17 U.S.C. § 512. **15)** Directive 2000/31/CE (Directive E-Commerce) (art. 12-15); Directive 2001/29/CE (InfoSoc) (art. 8 al. 3); Directive 2004/48/CE (art. 11). **16)** Rapport (n. 2), 3 concluant à l'absence d'intervention législative («Il faut donc renoncer a priori à l'introduction d'un instrument supplémentaire relevant du droit civil») et le même jour à la nécessité de légiférer en matière de droit d'auteur dans le rapport explicatif du Conseil fédéral du 11 décembre 2015 sur la modernisation du droit d'auteur, 31 («Le droit d'auteur constitue une exception. Pour lutter efficacement contre le piratage, il est nécessaire de se doter de réglementations spécifiques»). **17)** On peut aussi imaginer une violation de la LPD (p. ex. les utilisateurs d'un réseau social publient des données personnelles d'une personne. La légitimation passive en cas d'atteinte à la personnalité s'applique aussi à cet égard en raison du renvoi de l'art. 15 al. 1 à l'art. 28 CC, cf. Rapport (n. 2), 35. **18)** Arrêt du Tribunal fédéral 5A_792/2011 du 14.1.2013, consid. 6.2–6.3; La doctrine a critiqué cet arrêt au motif que cela conduisait à une légitimation passive illimitée, Schoch/Schüepp, Jusletter du 13.5.2012, n° 36. Cf. toutefois TF, 6 mai 2015, 5A_658/2014, sic! 2015, 571, c. 4.1 «Carl Hirschmann», rejetant la qualité de participant de celui qui met sur son site web un lien général vers le site Internet d'un journal ou d'une station de radio car le lien est «trop peu spécifique». **19)** Arrêt du Tribunal fédéral 5P.308/2003 du 28.10.2003, consid. 2.5 (propriétaire d'un site Web privé qui y reproduisait des articles de journaux contenant des atteintes à la personnalité); ATF 106 II 92 (journal qui avait reproduit des courriers de lecteurs de ce type); ATF 126 III 161 (imprimerie qui avait participé à la diffusion d'une série d'articles diffamatoires). **20)** Infra 5. Cf. toutefois: Aebi-Müller Regina E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Berne 2005, N 140; Geiser Thomas, Zivilrechtliche Fragen des Kommunikationsrechts, medialex 1996, 203 ss, 204, considérant qu'elle est aussi limitée par la causalité entre l'atteinte et la participation du prestataire. L'atteinte devrait être ainsi favorisée de manière générale par la participation et le demandeur devrait prouver la prévisibilité de l'atteinte. Rosenthal David, Aktuelle Anwaltspraxis 2013, 727 s.: admettant la légitimation passive des fournisseurs d'hébergement pas nécessairement celle des FAI faute de lien de causalité adéquate entre l'atteinte et leur participation. Contra: Rigamonti, considérant que la causalité semble tout le temps remplie puisque les services d'un prestataire sont généralement aptes «selon le cours ordinaire des choses et l'expérience de la vie» à entraîner la violation. **21)** Hess-Blumer Andri, Teilnahmehandlungen im Immaterialgüterrecht unter zivilrechtlichen Aspekten, sic! 2003, 100 s.; Schoch Nik/Schüepp Michael, Provider-Haftung «de près ou de loin»?, in: Jusletter du 13 mai 2012, 27 ss., justifiant l'application des règles de droit des brevets et de design aux atteintes de droit d'auteur au motif que législateur souhaitait une règlementation aussi uniforme que possible dans tout le droit de la propriété intellectuelle. Ils refusent par ailleurs d'appliquer la légitimation en référence à CC 28 au motif que la propriété intellectuelle porte sur des biens économiques, tandis que CC 28 porte sur des biens de la personnalité dont l'atteinte suppose une pesée des intérêts. **22)** ATF 129 III 588 (machine à broder à navettes), soulignant également que la règlementation de la participation inscrite à l'art. 66, let. d, LBI correspond au niveau du contenu à celle de l'art. 50 CO. **23)** Cf. toutefois Equey, 250, soulignant notamment l'éventuelle position de garant des prestataires qui permettrait de fonder une responsabilité pénale en tant que complice. Cf. aussi TF, 1B_242/2009, du 21.10.2009: dans un arrêt non officiellement publié du Tribunal cantonal vaudois du 2.4.2003, le juge a décidé que l'accès à Internet n'était pas un objet susceptible d'un séquestre/confiscation pénal. Il a toutefois demandé que les FAI soient informés du fait qu'ils pouvaient se rendre coupables de complicité de l'acte principal s'ils ne procédaient pas au blocage. **24)** Cf. toutefois Cottier, 690, rappelant que les exploitants de plateforme exercent généralement un certain contrôle éditorial et pourraient être ainsi considérés comme médias périodiques, même si le TF a pour l'instant refusé d'appliquer l'art. 266 CPC (mesures à l'encontre des médias) à un exploitant d'un réseau social. TF, 4 mai 2011, 5A_790/2010, c. 5.2; TF, 10 octobre 2013, 1C_335/2013. **25)** Cottier, 684. **26)** Cf. Schwarzenegger Christian, Sperrverfügungen gegen Access-Provider – über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, In: Internet-Recht und Electronic Commerce Law, Bern 2003, 249 ss. Contra: Heimgartner, Kommentar zur StPO, N 1a. **27)** Tribunal cantonal valaisan du 18 juin 2014, c. 4d («Le blocage provisoire, puis le cas échéant définitif, de l'accès à un blog contenant des 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»). Il s'agissait d'un revirement de jurisprudence: Tribunal cantonal du 2 avril 2003, JdT 2003 III p. 123, rejetant une ordonnance de blocage au motif («aucun objet [...] susceptible de confiscation») puis modifiant cette approche suite à l'arrêt du Tribunal pénal fédéral du 13 février 2005, BV 2004.26, admettant le blocage de sites web ayant servi à la publicité et à la vente illicite de produits thérapeutiques et médicaux au motif que l'adage «qui peut le plus peut le moins» permet de bloquer l'accès plutôt que de saisir le matériel; Tribunal cantonal du 3 avril 2008 («Bloquer définitivement l'accès à des sites donnés par les moyens techniques appropriés est possible, comme les recourantes l'admettent, et équivaut, dans ses effets, à une destruction au sens de l'art. 69 al. 2 CP. Certes, une telle opinion s'écarte de celle exprimée par l'autorité de céans dans son arrêt du 2 avril 2003. L'arrêt du Tribunal pénal fédéral du 16 février 2005 [...] permet toutefois un tel revirement»). **28)** TF, 19 mars 2015, 1B_294/2014, c. 4 («kann offen bleiben, ob die betroffenen Internet-Domains unter die einziehbaren gefährlichen Gegenstände bzw. deliktischen Instrumente subsumiert werden könnten. Die angefochtene Sperrung von Webseiten tangiert das verfassungsmässige Recht des Beschwerdeführers auf Meinungsäusserungs- und Informationsfreiheit. Jede Person hat insbesondere das Recht, ihre Meinung ungehindert zu äussern und zu verbreiten (Art. 16 Abs. 2 BV)»; Cottier, 685. Cf. Guyot/Métille, le Tribunal fédéral refuse le séquestre pénal d'un domaine ou d'un site web, medialex 2015, 69, qui considèrent que, en refusant l'analogie (entre le blocage comme cessation d'un comportement et la destruction au sens de CP 69 al. 2), le TF a mis fin aux décisions cantonales qui considéraient que des sites web rendaient possible la réalisation de l'infraction et pouvaient ainsi faire l'objet d'un séquestre. **29)** Guyot Nicolas/Métille Sylvain, 69. **30)** Guyot/Métille (n. 28), 69. **31)** Le TF devait se prononcer sur la validité d'une ordonnance du procureur vaudois requise contre Google respectivement Facebook visant à la production de données d'un compte utilisateur (identité de l'internaute, adresses IP utilisées pour créer le compte, le log de connexions sur une certaine période et le contenu privé du compte) qui aurait diffusé des œuvres de droit d'auteur respectivement qui aurait commis des injures et calomnies à l'égard d'un journaliste belge, TF, du 16 novembre 2016, 1B_142/ 2016, c. 3.1 («Compte tenu de cette lacune, le Procureur pouvait se fonder directement sur la disposition générale de l'art. 265 CPP pour édicter un ordre de production»). Le TF a toutefois refusé de l'appliquer en l'espèce car il n'est pas prouvé que l'entité suisse ait un accès direct sur les données («Il n'est pas démontré que la société suisse ait un accès direct ou une quelconque maîtrise sur les données relatives à ce service de messagerie») (c. 3.6). Il est intéressant de relever ici que, paradoxalement dans une décision rendue 1 mois plus tard, le TF a considéré que CPP 269 ss était applicable l'obligation de dépôt était applicable à l'égard des services de Gmail mais a refusé de l'appliquer pour des motifs procéduraux (la mesure n'avait pas été validée par le TMC) (CPP 273 al. 2) (TF, du 16 décembre 2016, c. 1.4.3). **32)** Dans l'arrêt «Blogger» (n. 28), le TF s'est bien gardé de toute position claire sur cette question et s'est contenté de renvoyer à l'instance précédente pour d'autres questions de procédure et de fond (soupçons et proportionnalité). **33)** N. 27 et 28. Pour des critiques générales sur la tendance à appliquer les règles de droit réel aux biens numériques, Benhamou Yaniv, Bien et immatériel: rapport suisse, in L'immatériel: Journées internationales de l'Association Henri Capitant 2014, Bruxelles (Bruylant) 2015, p. 311. **34)** Contrairement à CP 69, elles n'exigent toutefois pas de mise en danger de l'ordre public. ATF 132 IV 55, c. 1a; FF 1985 1061. **35)** La notion d'objets ou représentations s'entend largement (p. ex. CD, DVD, autres supports électroniques) mais porte bien sur le support en tant qu'objet. Cf. TPF SK.2007.4 du 4 juin 2007, c. 17.1 («les sites gérés par A. avaient pour objectif principal, sinon unique, d'apporter un soutien aux activités et à la propagande de réseaux terroristes islamiques, en particulier du réseau Al-Qaïda [...] Aux fins visées par l'art. 69 CP doivent ainsi être confisqués, puis détruits, les instruments informatiques (ordinateurs, disques durs, floppy disk, CD-ROM, modem, imprimantes, etc.) ayant été utilisés par les accusés ou par des tiers pour recevoir, alimenter ou créer des liens avec les sites en question, ainsi que tous les écrits, enregistrements sonores ou vidéos reproduisant en tout ou en partie le contenu des mêmes sites.»); Moreillon Laurent et al., Petit Commentaire, 2ème éd., Bâle 2017, art. 135 CP N 6; Aebersold Peter, Basler Kommentar Strafrecht II, 3ème éd., Bâle 2013, art. 135 N 11. **36)** Cf. Infra 4. Même les actes de violence et de terrorisme ne peuvent pas faire l'objet d'une mesure contraignante mais seulement de coopération. **37)** Même si le juge pénal n'a pas la même liberté que le juge civil quant au comblement des lacunes, il est tout de même autorisé à interpréter

une norme de manière extensive et à combler les lacunes proprement dites par le raisonnement analogique: ATF 127 IV 198, c. 3b, JdT 2003 IV IV 112; Moreillon et al. (n. 35), art. 1 N 30. **38)** ATF 140 IV 181, c. 2.4, JdT 2015 IV 167, c. 2.6: après que le destinataire a consulté son compte, avant l'e-mail ne peut pas être séquestré mais uniquement placé sous surveillance. **39)** La notion de morale et d'ordre public est en effet une notion large évolutive et couvre notamment la propagation de propos négationnistes, ATF 127 IV 203; Hirsig-Vouilloz Madeleine, Commentaire romand du Code pénal I, Bâle 2009, Art. 69 N 27. **40)** «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» (Annexe ODI). L'OFCOM est le registre pour le TLD «.swiss» et a délégué cette tâche à la fondation Switch pour le TLD «.ch». **41)** Supra n. 10. **42)** Cottier, 686, relève que cette démarche a porté ses fruits dans certains domaines, p. ex. dans la lutte contre la pédopornographie. **43)** Rapport (n. 2), 31: Une action contre un participant qui ne peut pas raisonnablement éviter ni faire cesser l'atteinte est en conséquence vouée à l'échec. **44)** Rapport (n. 2), 31, comparant une imprimerie typique et un hébergeur en citant l'ATF 126 III 161 (une «imprimerie typique doit toutefois être considérée comme sensiblement plus proche des contenus qu'un fournisseur d'hébergement typique dont les services sont largement automatisés»). **45)** Supra n. 27. **46)** CF. CJUE C-70/10 du 24.11.2011 (Scarlet c. SABAM), appréciant différents droits fondamentaux, en particulier la protection de la propriété intellectuelle (art. 17.2 Charte des droits fondamentaux), la liberté du commerce des FAI (art. 16 Charte des droits fondamentaux), la liberté d'expression des internautes et exploitants de plateforme (art. 11 Charte), protection de la vie privée et des données personnelles (art. 7–8 Charte des droits fondamentaux). D'autres droits fondamentaux ont parfois été invoqués (p. ex. droit au secret des télécommunications et à la protection des données) mais n'ont pas empêché l'injonction de blocage. Le secret des télécommunications protège uniquement le contenu de la communication qui n'est pas affecté par la mesure de blocage, et pas les informations publiques. Le traitement des données est autorisé par contrat entre l'internaute et le FAI. Pour une analyse plus détaillée, cf. Oliver Jo/Blobel Elena, Website blocking injunctions – a decade of development, Schulthess 2017, 27. **47)** Cf. CEDH, décision du 19 février 2013, Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden (40397/12). **48)** CJUE, arrêt du 27 mars 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Ors (C-314/12). Pour des décisions nationales, cf. références citées par Oliver/Blobel (n. 46), n. 117. **49)** P. ex. Cour suprême allemande (BGH), décision du 26 novembre 2015, Universal Music GmbH et al. v. Telefonica Germany GmbH & Co. OHG (I ZR 174/14), indiquant que la mesure de blocage ne peut pas être admise uniquement à l'égard de sites web offrant du contenu uniquement illicite. Dans certains cas, elle doit être possible même si elle conduit à la suspension de contenu légal. **50)** CJUE, arrêt du 27 mars 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Ors (C-314/12), c. 56: «les mesures qui sont adoptées par les fournisseurs d'accès doivent être strictement ciblées, en ce sens qu'elles doivent servir à mettre fin à l'atteinte portée par un tiers au droit d'auteur ou à un droit voisin, sans que les utilisateurs d'Internet ayant recours aux services de ce fournisseur afin d'accéder de façon licite à des informations s'en trouvent affectés». La mesure ordonnée quant à la technique visée varient d'une juridiction à l'autre: en Belgique et en France, les tribunaux laissent généralement la question technique à l'appréciation du FAI, tandis qu'au Danemark et en Finlande les tribunaux ordonnent la méthode exacte du blocage, cf. Oliver/Blobel (n. 46), 25. **51)** CEDH, décision du 19 février 2013, Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden (40397/12). **52)** Cf. UPC Telekabel, cité en n. 48, indiquant que la mesure doit être «strictement ciblée». Cf. aussi la jurisprudence CEDH: l'injonction de blocage doit être «foreseeable in its application if it is formulated with sufficient precision to enable individuals (...) to regulate their conduct» (Ahmet Yildirim, 18 Dec. 2012); «must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise» (ECrHR, Sanoma, 14.9.2010, § 82). **53)** Rapport explicatif (n. 16), 70–72: «sont ciblés les sites Internet qui hébergent principalement des offres pirates (sites pirates). Ne sont pas visées les offres d'oeuvres et autres objets isolés rendus accessibles de manière illicite qui se trouvent sur des sites proposant essentiellement des contenus licites [...] Sont donc ciblés les sites Internet qui hébergent principalement des offres pirates.». **54)** Arrêt de la Cour suprême des Etats-Unis d'Amérique du 27 juin 2005, 545 U.S. (2005). Pour une analyse de l'arrêt, cf. Urs Portmann/Peter Ling, Le partage de fichier en ligne après l'arrêt Groksoter et dans le projet de révision de la LDA, CEDIDAC 2005. **55)** Art. 27 2.3 Canadian Copyright Act. **56)** CEDH, Neij and Sunde Kolmisoppi v. Sweden, 19 février 2013. **57)** CEDH Delfi AS c. Estonie, 16 juin 2015 (n° 64569/09). **58)** PLDA va dans ce sens en rappelant que «La mesure arrêtée doit aussi être proportionnée sur le plan technique ou sur celui de l'exploitation pour le fournisseur de services de télécommunication» et prévoit que la FAI peut faire opposition comme prévu à l'art. 66e, al. 2, let. b. **59)** Rapport (n. 2), p. 47 **60)** Rapport explicatif (n. 16), 72. **61)** Equey, 331. **62)** Equey, 330, expliquant que le FAI peut maîtriser ces coûts au moyen d'un logiciel permettant de répondre à une requête DNS, soit directement (parce qu'il connaît l'URL) ou indirectement (en interrogeant le registre concerné). **63)** Cf. la récente décision «Allostreaming» de la Cour de cassation, arrêt n° 909 du 6 juillet 2017 opposant l'Union des producteurs de cinéma à SFR, Orange, Free, Bouygues télécom, et autres. Cf. Oliver/Blobel (n. 48), 19 et les nombreuses références citées, en particulier la décision Cartier dans laquelle la Court of Appeal a donné différents motifs justifiant que l'opérateur supporte les coûts. Cf. aussi Federal Court of Australia, judgment of 15 December 2016, Roadshow Films Pty Ltd v. Telstra Corporation Ltd (FCA 1503), où le tribunal a ordonné au demandeur de payer AUD 50 pour chaque nom de domaine bloqué auprès de chaque FAI mais refusé de lui faire supporter les coûts généraux au motif qu'ils font partie des «coûts généraux pour conduire une telle activité». **64)** Sur le remboursement de tels frais en général, cf. Jeanneret Yvan/Kuhn André, Précis de procédure pénale, Berne 2013, N 5079. **65)** cf. Equey, 331, indiquant que les systèmes sont souvent automatisés, déjà en place pour bloquer d'autres contenus (p. ex. en matière de lutte contre la pornographie et le terrorisme) et permettent le blocage d'autres adresses IP/URL à moindres coûts (p. ex. via les services «Whitebox» ou «Netclean» permettant un filtrage des seules listes d'adresses IP suspectes). Cf. Oliver/Blobel (n. 48), 19, mentionnant une décision anglaise dans lesquelles le coût marginal a été établi à £ 100 par nom de domaine (après un coût de mise en place initiale de £ 5,000) (Court of Appeal, judgment of 6 July 2016, Cartier International AG and Ors v. British Sky Broadcasting Ltd and Ors ([2016] EWCA Civ 658), para. 19). **66)** BGH, arrêt du 26 novembre 2015, (1 ZR 174/14); BGH, arrêt du 26 novembre 2015, (I ZR 3/14). **67)** Rapport explicatif (n. 16), 35: le concours des hébergeurs est requis en premier lieu (car ils sont plus proches du contenu) et les FAI n'interviennent par le biais de blocages d'accès que subsidiairement «dans les cas où lutter directement contre les modèles commerciaux fondés sur les violations du droit d'auteur s'avère impossible du fait que l'exploitant parvient à rester hors d'atteinte grâce à un choix judicieux de son implantation ou par le recours à un brouillage technique». **68)** En droit suisse, on se rappelera que, vu les dispositions légales ne prévoyant pas une telle subsidiarité, la jurisprudence permet au demandeur d'agir à choix contre qui il souhaite, supra n. 18. En droit européen, l'art. 8(3) InfoSoc prévoit la mesure de blocage sans exigence de subsidiarité et le considérant 59 précise que le blocage doit être possible sans préjudice des autres sanctions. Cf. contribution de Oliver/Blobel (n. 48), 8. **69)** Au sujet du droit à la désindexation en droit suisse, cf. Meier Philippe, Le droit à l'oubli: la perspective de droit suisse, Lausanne 2015, 23 ss. **70)** Cf. décision «Allostreaming» du 15 mars 2016 de la cour d'appel de Paris précédent la décision de la Cour de cassation citée en n. 63. Cette décision confirmait tant les mesures de blocage à l'égard des FAI que les demandes de désindexation à l'égard des moteurs de recherche (Google, Yahoo). **71)** Cf. Oliver/Blobel (n. 48), 23 donnant l'exemple de The Pirate Bay qui a utilisé depuis 2012 différents noms de domaines, dont .org (qu'elle a cessé d'utiliser après une procédure américaine), .se (qu'elle a cessé d'utiliser après le séquestre du nom de domaine en Suède), .gs, .la, .mn, .am et .gd. **72)** CJUE, arrêt du 27 mars 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Ors (C-314/12), c. 58 ss.; CJUE, arrêt du 24 novembre 2011, Scarlet Extended SA v. Société Belge Des Auteurs, Compositeurs et Éditeurs SCRL (SABAM) (C-70/10), c. 43. **73)** Brett Danaher/Michael D. Smith/Rahul Telang, Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior, Pittspurg 2016; Site Blocking Efficacy Study United Kingdom, Incopro, 2014. **74)** Equey, 332. **75)** Cf. Oliver/Blobel (n. 48), 23. **76)** High Court of Justice, Chancery Division, judgment of 13 March 2017, The Football Association Premier League Limited v. British Telecommunications Plc and Ors ([2017] EWHC 480 (Ch)). **77)** Bohnet, N 86. **78)** Hofmann, 208: avec l'exécution directe, les mesures demandées sont prises par le tribunal saisi du fond du litige: dans son dispositif, le tribunal peut d'ores et déjà, sur requête de l'une des parties, ordonner l'exécution de sa décision ou en fixer les modalités (art. 236 al. 3 CPC; art. 337 al. 1 CPC). **79)** Hofmann, 209: après le dépôt de la requête en exécution, le tribunal de l'exécution examine d'office le caractère exécutoire de la décision présentée (art. 341 al. 2 CPC) et impartit un délai à la partie intimée pour se prononcer sur la requête (art. 339 al. 2 CPC) (qui peut notamment faire valoir que la condition n'est pas remplie ou que la contre-prestation n'a pas été effectuée) avant de décider d'une mesure d'exécution (indirecte) parmi celles prévues à l'art. 343 CPC. **80)** Rapport (n. 2), 31: Une action contre un participant qui ne peut pas raisonnablement éviter ni faire cesser l'atteinte est en conséquence vouée à l'échec. **81)** Rapport (n. 2), 31, comparant une imprimerie typique et un hébergeur en citant l'ATF 126 III 161 (une «imprimerie typique doit toutefois être considérée comme sensiblement plus proche des contenus qu'un fournisseur d'hébergement typique dont les services sont largement automatisés»). **82)** Rapport explicatif (n. 16), 73.